Waltteri Ylitalo

NEUTRALISAATIOTEKNIIKOIDEN HYÖDYNTÄMINEN OSANA ORGANISAATIOIDEN TIETOTURVATUTKIMUSTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Ylitalo, Waltteri
Neutralisaatiotekniikoiden hyödyntäminen osana organisaatioiden tietoturvatutkimusta
Jyväskylä: Jyväskylän yliopisto, 2021, 44 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Marttiin, Pentti

Informaatioteknologian valtavirtaistumisen seurauksena yhä useammat organisaatiot toimialasta riippumatta hyödyntävät informaatioteknologiaa operatiivisessa ja strategisessa toiminnassaan. Hyötyjen ohella informaatioteknologian käyttö on tuottanut uusia tietoturvaan liittyviä uhkakuvia, joihin organisaatiot pyrkivät vastaamaan moniulotteisilla ratkaisuilla. Yksi merkittävimmistä tunnistetuista tietoturvauhista on työntekijöiden tietoturvaohjeistuksen vastainen toiminta, minkä seurauksena tärkeäksi kysymykseksi on noussut, miksi työntekijät poikkeavat ohjeista. Lupaavana tuoreena suuntauksena esiintyvät neutralisaatiotekniikat, jotka esittävät työntekijöiden neutralisoivan itselleen haitallisia ohjeistuksen vastaisesta toiminnasta aiheutuvia seurauksia. Tämä tutkielma tuottaa kuvailevan kirjallisuuskatsauksen neutralisaatiotekniikoita hyödyntäviin organisaatioiden tietoturvaa tutkiviin tutkimuksiin. Tutkielman avulla tuotetaan vastaus tutkimuskysymyksiin, jotka ovat miten neutralisaatiotekniikoita on hyödynnetty osana organisaatioiden tietoturvatutkimusta ja minkälaisia tuloksia tutkimukset ovat saavuttaneet koskien neutralisaatiotekniikoita. Tutkielman tulosten perusteella neutralisaatiotekniikoita hyödyntävät julkaisut jaetaan neljään aihepiiriin ja todetaan, että tutkimusten painopiste on muuttunut viimeisen kymmenen vuoden aikana. Lisäksi tutkielman tulosten perusteella todetaan, että neutralisaatiotekniikat tuottavat vahvaa tukea neutralisaatiotekniikoiden kriittiselle roolille osana tietoturvaa sekä neutralisaatiotekniikoiden olevan vahvasti olosuhderiippuvaisia, mikä aiheuttaa ongelmia yleistettävyydelle. Lopuksi tutkielma esittää aihepiirin osalta keskeisiä jatkotutkimuksen kohteita, jotka vaihtelevat kokonaisista tutkimussuuntauksista suoriin yksittäisiin tutkimuskohteisiin.

Asiasanat: neutralisaatiotekniikat, tietoturva, tietoturvakäyttäytyminen, tietoturvaohjeistus, organisaatioiden tietoturva

ABSTRACT

Ylitalo, Waltteri
The use of neutralization techniques within organizational information security research
Jyväskylä: University of Jyväskylä, 2021, 44 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Marttiin, Pentti

Information technology has become a key component in strategic and operational functions across most market sectors. Alongside the benefits and perks information technology has also brought new threats regarding information security, which organization have tried to resolve with various solutions. A pivotal threat identified by experts is the human factor of cybersecurity and more specifically employee non-compliance towards internal information security policies. A promising line of research in understanding this phenomenon is the theory of neutralization techniques, which argues that employees are able to break organizational security policies by neutralizing the negative social consequences caused by their actions. This thesis provides a descriptive literature review regarding the use of neutralization techniques within organizational information security research. More specifically this thesis provides an answer to the following research questions, how have neutralization techniques been used in organizational information security research and what types of results have these studies generated regarding the techniques of neutralization. Based on the findings of this thesis existing research is divided into four groups based on their topic and findings show that the focus of these studies has shifted over the past decade. The findings also show that neutralization techniques are condition dependent, which cause problems in generalization and that existing research finds strong support for the importance of neutralization as a part of cybersecurity. Finally, this thesis presents recommendations on future research by offering broader future research areas and more specific individual research topics.

Keywords: neutralization techniques, information security, information security behavior, information security policy, organizational information security

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viimeisten vuosikymmenien aikana ihmiset ympärimaailman ovat olleet osana suurinta yhteiskunnan mullistusta sitten teollisen vallankumouksen ja todistaneet digitaalisen vallankumouksen alkua. Informaatioteknologian valtavirtaistumisen yhteydessä yhä useammat yritysten ja yhteiskunnan tarjoamat palvelut ovat siirtyneet digitaaliseen muotoon mullistaen monet arjen keskeisistä toiminnoista (Williams, Chatterjee & Rossi, 2008). Vastatakseen kuluttajien vaatimuksiin organisaatiot ovat muovanneet omaa palveluiden tuotantoaan ja kehittäneet uusia digitaalisia työkaluja hyödyntäviä toimintamenetelmiä (Williams ym., 2008; Vendrell-Herrero, Bustinza, Parry & Georgantzis, 2017). Jatkuvan kehityksen seurauksena yhä suurempi osa organisaatioiden tärkeistä strategisista toiminnoista toimii tänä päivänä teknisillä laitteilla ja informaatioteknologian rooli on keskeinen lähes toimialasta riippumatta.

Informaatioteknologian tehokas hyödyntäminen on mahdollistanut organisaatioille kyvyn tuottaa uusia innovaatioita, tehostaa toimintaansa sekä muovannut täysin uusi toimialoja (Versteeg & Bouwman, 2006). Menestyksestä huolimatta informaatioteknologian integroiminen osaksi organisaation toimintaa on aiheuttanut riskienhallinnan näkökulmasta uusia ja potentiaalisesti erittäin haitallisia uhkakuvia. Tiedon arvon kasvaessa ja kyberrikollisuuden yleistyessä organisaatioiden tietoturvasta vastaavat toimijat joutuvat kamppailemaan jatkuvassa tietoturvauhkien ja suojausmenetelmien kilpajuoksussa varmistaakseen tietoturvallisen toiminnan (Tounsi & Rais, 2018).

Säännöllisen kehitystyön ja ajan tasalla toimivan riskienhallinnan ansioista monet toimijat ovat voineet ottaa käyttöönsä entistä tehokkaampia teknisiä ratkaisuja kriittisten teknologioidensa turvaamiseksi. Tietoturvan teknisen ulottuvuuden kehittymisestä huolimatta tietoturvauhat ovat yhä merkittävästi läsnä osana organisaatioiden jokapäiväistä operatiivista toimintaa. Teknologisen kehityksen seurauksena monet verkkorikollisuutta harrastavat tahot ovat huomanneet teknologian heikkouksia hyödyntävien hyökkäysten olevan entistä vaivalloisempia ja haastavampia toteuttaa, minkä seurauksena merkittävä osa hyökkäyksistä kohdennetaankin tänä päivänä tietoturvan inhimilliseen ulottuvuuteen, eli ihmisiin (Abawajy, 2014).

Tänä päivänä organisaatioiden tietoturva-asiantuntijat tunnistavat riskienhallinnan yhteydessä inhimillisen tietoturvan kriittisten roolin osana tietoturvan kokonaisuutta. Asiantuntijoiden ja tutkijoiden mukaan tänä päivänä valtaosa organisaatioihin kohdistuvista kyberiskuista ovat kohdistettuja työntekijöihin, minkä seurauksena organisaatioiden henkilöstön puutteellinen tietoturvaosaaminen nähdään yhtenä merkittävimmistä tietoturvauhkista (Dlamini, Eloff & Eloff, 2009; Warkentin & Willison, 2009). Vastatakseen henkilökuntaan kohdistuviin hyökkäyksiin monet organisaatioista hyödyntävät erilaisia tietoturvakoulutuksia ja muita interventiota valmiuden ylläpitämiseksi. Kyseisten menetelmien on tutkimusten perusteella osoitettu lisäävän osaamista ulkoisia tietoturvauhkia kohtaan (Abawajy, 2014).

Ulkoiset tietoturvauhat eivät kuitenkaan muodosta koko riskien joukkoa, minkä seurauksena ulkoisten uhkien torjumisen ohella merkittävänä inhimillisen tietoturvan elementtinä toimii myös työntekijöiden sitoutuminen tietoturvaohjeistusten noudattamiseen. Alan asiantuntijoiden arvioiden perusteella jopa yli puolet organisaatioiden kohtaamista tietomurroista ovat tietoturvaohjeistusten vastaisesti toimineiden työntekijöiden aiheuttamia (Vance, Siponen & Pahnila, 2012; D'arcy, Hovav & Galletta, 2009). Kyseisen tiedon valossa organisaatioiden tietoturvaa käsittelevä tutkimuskirjallisuus onkin pyrkinyt ymmärtämään syitä tietoturvaohjeistuksen vastaisen käytöksen taustalla.

Tutkitun tiedon perusteella useat tutkijaryhmät ovat esittäneet eri malleja, jotka pyrkivät ennustamaan työntekijöiden tietoturvakäyttäytymistä. Yksi tärkeimmistä ja laajimmin hyödynnetyistä malleista tietoturvan kontekstissa on peloteteoria (englanniksi deterrence theory), jonka mukaan erilaisten pelotteiden ja sanktioiden avulla voidaan ehkäistä rationaalisten henkilöiden tietoturvaohjeistuksen vastaista toimintaa (D'arcy & Herath, 2011). Vaikka peloteteoriaa on hyödynnetty laajasti useiden tutkijoiden toimesta ovat teorialla saadut tulokset olleet ristiriitaisia, minkä seurauksena kasvava joukko alan tutkijoita on alkanut kyseenalaistamaan teorian valta-asemaa (Siponen & Vance, 2010).

Uutena lupaavana tutkimussuuntana esiintyy neutralisaatiotekniikoita hyödyntävät tietoturvatutkimukset. Neutralisaatiotekniikat ovat peloteteorian tapaan kriminologian tutkimuksesta omaksuttu teoria, joka argumentoi yksilöiden hyödyntävän erilaisia neutralisaatiomenetelmiä ei toivotun toiminnan yhteydessä. Alkuperäinen kriminologian tutkimuskirjallisuus soveltaa neutralisaatiotekniikoiden käyttöä sosiaalisten haittojen, kuten häpeän lieventämiseen, mutta poikkitieteellinen kirjallisuus on osoittanut, että neutralisaatiota voidaan myös hyödyntää konkreettisten haittojen, kuten sanktioiden ja pelotteiden heikentämiseen (Siponen & Vance, 2010). Kyseisen tiedon valossa neutralisaatiotekniikoiden hyödyntäminen esiintyykin mahdollisena syynä pelotteista ja sanktioista huolimatta tapahtuville tietoturvarikkomuksille.

Tämän tutkielman tavoitteena on suorittaa kuvaileva kirjallisuuskatsaus neutralisaatiotekniikoita hyödyntäviin organisaatioiden tietoturvatutkimuksiin. Tutkielman tarkastelee neutralisaatiotekniikoita kahdesta keskeisestä näkökulmasta, jotka ovat neutralisaatiotekniikoiden rooli tutkimuksissa sekä tutkimus-

tulokset koskien neutralisaatiotekniikoita. Näiden kriteerien pohjalta tutkielman tutkimuskysymyksiksi muodostuvat seuraavat:

- Miten neutralisaatiotekniikoita on hyödynnetty osana organisaatioiden tietoturvatutkimusta?
- Minkälaisia tutkimustuloksia neutralisaatiotekniikoita hyödyntävät tutkimukset ovat tuottaneet koskien neutralisaatiotekniikoita?

Tutkielman toteuttamisen osalta aineistoa kerättiin Jyväskylän yliopiston tarjoamista palveluista, kuten JYKDOK:ista sekä yliopiston tarjoamista tietokannoista. Tämän lisäksi aineiston haussa hyödynnettiin myös Google Scholar palvelua. Tutkimusaineiston valintaan vaikuttavat ensisijaisesti kaksi kriteeriä, jotka ovat tutkimuksen julkaisualustan laatu sekä tutkimuksen tuoreus. Aineiston laatua arvioitiin julkaisualustan JUFO-luokituksen perusteella sekä julkaisujen sisällöllisen luotettavuuden osalta. Tutkielman aineiston osalta pyrittiin hyödyntämään ensisijaisesti tutkimuksia, jotka saavuttavat Julkaisufoorumin arvosteluasteikolla luokan kaksi tai kolme.

Aineiston toisen kriteerin eli tutkimusten julkaisuvuoden osalta tavoitteena oli hyödyntää mahdollisimman tuoreita julkaisuja, jotka ovat julkaistu 2000-luvulla. Tämän rajauksen tarkoituksena oli varmistaa tutkielmassa käsiteltävien julkaisujen osuvuus tutkimuskysymyksiin sekä varmistaa aineiston riittävä rajaus. Tutkielman keskeinen teoreettinen viitekehys ulottuu kauas 1950-luvulle, minkä seurauksena kaikkien tutkimusten systemaattinen käsittely ei ole tietoturvan näkökulmasta relevanttia eikä edes mahdollista. Poikkeuksen tutkimusten ajankohtaan muodostaa tutkielman toinen luku, jossa käsitellään neutralisaatiotekniikoiden teoriaa. Tämän luvun yhteydessä hyödynnetään neutralisaatiotekniikoiden teoreettisen taustan kannalta tärkeitä julkaisuja, joiden julkaisu ajankohta sijoittuu 1900-luvulle.

Tutkielman lopun rakenne noudattaa seuraavaa kaavaa. Tutkielman toisessa luvussa tarkastellaan neutralisaatiotekniikoiden teoriaa, määritelmää sekä tiivisti teorian historiallista kehitystä. Kolmannessa luvussa tarkastellaan neutralisaatiotekniikoita organisaation tietoturvan yhteydessä hyödyntäviä tutkimuksia sekä esitellään tutkimusten tavoitteita ja tuloksia. Neljässä luvussa esitetään tutkielman löydöksiä ja vastataan tulosten avulla tutkielman tutkimuskysymyksiin. Tulosten lisäksi neljäs luku sisältää myös tulosten pohdintaosion, jossa tarkastellaan tulosten perusteella saavutettuja johtopäätöksiä sekä niiden perusteella ilmeneviä implikaatioita ja esiin nousevia jatkotutkimusaiheita. Viimeisenä tutkielman lukuna on yhteenveto, jonka yhteydessä tiivistetään tutkielman keskeinen sisältö ja löydökset.

2 NEUTRALISAATIOTEKNIIKOIDEN TEOREETTINEN TAUSTA

Tässä pääluvussa käsitellään neutralisaatiotekniikoiden teoreettinen tausta sekä määritellään tutkielman kannalta keskeiset käsitteet. Luku alkaa tiiviillä katsauksella neutralisaatiotekniikoiden historiaan ja jatkaa siitä neutralisaatiotekniikoiden määrittelyyn. Neutralisaatiotekniikoiden yleisen määritelmän pohjalta jatketaan viiden keskeisimmän neutralisaatiotekniikan kattavampaan esittelyyn ja määrittelyyn. Luvun viimeisessä alakappaleessa suoritetaan tiivis katsaus viiden päätekniikan ulkopuolelle jääneisiin neutralisaatiotekniikoihin, ja pyritään tarjoamaan lukijoille laajempi teoreettinen pohja neutralisaatiotekniikoista.

2.1 Neutralisaatiotekniikoiden historia

Neutralisaatiotekniikoiden alkuperäinen teoreettinen pohja ulottuu aina 1940-luvulle, jossa sosiologian sekä kriminologian tutkijat pyrkivät ymmärtämään eri väestönryhmien sosiaalisista normeista poikkeavaa käyttäytymistä. Merkittävänä neutralisaatiotekniikoiden syntyyn vaikuttaneena tutkimuksena voidaan pitää Edwin Sutherlandin vuonna 1945 julkaistua tutkimusta koskien niin sanottua ”white collar crime” eli esimiestason työntekijöiden tekemiä rikoksia (Kaptein & van Helvoort, 2019). Tutkimuksessaan Sutherland esitti työntekijöiden hyödyntävän rationalisointia eli järkeilyä rikostensa yhteydessä, minkä avulla he pyrkivät selittämään toimintaansa moraalisesti hyväksyttäväksi (Sutherland, 1945; Kaptein & van Helvoort, 2019).

Vajaa kymmenen vuotta myöhemmin Donald Cressey tutki puolestaan erilaisia huijauksia harrastavien rikollisten toimintaa vuonna 1951 julkaistussa tutkimuksessaan. Tutkimuksen pohjalta Cressey havaitsi huijareiden hyödyntävän, esimerkiksi itselleen edullista sanamuotoilua osana omaa rikollista toi-

mintaansa (Maruna & Copes, 2005; Kaptein & van Helvoort, 2019). Sanamuotoilun avulla huijauksia harrastaneet rikolliset pyrkivät perustelemaan ja järkeilemään toimintansa itselleen täysin lailliseksi sekä hyväksyttäviksi.

Edellä mainitut teoriat toimivat teoreettisena pohjana vuonna 1957 julkaistulle Gresham Sykesin ja David Matzan tutkimukselle, jossa he pyrkivät tutkimaan nuorisorikollisten rikolliseen toimintaan vaikuttavia tekijöitä (Sykes & Matza, 1957; Maruna & Copes, 2005). Sykes and Matza hyödynsivät omassa tutkimuksessaan aikaisempaa rationalisoinnin teoreettista pohjaa sekä haastoivat vuonna 1955 julkaistua kilpailevaa Albert Cohenin teoriaa alakulttuureista, joissa rikoksen tekijät pyrkivät luomaan omia moraalisia ja sosiaalisia normejaan (Minor, 1981). Sykes ja Matza kritisoivat Cohenin näkemystä omassa tutkimuksessaan, jossa he korostivat rikokseen syyllistyneiden nuorten tunnustavan ja jopa joltain osin kunnioittavan yhteiskunnan normeja rikollisesta toiminnastaan huolimatta (Sykes & Matza, 1957). Tämän johtopäätöksen perusteella olisi Sykesin ja Matzan mukaan epätodennäköistä, että rikoksiin syyllistyneet henkilöt pyrkisivät kokonaan uudistamaan yhteiskunnan normeja. Sykes ja Matza argumentoivat omassa tutkimuksessa nuorten hyödyntävän ensisijaisesti järkeilyä sekä neutralisointia omien tekojensa hyvittämiseksi, yhteiskunnan normeja vastaan kapinoimisen sijaan.

Aikaisemman teoreettisen pohjan hyödyntämisen ohella Sykes ja Matza pyrkivät myös tutkimuksessaan laajentamaan näkemystä rationalisoinnista. Aikaisemmassa rationalisaatiota käsittelevässä tutkimuskirjallisuudessa korostui näkemys, jossa rikollisen tai muuten normien vastaisen käytöksen hyvittäminen tapahtui vasta teon jälkeen. Sykes ja Matza kritisoivat omassa tutkimuksessaan tätä näkemystä ja pyrkivät argumentoimaan rationalisoinnin tapahtuvan jo ennen normeja rikkovaa tapahtumaa (Kaptein & van Helvoort, 2019). Sykes ja Matza esittävätkin, että normien rikkomisesta aiheutuvaa moraalista haittaa pyritäänkin ehkäisemään jo ennen varsinaista tekoa hyödyntämällä neutralisaatiotekniikoita, mikä mahdollistaa kynnyksen ylittämisen ennen tietotoisesti väärää tekoa (Sykes & Matza, 1957).

Tutkimuksessaan Sykes ja Matza esittelevät ensimmäistä kertaa myös neutralisaatiotekniikat käsitteenä, minkä jälkeen käsitettä ryhdytään hyödyntämään osana tulevaa tutkimuskirjallisuutta. Sykesin ja Matzan tutkimusta seuranneessa tutkimuskirjallisuudessa käsitteitä neutralisaatiotekniikat sekä rationalisointi käytetään samaa tarkoittavana terminä ja näiden rajaa pidetään häilyvänä (Kaptein & van Helvoort, 2019). Tämän tutkielman osalta neutralisaatiotekniikoita tullaan tästä eteenpäin käsittelemään omana itsenäisenä käsitteenään eikä, sillä tulla viittaamaan aikaisempaan Sutherlandin käyttämään rationalisaation käsitteeseen.

Sykesin ja Matzan alkuperäisen tutkimusartikkelin pohjalta neutralisaatiotekniikoita on hyödynnetty laajasti osana kriminologian sekä muiden tieteenalojen tutkimusta (Maruna & Copes, 2005). Erityisenä neutralisaatiotekniikoiden meriittinä Maruna ja Copes mainitsevat teorian onnistuneen soveltamisen osana haastavampaa sekä vaativampaa kriminologian tutkimusta. Kriminologian ohella tutkijat ovat myös onnistuneet hyödyntämään neutralisaatiotek-

niikoita osana poikkitieteellistä tutkimusta, ja malli on saavuttanut suosiota osana monia eri tutkimusaloja. Neutralisaatiotekniikoita on hyödynnetty, esimerkiksi, osana liike-elämän etiikkaa (De Bock & Van Kenhove, 2011) sekä organisaatioiden tietoturva ohjeistusten noudattamista ja yleistä tietoturvaa (Siponen & Vance, 2010) käsittelevää tutkimusta.

Nykyään neutralisaatiotekniikat ovat yhä laajasti hyödynnetty malli, jonka avulla pyritään vastamaan, esimerkiksi tietoturvakäyttäytymistä koskeviin kysymyksiin. Menestyksestään huolimatta neutralisaatiotekniikat ovat kohdanneet myös kritiikkiä sekä tuottaneet ajoittain ristiriitaisia tuloksia (Maruna & Copes, 2005). Tunnistettujen rajoitusten ja puutteiden johdosta neutralisaatiotekniikoiden kehitys jatkuu vielä tänäkin päivänä yli 60 vuotta teorian esittelemisen jälkeen (Kaptein & van Helvoort, 2019).

2.2 Neutralisaatiotekniikoiden määritelmä

Neutralisaatiotekniikoiden määritelmä on melko vakiintunut tutkimuskirjallisuudessa sisältönsä ja tarkoituksena osalta. Tutkimuskirjallisuus esittelee neutralisaatiotekniikat pääsääntöisesti kriminologian teoriana, joka pyrkii selittämään, miten normeista poikkeavaa toimintaa pyritään selittämään, perustelemaan tai oikeuttamaan. Vakiintuneesta käsityksestä huolimatta neutralisaatiotekniikoiden määrittely poikkeaa tutkijoiden keskuudessa erityisesti sanamuotojen osalta. Virallisen muotoilun ohella tutkimuskirjallisuudessa ilmenee eroja myös neutralisaatiotekniikoiksi luettavien menetelmien välillä.

Alkuperäisessä julkaisussaan tutkijat Sykes ja Matza määrittelevät neutralisaatiotekniikat menetelmiksi, joilla rikollista toimintaa harrastavat yksilöt, voivat oikeuttaa sekä perustella omaa toimintaansa ja täten välttää omasta normien vastaisesta toiminnastaan aiheutuvia sosiaalisia haittoja (Sykes & Matza, 1957). Keskeisenä piirteenä Sykes ja Matza korostavat neutralisaatiotekniikoiden tarjoamaa mahdollisuutta perustella normien vastainen toiminta ennen tapahtumaa, minkä johdosta toimintaan syyllistyvä henkilö voi neutralisoida moraaliset tekoa estävät kynnykset.

Willison, Warkentin ja Johnston (2018) määrittelevät omassa tietoturvaa koskevassa tutkimuksessaan neutralisaatiotekniikat tekniikoiksi, joilla rikoksentekijät voivat vapauttaa itsensä omaksutuista normeista sekä sosiaalisesta paheksunnasta. Tämän seurauksena rikostentekijät voivat toteuttaa aikomuksensa vapaasti ilman syyllisyyden tai häpeä tunnetta (Willison ym., 2018). Oleellisena erona Sykesin ja Matzan määritelmään Willison ym. määrittelevät neutralisaatiotekniikat vahvempina menetelminä. Heidän määritelmässään neutralisaatiotekniikoita hyödyntävät henkilöt voivat vapautua täysin moraalisista rajoitteista, kuten häpeästä, verrattuna Sykesin ja Matzan määritelmään, jossa häpeän tunnetta vain lievennetään tai tilapäisesti sivuutetaan.

Siponen ja Vance (2010) puolestaan määrittelevät omassa tutkimuksessaan neutralisaatiotekniikat järkeilynä, jonka avulla organisaatioiden työntekijät voivat minimoida heidän toiminnastaan johtuvien haitallisten seurausten määrää.

Siposen ja Vancen tutkimuksessa esitellyn määrittelyn pohjalta normien vastaiseen toimintaan syyllistyneet henkilöt, eivät ensisijaisesti vapauta itseään syyllisyyden tunteestaan, mutta he pystyvät rationalisaation avulla minimoimaan ja vähentämään mahdollisten sanktioiden vaikuttavuutta. Huomion arvoista tutkimuksen määrittelyssä ovat käytetyt sanavalinnat neutralisaatiotekniikoista. Siponen ja Vance käyttävät omassa määrittelyssään termiä rationalisaatio eivätkä, esimerkiksi, termejä oikeutus tai neutralisaatio.

Poiketen aiemmin mainituista määritelmistä neutralisaatiotekniikat voidaan myös nähdä yksilöä laajemmasta näkökulmasta. Muun muassa työyhteisöjen tietokoneen käyttöä tutkivat julkaisut määrittelevät neutralisaatiotekniikat menetelmiksi, joiden avulla työyhteisön jäsenet voivat perustella itselleen sekä muille työyhteisön jäsenille omaa yhtiön sääntöjen vastaista toimintaansa (Lim, 2002; Cheng, Li, Zhai & Smyth, 2014). Kyseinen määritelmä laajentaa neutralisaatiotekniikoiden vaikuttavuutta yksittäisten normeja rikkovien henkilöiden ulkopuolelle ja painottaa myös perustelujen vaikutusta ulkopuolisten henkilöiden suhtautumiseen rikkomusten osalta.

Yksittäisistä sanavalintojen sekä käsitteiden eroista huolimatta neutralisaatiotekniikat ymmärretään ja määritellään tutkijayhteisön keskuudessa melko yksimielisesti ja vakiintuneesti. Myös neutralisaatiotekniikoiden teoreettinen vaikutus esiintyy määritelmissä hyvin samankaltaisena, vaikkakin vaikutuksen laajuudessa sekä vaikutusalueessa esiintyy pientä hajontaa. Yleisen määritelmän sijaan merkittävämpi tutkijoita jakava piirre neutralisaatiotekniikoiden suhteen ovat yksittäiset tekniikat ja niiden sisältö. Neutralisaatiotekniikoiden kehittämisen jälkeen useat tutkimusartikkelit ovat esittäneet lisäyksiä ja muutoksia olemassa oleviin tekniikoihin (Maruna & Copes, 2005).

Seuraavaksi käsitellään tarkemmin yksittäisten neutralisaatiotekniikoiden määritelmiä sekä niiden keskeisiä ominaisuuksia.

2.3 Alkuperäiset neutralisaatiotekniikat

Neutralisaatiotekniikoita hyödyntävä tutkimuskirjallisuus nojautuu yhä tänäkin päivänä vahvasti Sykesin ja Matzan alkuperäisessä tutkimuksessa esiteltyyn teoreettiseen viitekehykseen. Tutkimuksessaan Sykes ja Matza tunnistavat ja esittelevät viisi yksittäistä tekniikkaa, jotka yhdessä muodostavat neutralisaatiotekniikoiden mallin (Sykes & Matza, 1957). Kyseiset tekniikat tunnetaan tiedeyhteisön keskuudessa nimellä ”famous five” ja ne ovat laajasti tiedeyhteisön tunnustamia sekä yleisimmin osana neutralisaatiotekniikoita hyödyntävää tutkimusta (Maruna & Copes, 2005).

Sykesin ja Matzan määrittelemät alkuperäiset neutralisaatiotekniikat ovat vastuun kieltäminen, vahingon kieltäminen, uhrin kiistäminen, tuomion tuomitseminen sekä vetoaminen korkeampiin velvollisuuksiin (Sykes & Matza, 1957). Vaikka alkuperäinen tutkimus ei esitä suoria empiirisiä havaintoja tai perusteluja yksittäisten tekniikoiden valintojen tai hyödyntämisen suhteen, ar-

gumentoivat Sykes ja Matza näiden tekniikoiden edustavan kriittistä osaa syistä sosiaalisten normien ohittamisen taustalla.

Alkuperäisten neutralisaatiotekniikoiden laajasta soveltamisesta huolimatta, tekniikat ovat kohdanneet myös kritiikkiä (Fritsche, 2005) ja niiden soveltamisessa on eroja eri tutkimusalojen välillä. Eroavuudet ilmenevät kuitenkin useimmiten yksittäisten tekniikoiden hylkäämisen tai vaihtamisen muodossa, minkä seurauksena alkuperäinen runko on edelleen vahvasti osana tutkimusten teoreettisena taustana. Sykesin ja Matzan esittelemän teorian kohtaamaa kritiikkiä ja siitä seurannutta kehitystä käsitellään tarkemmin tämän luvun viimeisessä alaluvussa.

Seuraavaksi käsitellään ja määritellään tarkemmin Sykesin ja Matzan esittelemät alkuperäiset neutralisaatiotekniikat. Alkuperäisten neutralisaatiotekniikoiden määrittelyn pohjalta tarkastellaan kappaleen lopussa tiiviisti myös muita tutkimuskirjallisuudessa esiteltyjä neutralisaatiotekniikoita sekä niiden piirteitä.

2.3.1 Vastuun kieltäminen

Ensimmäinen Sykesin ja Matzan esittelemä neutralisaatiotekniikka on vastuun kieltäminen (englanniksi denial of responsibility). Sykes ja Matza (1957) määrittelevät vastuun kieltämisen tekniikaksi, jossa rikolliseen toimintaan syyllistyneet henkilöt voivat esittää itsensä vapaaksi vastuusta hyödyntämällä jotakin vastuuta nostavaa seikkaa. Sykes ja Matza (1957) ulottavat omassa tutkimuksessaan tekniikan vaikuttavuuden pelkkää vahinkoa laajemmaksi ja korostavat, että vastuun kieltämistä voidaan soveltaa myös, esimerkiksi ulkoisista olosuhteista riippuviin tapahtumiin.

Myöhemmät neutralisaatiotekniikoita hyödyntävät tutkimukset tukeutuvat vahvasti Sykesin ja Matzan alkuperäiseen määritelmään ja määrittävät tekniikan melko vakiintuneesti. Esimerkiksi tutkijakaksikko Siponen ja Vance (2010) määrittelevät omassa tutkimuksessaan vastuun kieltämisen menetelmäksi, jossa rikkeeseen syyllistynyt henkilö voi kiistää oman syyllisyytensä, painottamalla ylitsepääsemättömiä ulkoisia tekijöitä. Kyseistä määritelmää hyödynnetään myös liike-elämän etiikan koskevassa tutkimuksessa, jossa kuluttajien tekemiä moraalisesti kyseenalaisia päätöksiä voidaan pyrkiä selittämään kuluttajista riippumattomilla tekijöillä (Chatzidakis, Hibbert & Smith, 2007).

2.3.2 Vahingon kieltäminen

Toisena neutralisaatiotekniikkana Sykes ja Matza (1957) esittelevät vahingon kieltämisen (englanniksi denial of injury), jossa teon neutralisoiminen keskittyy normien vastaisesta toiminnasta aiheutuvaan haittaan tai vahinkoon. Sykes ja Matza korostavat kyseisessä menetelmässä yhteiskunnan roolia ja sitä, miten osa rikoksista voidaan yhteiskunnan puolesta hyväksyä, mikäli seuraukset ovat mitättömiä. Tämän argumentin pohjalta Sykes ja Matza toteavat, että kyseinen toiminta voi antaa rikoksen tekijöille mahdollisuuden neutralisoida normien

vastaisen teon, mikäli he katsovat, että teosta ei synny suoraa vahinkoa (Sykes & Matza, 1957).

Vahingon kieltäminen on neutralisaatiotekniikka, jota hyödynnetään usein tietoturvatutkimuksissa. Tietoturvan tutkijat hyödyntävät monesti tekniikan määritelmässään Sykesin ja Matzan luomaa teoreettista pohjaa, mutta korostavat määritelmässään usein ensisijaisesti vahingon määrää, yhteiskunnan vaikutuksen sijaan. Barlow, Warkentin, Ormond sekä Dennis (2013) määrittelevät tekniikan menetelmäksi, jossa normien vastainen käytös voidaan rationalisoida, mikäli tapauksessa ei ole uhria tai kärsijää. Koska normien vastaisella toiminnalla ei ole suoraa uhria, voidaan teko toteuttaa ilman häpeän tai syyllisyyden tunnetta mahdollisista haitallisista seurauksista huolimatta (Barlow, Warkentin, Ormond & Dennis, 2013).

Vahingon kieltämisestä on esitetty myös pelkistetympiä sekä pehmeämpiä määritelmiä, esimerkiksi liike-elämän etiikan tutkimusten yhteydessä. Chatzidakis ym. (2007) määrittelevät vahingon kieltämisen menetelmäksi, jossa normien vastaista toimintaa ei voida pitää tuomittavana, jos kukaan ei suoraan kärsi toiminnasta. Samankaltaista määritelmää hyödyntävät myös De Bock ja Van Kenhove (2011), jotka määrittelevät tekniikan menetelmäksi, jossa yksilön tai organisaation toimintaa ei voida pitää tuomittavana, mikäli kukaan ei suoraan kärsi toiminnan seurauksena.

2.3.3 Uhrin kiistäminen

Uhrin kiistämisen (englanniksi denial of victim) määrittelyssä Sykes ja Matza (1957) poikkeavat aiemmin esitellyistä menetelmistä argumentoimalla, että kyseistä tekniikkaa hyödyntävät henkilöt usein tunnustavat oman tekonsa ja sen aiheuttamat seuraukset. Tästä huomatta teon haitallisia vaikutuksia voidaan neutralisoida perustelemalla, että kyseisestä teosta aiheutuneet seuraukset ovat uhrin näkökulmasta ansaittuja tai oikeutettuja ja täten myös itse tekoakin voidaan pitää oikeutettuna (Sykes & Matza, 1957). Sykes ja Matza esittävät omassa tutkimuksessaan myös, että uhrin kiistämisessä ei sinänsä tarvita varsinaista uhria, jonka syyksi teko voidaan vierittää. Sen sijaan he argumentoivat, että rikokseen syyllistyneet ja toiminnan tunnustavat henkilöt voivat pyrkiä neutralisoimaan tekonsa yksinkertaisesti toteamalla, että tekoa ei voida pitää rangaistavana ulkoisista olosuhteista johtuen (Sykes & Matza, 1957).

Kriminologian tutkimuksen ulkopuolella uhrin kiistäminen menetelmänä on hankalampi määritellä, koska uhrin määrittäminen ei ole aina yksiselitteistä (Silic, Barlow & Black, 2017). Esimerkiksi tietoturvatutkimuksen yhdessä varsinaisesta uhrista voi esiintyä erimielisyyksiä, mikäli teon uhrina on, esimerkiksi työntekijän oma työnantaja tai organisaatio. Vestman esittää omassa neutralisaatiotekniikoita käsittelevässä väitöskirjassaan, että esimerkiksi organisaation sisäisten rikkomusten seurauksena uhrina voidaan pitää vaihtelevasti joko yksittäistä työyhteisön jäsentä, kokonaista työyhteisön osastoa tai jopa koko organisaatiota (Vestman, 2020, s. 119–120).

On huomion arvoista mainita, että useat tietoturvaa sekä organisaatioiden tietoturvaa käsittelevät julkaisut eivät sisällä uhrin kiistämismenetelmää osana neutralisaatiotekniikoita hyödyntävää tutkimusta. Kyseinen menetelmä on monesti korvattu Sykesin ja Matzan alkuperäisten neutralisaatiotekniikoiden ulkopuolisella menetelmällä, joita käsitellään tämän luvun viimeisessä alaotsikossa.

Uhrin kiistämistä hyödyntävät tietoturvatutkimukset sekä tietokoneella tehtyjä rikkomuksia koskevat tutkimukset määrittelevät menetelmän usein siten, että rikkomuksen uhri ansaitsi aiheutuneet seuraamukset (Cheng ym., 2014). Kyseisessä määritelmässä lähtökohtana on, että menetelmää hyödynnettäessä on olemassa kohde, jonka syyksi teko voidaan neutralisoitaessa vierittää, eikä tässä määritelmässä tukeuduta Sykesin ja Matzan esittämään mahdollisuuteen hyödyntää pelkkiä olosuhteita osana neutralisaatiota.

2.3.4 Tuomion tuomitseminen

Neljäntenä Sykesin ja Matzan esittelemänä neutralisaatiotekniikkana toimii tuomion tuomitseminen (englanniksi condemnation of the condemners), joka määritellään heidän alkuperäisessä tutkimuksessaan menetelmäksi, jossa rikkomuksen tehneet henkilöt kyseenalaistavat tekojen tuomitsijan tai tuomitsijat (Sykes & Matza, 1957). Kyseistä tekniikkaa hyödyntävät henkilöt pyrkivät, siten siirtämään ja torjumaan huomion pois omasta toiminnastaan kyseenalaistamalla tuomitsijoiden taustalla olevien henkilöiden omia henkilökohtaisia motiiveja tai vetoamalla tuomitsijoiden omaan toimintaan (Sykes & Matza, 1957).

Tietoturvaa ja tietokoneiden väärinkäyttöä tutkiva kirjallisuus määrittelee tuomion tuomitsemisen vahvasti pohjautuen Sykesin ja Matzan määritelmään. Esimerkiksi tutkijat Siponen ja Vance (2010) määrittelevät menetelmän omassa tutkimuksessaan tekniikaksi, jolla henkilö voi neutralisoida oman toimintansa kohdentamalla syyn rikkomuksen kohteeseen. Kyseisessä määritelmässä korostuu ajatus siitä, että kohteen ei välttämättä tarvitse olla ihminen tai viranedustaja, kuten esimerkiksi poliisi, vaan tuomitsemisen kohteena voi olla esimerkiksi epäreiluksi koettu laki tai ohjeistus (Siponen & Vance, 2010).

Tuomion tuomitsemiseen tutkimuskirjallisuus esittelee myös edellä mainittuja suppeampia määritelmiä, joissa ei esimerkiksi oteta kantaa menetelmän soveltamisen kohteisiin. Cheng ym. (2014) määritelmän mukaan tuomion tuomitseminen on menetelmä, jonka avulla rikkomukseen syyllistynyt henkilö pyrkii siirtämään syyn itseltään kritisoimalla tuomitsijoita. Silic ym. (2017) puolestaan määrittelevät tekniikan yksinkertaisesti menetelmäksi, jonka avulla syyllisyys neutralisoidaan siirtämällä syy tuomitsijaan.

Verrattuna aikaisempiin määritelmiin liike-elämän eettisyyttä tutkivat sekä neutralisaatiotekniikoita hyödyntävät tutkimukset tarjoavat myös oman näkemyksensä tekniikan määrittelyyn. Alan tutkimukset painottavat omassa määritelmässään teon neutralisoimista vastuun väistämisellä, mutta määritelmät hyödyntävät myös tuomitsijan roolia osana neutralisaatiota. Tutkijat De Bock sekä Van Kenhove (2011) määrittelevät omassa tutkimuksessaan tuomion tuo-

mitsemisen tekniikaksi, jolla syyllisyys voidaan välttää korostamalla tuomitsijoiden samankaltaista paheksuttavaa toimintaa. Samankaltaista määritelmää hyödyntävät myös Chatzidakis ym. (2007), jotka määrittelevät tuomion tuomitsemisen menetelmäksi välttää väärintoimisen syytökset osoittamalla tuomitsijoiden syyllistyvän paheksuttavaan toimintaan.

2.3.5 Vetoaminen korkeampiin velvollisuuksiin

Viimeisenä Sykesin ja Matzan määrittelemänä neutralisaatiotekniikkana on vetoaminen korkeampiin velvollisuuksiin (englanniksi appeal to higher loyalties). Sykes ja Matza (1957) määrittelevät omassa tutkimuksessaan tekniikan dilemmana, jossa rikoksen tekijän joutuu valitsemaan toiminnassaan ristiriitaisten normien väliltä säännöt tai lait, joita seurata. Ristiriitaisten normien seurauksena rikkomukseen syyllistyvä henkilö voi tietoisesti joutua rikkomaan odotuksia tai sääntöjä, joita hän muuten kunnioittaa, mutta jotka ovat samalla ristiriidassa toisten korkeammalle priorisoitujen sääntöjen kanssa (Sykes & Matza, 1957).

Maruna ja Copes (2005) hyödyntävät omassa määritelmässään Sykesin ja Matzan alkuperäistä määritelmää, mutta tarkentavat omassa tutkimuksessaan määritelmän yksityiskohtia. Tutkimuksessaan Maruna ja Copes (2005) määrittelevät tekniikan menetelmäksi, jolla rikkomuksen tehneet voivat neutralisoida oman toimintansa korostamalla, että heidän toimintansa on linjassa jokin yksittäisen ja spesifin ryhmän asettaman normiston kanssa. Oleellisena lisähuomiona on, että Marunan ja Copesin määritelmässä todetaan henkilön olevan kyseisen ryhmän jäsen eikä esimerkiksi ulkopuolinen ryhmän kannattaja (Maruna & Copes, 2005).

Kriminologian ulkopuolella vetoaminen korkeampiin velvollisuuksiin määritellään jokseenkin alkuperäisestä määritelmästä poikkeavaksi. Esimerkiksi Cheng ym. (2014) määrittelevät tekniikan menetelmäksi, jolla rikkomuksen tehnyt henkilö voi oikeuttaa tekonsa esittämällä teon hyötyjen ylittävän teon haitat pidemmällä aikavälillä. Tutkijat Siponen ja Vance (2010) puolestaan määrittelevät omassa tutkimuksessa tekniikan menetelmäksi, jossa ristiriitaiseen tilanteeseen joutuneen henkilön täytyy rikkoa ohjeistuksia tai sääntöjä selvitäkseen tilanteesta.

Liike-elämän etiikan tutkimukset tarjoavat myös oman näkemyksen tekniikan määritelmään korostamalla määritelmässään kuluttajien kokemia ihanteita ja arvoja. Esimerkiksi kuluttajien käyttäytymistä tutkiva kirjallisuus esittelee määritelmän, jossa tekniikka esitellään menetelmänä, jonka avulla kyseenalaisilla kuluttajatottumuksilla operoivat voivat perustella käyttäytymistään siten, että heidän tavoitteenaan on toteuttaa korkeamman tason ideologiaa tai tavoitteita (Chatzidakis ym., 2007; De Bock & Van Kenhove, 2011).

2.4 Muita neutralisaatiotekniikoita

Vaikka Sykesin ja Matzan esittelemät viisi neutralisaatiotekniikkaa ovat laajasti hyödynnettyjä osana monien eri tutkimusalojen kirjallisuutta, ovat kyseiset tekniikat saaneet osakseen myös kritiikkiä. Immo Fritsche (2005) esittää omassa tutkimusartikkelissaan neutralisaatiotekniikoiden taustaparametrien olevan monissa tutkimuksissa itsestäänselvyytenä otettuina. Tämän lisäksi hän kritisoi myös Sykesin ja Matzan esittelemiä tekniikoiden listaa mielivaltaiseksi sekä puutteelliseksi valittujen tekniikoiden suhteen (Fritsche, 2005). Alkuperäiset neutralisaatiotekniikat ovat myös saaneet kritiikkiä tekniikoiden päällekkäisyyksistä, minkä on katsottu aiheuttavan vääristymiä sekä haasteita tutkimuksissa saavutettuihin tutkimustuloksiin (Maruna & Copes, 2005).

Esitetyn kritiikin sekä jatkuvan kehityksen seurauksena useat tutkijat ovat määrittäneet omia ratkaisu- sekä parannusehdotuksia paikkaamaan Sykesin ja Matzan kehittämän teorian puutteita. Kehitystyön seurauksena monet tutkijat ovat myös tuottaneet täysin uusi tekniikoita, joita hyödynnetään vaihtelevasti neutralisaatiotekniikoiden tutkimuksen yhteydessä (Maruna & Copes, 2005). Tekniikoiden hyödyntämisen ohella myös uusien neutralisaatiotekniikoiden tunnustaminen vaihtelee tutkijayhteisön keskuudessa. Esimerkiksi Willison ja Warkentin (2013) esittelevät vuonna 2013 julkaistussa tutkimuksessaan 17 neutralisaatiotekniikkaa. Laajemman käsityksen neutralisaatiotekniikoista tarjoavat tutkijat Kaptein ja Van Helvoort, jotka pyrkivät tuottamaan kattavamman mallin neutralisaatiotekniikoista. Heidän mallissaan neutralisaatiotekniikat ovat jaettu 12 päätekniikkaan, jotka jakautuvat alimmalla tasolla 60 alatekniikaksi (Kaptein & Van Helvoort, 2019).

Koska neutralisaatiotekniikoiden määrästä ei ole tiedeyhteisön keskuudessa selvää yhteisymmärrystä ja koska kirjallisuudessa esiintyvien neutralisaatiotekniikoiden määrä on merkittävä, ei ole tutkielman kannalta tarkoituksenmukaista määritellä jokaista tekniikkaa erikseen. Tästä johtuen tutkielmassa tullaan määrittelemään vain tutkielman kannalta oleellisimmat tekniikat, jotka esiintyvät erityisesti tietoturvaa koskevassa tutkimuksessa.

Vetoaminen tilien pysymiseen tasapainossa (englanniksi metaphor of the ledger) on Klockarsin vuonna 1974 esittämä neutralisaatiotekniikka, jonka mukaan rikkomukseen syyllistynyt henkilö voi pyrkiä oikeuttamaan tekonsa ylläpitämällä kirjaa omista hyvistä ja huonoista teoistaan. Tekniikan keskeisenä ajatuksena on, että yksittäiset rikkomukset tai ohjeiden vastaiset teot voidaan oikeuttaa tai ovat jopa hyväksyttäviä, mikäli tekoon syyllistyneellä henkilöllä on riittävästi tekoa edeltäviä hyviä tekoja.

Tuoreemmat tekniikkaa hyödyntävät tutkimukset korostavat menetelmän määrittelyn yhteydessä oikeaoppisesta toiminnasta aiheutunutta ”ylijäämää”, eivätkä varsinaisesti tilien tasaamista. Esimerkiksi Lim (2002) esittää omassa tutkimuksessaan, että tekniikkaa hyödyntävät henkilöt kerryttävät oikeaoppisten tekojen seurauksena positiivista pääomaa, joita he ovat oikeutettuja hyödyntämään normien vastaisiin tekoihin. Samankaltaista määritelmää hyödyn-

tävät myös Siponen ja Vance, jotka omassa tutkimuksessaan määrittelevät tekniikan menetelmäksi, jonka avulla normien vastainen toiminta voidaan oikeuttaa, mikäli henkilöllä on varaa toteuttaa teko kertyneen ylijäämän avulla (Siponen & Vance, 2010).

Vetoaminen toimimiseen pakon edessä (englanniksi defence of necessity) on Minorin vuonna 1981 esittelemä neutralisaatiotekniikka, jonka mukaan tekniikkaa hyödyntävät henkilöt voivat toteuttaa normien vastaisen teon ilman häpeän tunnetta tai muita sosiaalisia haittoja, mikäli teko voidaan katsoa välttämättömäksi (Minor, 1981). Minorin hyödyntämässä määritelmässä esiintyy ajatus olosuhteiden mielletystä pakottavuudesta, mikä laajentaa tekniikan sovellusaluetta. Käytännön tasolla kyseinen määritelmä mahdollistaa tekniikan hyödyntämisen, esimerkiksi kyseenalaisten yrityskäytäntöjen neutralisoimisessa, vaikka yritysten välisestä kilpailusta johtuvat olosuhteet eivät sinänsä tarjoaisi yhtä ainutta pakottavaa mahdollisuutta (Minor, 1981).

Tietoturvatutkimuksen yhteydessä vetoaminen toimimiseen pakon edessä määritellään usein myös absoluuttisen välttämättömyyden kautta. Siponen ja Vance (2010) määrittelevät tekniikan menetelmänä, jota hyödyntävät henkilöt uskovat toimintansa olevan välttämätöntä ja olosuhteista johtuen jopa ainut mahdollinen vaihtoehto. Samankaltainen, mutta suppeampi määritelmä löytyy myös Barlow ym. tutkimuksesta, jossa tekniikka määritellään menetelmäksi, jolla teko voidaan perustella esittämällä tehty teko ainoaksi vaihtoehdoksi ulkoisista olosuhteista johtuen (Barlow, Warkentin, Ormond & Dennis, 2018).

3 NEUTRALISAATIOTEKNIIKOITA HYÖDYNTÄVÄT TUTKIMUKSET

Tässä pääluvussa esitellään ja tarkastellaan organisaatioiden tietoturvaa käsitteleviä tutkimuksia, jotka hyödyntävät neutralisaatiotekniikoita osana tutkimusta. Luvun tavoitteena on tuottaa kattava käsitys siitä, miten neutralisaatiotekniikoita on sovellettu käytännössä osana organisaatioiden tietoturvatutkimusta. Tämän lisäksi luku pyrkii myös vastaamaan siihen, minkälaisia tuloksia tutkimukset ovat saavuttaneet neutralisaatiotekniikoiden suhteen sekä tulosten pohjalta johdettuja päätelmiä. Selkeyden ja luettavuuden osalta luvussa käsiteltävät tutkimukset on pyritty ryhmittelemään tutkimuksessa tunnistettuihin aihepiireihin ja sitä kautta neljään alalukuun.

3.1 Neutralisaatiotekniikat tietoturvarikkomusten ennustajana

Organisaatioiden sekä tutkimuskirjallisuuden tarve ymmärtää tietoturvaohjeistuksen vastaiseen käytökseen vaikuttavia tekijöitä on johtanut monien teorioiden esittämiseen, jotka pyrkivät ennustamaan sekä vaikuttamaan yksilöiden tietoturvakäyttäytymiseen. Yksi keskeisimmistä ja laajimmin sovellutuista malleista tietoturvakäyttäytymisen selittämiseen on peloteteoria, joka ennustaa ihmisten toimivan rationaalisesti punniten tekojensa mahdollisia seurauksia sekä niiden todennäköisyyttä suhteessa teosta koituviin hyötyihin. Tätä näkemystä vastaan on kuitenkin viimeisen reilun vuosikymmenen aikana syntynyt uusi koulukunta, joka haastaa kirjallisuudessa vallitsevaa käsitystä peloteteorian toimivuudesta tietoturvarikkomusten ennustajana.

Merkittävänä organisaatioiden tietoturvaa neutralisaatiotekniikoiden avulla tarkastelevana tutkimuksena toimii Siposen ja Vancen vuonna 2010 ilmestynyt tutkimus, koskien syitä organisaatioiden työntekijöiden tietoturvaohjeistusten vastaiseen toimintaan. Tutkimuksessaan Siponen ja Vance hyödyntävät kuutta neutralisaatiotekniikka sekä perinteisempiä tekijöitä, kuten virallisia sanktioita, epävirallisia sanktioita sekä häpeää ja pyrkivät ymmärtämään, mitkä

kyseisistä tekijöistä ennustavat työntekijöiden aikomuksia rikkoa organisaatioidensa tietoturvaohjeistuksia. Tutkimusaineiston osalta tutkimus hyödyntää skenaariomallinnusta aineiston keräämiseen ja tutkimuksessa osallisena on reilut 1400 ihmistä kolmesta eri suomalaisesta yrityksestä.

Siposen ja Vancen (2010) tutkimuksen tulokset osoittavat neutralisaatiotekniikoiden olevan merkittävässä roolissa työntekijöiden tietoturvakäyttäytymisen suhteen sekä niiden ansaitsevan tarkempaa huomioimista jatkotutkimuksen osalta. Tutkimuksen tulokset tukevat hypoteesia, joka ennustaa neutralisaatiotekniikoiden lisäävän työntekijöiden aikomuksia ja taipumusta rikkoa organisaatioidensa tietoturvaohjeistusta (Siponen & Vance, 2010). Lisäksi Siposen ja Vancen tuottamat tulokset eivät löydä tukea sanktioiden tai häpeän negatiiviselle vaikutukselle työntekijöiden taipumukseen rikkoa tietoturvaohjeistuksia.

Siposen ja Vancen ohella myös muut tutkijaryhmät ovat hyödyntäneet samankaltaista tutkimusasetelmaa tutkiakseen työntekijöiden aikomuksia työpaikan tietokoneiden väärinkäyttöön. Willison ym. (2018) tutkivat omassa julkaisussaan tekijöitä, jotka vaikuttavat organisaatioiden työntekijöiden aikomukseen käyttää työkoneitaan ohjeistuksen vastaisesti. Tutkimus hyödyntää mallia, joka sisältää ominaisuuksia peloteteoriasta, neutralisaatiotekniikoita sekä osia organisaatioiden oikeudenmukaisuudesta teoriasta. Mallin tavoitteena on ymmärtää eri teorioiden keskinäisiä suhteita sekä niiden vaikutuksia työntekijöiden aikomuksiin rikkoa organisaatioiden tietoturvaohjeistuksia (Willison ym., 2018).

Willison ym. (2018) tutkimuksen tulokset löytävät yhteyden proseduraalisen oikeudenmukaisuuden sekä neutralisaatiotekniikoiden välillä, mikä tutkijoiden mukaan viittaa siihen, että organisaatioiden työntekijät ovat valmiimpia hyödyntämään neutralisaatiotekniikoita, mikäli he kokevat joutuneensa epäoikeudenmukaisten menettelytapojen uhriksi. Huomion arvoista tutkimuksen tuloksissa on myös, että kaikki tutkimuksessa sovelletut neutralisaatiotekniikat eivät tuottaneet kyseistä yhteyttä. Sovelletuista neutralisaatiotekniikoista vain uhrin kiistäminen ja vetoaminen tilien pysymiseen tasapainossa näyttivät olevan yhteydessä proseduraaliseen oikeudenmukaisuuteen (Willison ym., 2018).

Neutralisaatiotekniikoiden ja proseduraalisen oikeudenmukaisuuden keskinäisen yhteyden lisäksi Willison ym. (2018) tulokset löytävät tukea myös argumentille, joka ennustaa neutralisaatiotekniikoiden hyödyntämisellä olevan positiivinen vaikutus työntekijöiden aikomuksiin toimia tietoturvaoheistusten vastaisesti. Näiden tulosten perusteella tutkijat toteavat, että organisaatiot voivat vaikuttaa työntekijöidensä tietoturvakäyttäytymiseen varmistamalla organisaatioiden toimintatapojen oikeudenmukaisuuden. Mikäli työntekijät kokevat organisaatioiden toimintatapojen olevan oikeudenmukaisia he ovat vähemmän alttiita hyödyntämään neutralisaatiotekniikoita ja täten myös vähemmän alttiita rikkomaan tietoturvaohjeistuksia (Willison ym., 2018).

Tuoreimmassa aihepiirin tutkimuksessa tutkijat Simola, Virtanen sekä Santonen (2020) käsittelevät neutralisaatiotekniikoita sekä persoonallisuuspiirteitä, jotka ennakoivat neutralisaatiotekniikoiden käyttöä. Tämän lisäksi tutki-

mus tarkastelee myös vajaan 150 suomalaisen kadetin näkemyksiä tietoturvasta sekä mahdollisesta neutralisaatiotekniikoiden hyödyntämisestä. Tutkimuksen tavoitteena on tuottaa aikaisempaa laajempaa ymmärrystä koskien yksittäisten neutralisaatiotekniikoiden ja persoonallisuuspiirteiden välisistä suhteista sekä myös näiden roolista tietoturvarikkomusten taustalla.

Simolan ym. (2020) tutkimus tarjoaa tulostensa osalta tärkeitä sekä myös jossain määrin positiivisia tuloksia koskien organisaatioiden tietoturvaa. Tulosten osalta suurin osa vastaajista asennoitui negatiivisesti tutkimuksen skenaarioissa esiteltyihin mahdollisuuksiin hyödyntää neutralisaatiota. Kyseisen tuloksen perusteella voidaankin todeta, että tietoturvaa pidetään korkeassa arvossa armeijan kontekstissa (Simola ym., 2020). Tietoturvaan liittyvän asennoitumisten ohella, tutkimus tuotti myös tukea aiemmille tutkimuksille, jotka ennustavat yksittäisten personallisuuspiirteiden lisäävän tietoturvarikkeiden riskiä yleisemmällä tasolla.

Yleisen tietoturvan lisäksi tutkijat Simola ym. (2020) löytävät myös tukea hypoteesille, joka ennustaa persoonallisuuden piirteiden vaikuttavat yksittäisten neutralisaatiotekniikoiden valitsemiseen ja hyödyntämiseen. Tutkimukseen valittujen neutralisaatiotekniikoiden osalta yleisimmät neutralisaatiotekniikoiden käyttöä ennakoivat persoonallisuuden piirteet olivat korkea neuroottisuus, korkea machiavellismi sekä matala tunnollisuus (Simola ym., 2020). Kyseiset piirteet toistuvat käytännössä jokaisen mitatun neutralisaatiotekniikan yhteydessä. Poikkeuksia ennustavien persoonallisuuden piirteiden osalta tarjosivat vastuun kieltäminen sekä vetoaminen tilien pysymiseen tasapainossa. Vetoamiseen tilien pysymiseen tasapainossa vaikutti yleisimpien piirteiden ohella myös matala avoimuus ja vastuun kieltämisessä matala avoimuus sekä matala ekstroversio (Simola ym., 2020).

3.2 Neutralisaatiotekniikat organisaatioiden viestintää koskevassa tutkimuksessa

Toisena tutkimuskirjallisuudessa esiintyvänä aihepiirinä on neutralisaatiotekniikoiden hyödyntäminen osana tietoturvaan liittyvää viestintää sekä tietoturvatietoisuutta. Tutkimusten tavoitteena on tarkastella kohdennetusta ja tietoisesta viestinnästä saavutettavia tuloksia tietoturvan suhteen sekä ottaa kantaa voidaanko taipumusta neutralisaatiotekniikoiden käyttöön ehkäistä viestinnän keinoin. Tämän katsauksen osalta vain yksi tutkijaryhmä käsitteli tutkimuksissaan kyseistä aihepiiriä ja esiteltävät tutkimukset ovat osittain jatkumoa toisilleen.

Ensimmäisen tutkimuksen osalta tarkoituksena oli tarkastella organisaatioiden tietoturvaviestinnässä käsiteltäviä painopisteitä sekä määritellä voidaanko neutralisaatiotekniikoita painottavalla viestinnällä vaikuttaa työntekijöiden aikomuksiin rikkoa organisaatioidensa tietoturvaohjeistuksia. Barlow ym. (2013) tutkimuksen yhteydessä selviää, että merkittävänä teemana tietoturvaa

koskevassa viestinnässä on pelotteiden hyödyntäminen, eli virallisten sekä epävirallisten sanktioiden korostaminen tietoturvatietoisuuden lisäämisen yhteydessä. Tätä näkemystä haastamaan Barlow ym. (2013) esittävätkin hypoteesissaan, että neutralisaatiotekniikat lisäävät työntekijöiden aikomuksia rikkoa tietoturvaohjeistuksia sekä, että neutralisaatiotekniikoita vastaan räätälöidyllä viestinnällä voidaan vähentää aikomuksia toimia ohjeistusten vastaisesti yhtä tehokkaasti, kuin nykyisen sanktiopohjaisen viestinnän avulla.

Barlow ym. (2013) tutkimuksen tulosten perusteella hypoteeseille saadaan tukea vaihtelevasti. Tutkittujen neutralisaatiotekniikoiden perusteella vain vetoaminen toimimiseen pakon edessä näytti lisäävän työntekijöiden aikomusta tietoturvaohjeistusten rikkomiseen. Vaikka tutkimuksen tulokset eivät löydä muiden neutralisaatiotekniikoiden suhteen näyttöä aikeiden lisäämisestä, tuottaa tulos toisaalta tukea muussa kirjallisuudessa esiintyville hypoteeseille neutralisaatiotekniikoiden spesifeistä soveltuvuuksista ja sovelluskohteista. Sen sijaan tutkijat löytävät tukea hypoteesille, jonka mukaan aikeita tietoturvaohjeistusten rikkomiseen voidaan vähentää neutralisaatiotekniikoiden torjumiseen räätälöidyn viestinnän avulla. Myös hypoteesi, joka ennustaa neutralisaatiotekniikoiden heikentämiseen suunnatun viestinnän olevan yhtä tehokasta tietoturvarikkomusten vähentämiseen saa tukea aineiston perusteella (Barlow ym., 2013). Tutkimuksen tulokset tuottavat tukea aikaisemmalle tutkimuskirjallisuudessa esiintyvälle näkemykselle neutralisaatiotekniikoiden tärkeästä roolista osana organisaatioiden tietoturvaa sekä tarjoavat tukea näkemykselle, jonka mukaan viestinnän tulisi myös pyrkiä torjumaan neutralisaatiotekniikoiden käyttöä työntekijöiden keskuudessa.

Aikaisemman tutkimuksen pohjalta kyseiset tutkijat Barlow ym. ovat tuottaneet myös tuoreempaa tutkimusta spesifien viestinnän keinojen vaikutuksista osana organisaatioiden hyödyntämää tietoturvan koulutusta, harjoittelua sekä tietoisuuden ylläpitoa. Barlow ym. (2018) pyrkivät tutkimuksessaan tutkimaan voidaanko informatiivisen, normatiivisen tai antineutralisaatio pohjaisen viestinnän avulla vähentää työntekijöiden aikomuksia toteuttaa tietoturvarikkomuksia. Tämän ohella tutkijat pyrkivät myös tutkimuksensa yhteydessä tuottamaan tukea hypoteesille, jonka mukaan neutralisaatiotekniikat yleisellä tasolla lisäävät työtekijöiden aikomuksia rikkoa tietoturvaohjeistusta.

Tulosten osalta Barlow ym. (2018) tutkimus tarjoaa uutta tietoa erityisesti koskien neutralisaatiotekniikoiden torjumista tietoturvakoulutuksen avulla sekä samalla vahvistaa myös kirjallisuudessa vallitsevaa käsitystä neutralisaatiotekniikoiden tietoturvarikkeitä lisäävästä vaikutuksesta. Tutkimus löytää tukea hypoteesille, jonka mukaan neutralisaatiotekniikoiden käyttö lisää todennäköisyyttä tietoturvarikkomuksille (Barlow ym., 2018). Tulos on linjassaan alan tutkimuskirjallisuuden kanssa ja tuottaa ensisijaisesti lisätukea hypoteesille.

Varsinaisen viestinnän osalta Barlow ym. (2018) tulokset löytyvät tukea hypoteeseille, joiden mukaan informatiivisen viestinnän sekä antineutralisaatioon tähtäävän viestinnän avulla voidaan vähentää työntekijöiden aikomusta rikkoa tietoturvaohjeistusta. Menetelmien välillä on kuitenkin havaittavissa eroavaisuuksia ja tulosten perusteella antineutralisaatioon tähtäävän viestinnän

avulla saavutettavat tulokset ovat vahvempia kuin informatiivisen viestinnän avulla saavutetut tulokset. Informatiivisen viestinnän tehokkuuden suhteen toisena merkittävänä tekijänä olivat tutkimuksen skenaarioissa esiintyvät mahdollisuudet hyödyntää neutralisaatiota. Tulosten perusteella, mikäli tilaisuus hyödyntää neutralisaatiotekniikoita on vahvasti läsnä menettävät informatiivisen viestinnän keinot tehokkuutensa aikeiden heikentämisessä (Barlow ym., 2018).

3.3 Neutralisaatiotekniikat osana muita malleja

Organisaatioiden tietoturvaa käsittelevä tutkimuskirjallisuus tunnistaa tietoturvan monet ulottuvuudet, minkä seurauksena useat tutkimukset eivät pyri hyödyntämään vain yhtä yksittäistä mallia tai työkalua. Kyseinen näkemys on esillä myös neutralisaatiotekniikoita hyödyntävässä tutkimuskirjallisuudessa, jossa neutralisaatiotekniikoita on pyritty integroimaan osaksi jo olemassa oleviin malleihin tai tuottamaan uusia malleja, jotka sisältävät osia eri teoreettisista viitekehyksistä. Julkaisujen suhteen esiintyy vaihtelua tutkimusten tavoitteiden sekä tieteellisten kontribuutioiden suhteen. Osa malleja tuottavista tutkimuksista toimii puhtaasti teoreettisina julkaisuina, mutta valtaosa malleista ovat myös empiirisesti testattuja.

Puhtaasti teoreettisena panoksena neutralisaatiotekniikoiden suhteen esiintyy Willisonin ja Warketinin (2013) julkaisema tutkimus, joka pyrkii ymmärtämään aiempaa laajemmasta näkökulmasta syitä työntekijöiden tietoturvarikkomusten taustalla. Tutkijakaksikko pyrkii tarkastelemaan syitä erityisesti rikkomusten alkuvaiheessa eli tarkemmin sanottuna menetelmiä, jotka vaikuttavat varsinaisen aikomuksen syntyyn. Itse tutkimusartikkeli hyödyntää aikaisempaa vahvasti peloteteoriaan nojaavaa Straub-Welke Security Action Cycle:ä ja pyrkii laajentamaan tätä mallia integroimalla neutralisaatiotekniikat osaksi mallia (Willison & Warketin, 2013).

Laajennetun mallin määrittämisen ja esittelyn jälkeen tutkijat Willison ja Warketin (2013) eivät suorita tutkimuksen yhteydessä empiiristä testausta mallille, mutta he tarjoavat näkemyksensä tärkeimmistä mallia koskevista tulevaisuuden tutkimuskysymyksistä. Tutkimuksessa esiin nousee tarve tarkemmin rajatulle tiedolle neutralisaatiotekniikoiden soveltuvuuksista yksittäisten rikkomusten suhteen sekä yleisemmällä tasolla tarve löytää tukea hypoteesille, jonka mukaan neutralisaatiotekniikat ennakoivat työntekijöiden tekemiä rikkomuksia (Willison & Warkentin, 2013).

Tuoreempana mallina tutkimuskirjallisuudessa esiintyy Vancen, Siposen ja Straub:n (2020) neliulotteinen malli, joka hyödyntää sanktioita, häpeää, moraalisia uskomuksia sekä neutralisaatiotekniikoita ja pyrkii tutkimaan kulttuurillisten erojen vaikutusta tietoturvakäyttäytymiseen. Tutkimuksen tavoitteena on tuottaa aikaisempaa kattavampaa tietoa kulttuurillisten erojen vaikutuksista yksittäisiin tietoturvan työkaluihin sekä tuottaa aikaisempaan tutkimuskirjalli-

suuteen verrattuna merkittävästi laajempi kokonaisuus tutkimukseen osallistuneiden kansalaisuuksien ja maiden osalta.

Analysoidun aineiston pohjalta Vance ym. (2020) tutkimus löytää tukea hypoteesille, joka ennustaa neutralisaatiotekniikoiden olevan merkittävä ennustaja tietoturvarikkeiden todennäköisyydelle kulttuurillisista tekijöistä riippumatta. Neutralisaatiotekniikoiden ohella tulokset antavat myös tukea hypoteeseille, jotka ennustavat häpeän sekä moraalisten uskomusten vaikuttavan negatiivisesti aikomuksiin rikkoa tietoturvaohjeistuksia kulttuureista riippumatta. Kyseisten tulosten perusteella näyttäisi, siltä että kulttuurilliset tekijät eivät itsessään selitä tai vaikuta työntekijöiden kokemaan häpeään, moraalisiin uskomuksiin tai aikomuksiin hyödyntää neutralisaatiotekniikoita (Vance ym., 2020).

Kulttuurillisten tekijöiden ohella neutralisaatiotekniikoita on pyritty integroimaan osaksi mallia, joka pyrkii työympäristön, uskomusten sekä neutralisaatiotekniikoiden avulla arviomaan syitä tietoturvarikkomusten taustalla. Gwebu, Wang ja Yu (2020) esittelevät omassa tutkimuksessaan kyseisen mallin, jonka avulla he pyrkivät arvioimaan organisaatioiden sisäisten tekijöiden ja arvojen vaikutuksia neutralisaatiotekniikoiden hyödyntämisen todennäköisyyteen sekä työntekijöiden omiin henkilökohtaisiin uskomuksiin.

Gwebu ym. (2020) tutkimuksen tulosten perusteella voidaan todeta organisaatioissa korostetuilla arvoilla olevan vaikutusta neutralisaatiotekniikoiden hyödyntämiseen ja sitä kautta myös aikomuksiin poiketa tietoturvaohjeistuksesta. Tutkijat esittävät hypoteesissaan, että organisaatiot, jotka kannustavat työntekijöitään toimimaan maksimaalisen oman etunsa mukaisesti tai toimimaan maksimaalisen yhteisön edun mukaisesti lisäävät, neutralisaatiotekniikoiden käyttöä työntekijöidensä keskuudessa. Vastaavasti organisaatiot, jotka pyrkivät organisaation arvojen mukaisesti korostamaan sääntöjä sekä ohjeistuksia muiden arvojen sijaan, vähentävät neutralisaatiotekniikoiden käyttöä ja täten vähentävät myös työntekijöidensä aikomuksia poiketa tietoturvaohjeistuksista (Gwebu ym., 2020).

Tutkimus löytää myös tukea itsenäiselle hypoteesille, joka ennustaa neutralisaatiotekniikoiden lisäävän työntekijöiden aikomuksia rikkoa tietoturvaa koskevaa ohjeistusta (Gwebu ym., 2020). Kyseinen havainto on linjassaan tutkimuskirjallisuudessa vallitsevan käsityksen kanssa ja tuottaa ensisijaisesti tukea argumentille, joka esittää neutralisaatiotekniikoiden olevan oleellinen tekijä tietoturvarikkomusten taustalla.

Neutralisaatiotekniikoita hyödyntäviä malleja on myös pyritty hyödyntämään yksityiskohtaisemmassa kontekstissa, kuten työpaikan tietokoneiden väärinkäytössä. Kyseinen väärinkäyttö voi ilmetä, esimerkiksi työhön liittymättömänä Internetin selailuna, työpaikan ulkopuolisten sähköpostien lähettämisenä, haitallisten tiedostojen ja ohjelmien lataamisena tai pahimmillaan verkkorikollisuuden harrastamisena (Cheng ym., 2014). Ilmiön ymmärtämistä varten tutkijat ovat tuottaneet eri tekijöitä hyödyntäviä malleja, joista ensimmäinen hyödyntää oikeudenmukaisuusteoriaa organisaation kontekstissa sekä yksittäistä neutralisaatiotekniikkaa.

Vuonna 2002 julkaistussa tutkimuksessaan Lim pyrkii tuottamaan tutkittua tietoa sekä ymmärtämään selittäviä tekijöitä työntekijöiden harrastaman tietokoneiden väärinkäytön taustalla. Tutkimuksessa kehitetty malli hyödyntää neutralisaatiotekniikoista vetoamista tilien pysymiseen tasapainossa ja pyrkii tarkastelemaan vaikuttavatko organisaation oikeudenmukaisuusteorian osat menettelytapojen, vuorovaikutussuhteiden sekä jakava oikeudenmukaisuus aikomukseen hyödyntää kyseistä tekniikkaa (Lim, 2002). Edellä mainitun lisäksi tutkimus tuottaa empiiristä tietoa myös siitä, voidaanko vetoamista tilien pysymiseen tasapainossa pitää hyvänä ennustajana työntekijöiden aikomukselle väärinkäyttää työtietokoneita.

Lim (2002) tutkimuksen aineiston pohjalta saavutetut tulokset tukevat tutkimuksen alussa esitettyä hypoteesia, jonka mukaan vetoamista tilien pysymiseen tasapainossa hyödyntävät työntekijät ovat alttiimpia työpaikan tietokoneiden väärinkäytölle. Hypoteesin tukemisen ohella tulos on merkittävä myös siksi, että tulos antaa tietoa yksittäisen neutralisaatiotekniikan toimivuudesta tarkasti rajatun rikkomuksen yhteydessä. Tutkimuksen tulokset vahvistavat myös hypoteesit, jotka ennakoivat oikeudenmukaisuusteorian tekijöiden vaikuttavan todennäköisyyteen hyödyntää vetoamista tilien pysymiseen tasapainossa (Lim, 2002). Saavutettujen tulosten valossa vaikuttaisikin siltä, että oikeudenmukaisella organisaation sisäisellä toiminnalla voidaan vähentää työntekijöiden taipumusta hyödyntää vetoamista tilien pysymiseen tasapainossa.

Toinen Internetin ja tietokoneiden väärinkäyttöä käsittelevä tutkimus hyödyntää puolestaan peloteteoriaa, neutralisaatiotekniikoita sekä väärinkäytöstä aiheutuneen hyödyn vaikutuksia osana mallia, joka pyrkii selittämään väärinkäytöstä edeltävien päätösten syitä. Cheng ym. (2014) laajentavat aikaisempaa Limin (2002) tutkimusta integroimalla malliinsa kaikki alkuperäiset neutralisaatiotekniikat sekä myös peloteteorian keskeiset ominaisuudet, kuten sanktioiden kovuuden sekä sanktioiden varmuuden. Lisäksi malli pyrkii vertaamaan myös peloteteorian sekä neutralisaatiotekniikoiden keskinäistä voimakkuutta väärinkäytön ennustamisessa.

Cheng ym. (2014) tutkimuksen avulla saavutetut tulokset osoittavat, että neutralisaatiotekniikat ovat vahva ennustaja tietokoneiden ja Internetin väärinkäytölle työaikana. Tulos laajentaa Lim (2002) esittämää tutkimusta osoittaen, että vetoamisen tilien pysymiseen tasapainossa ohella myös kaikki alkuperäiset neutralisaatiotekniikat ennustavat työtekijöiden harrastamaa tietokoneiden väärinkäyttöä. Tutkimus ottaa myös kantaa peloteteorian ja neutralisaatiotekniikoiden keskinäiseen tehokkuuteen väärinkäytösten ennakoinnissa. Tulokset löytävät tukea hypoteesille, joka ennustaa neutralisaatiotekniikoiden olevan voimakkaampi ennustaja työntekijöiden väärinkäytön aikomusten suhteen (Cheng ym., 2014).

3.4 Neutralisaatiotekniikoiden hyödyntäminen käytännön sovellutuksissa

Viimeisenä aihekokonaisuutena ovat käytännön tutkimukset, jotka pyrkivät hyödyntämään neutralisaatiotekniikoita erilaisissa reaalimaailman ympäristöissä sekä testaamaan neutralisaatiotekniikoiden toimintaa tarkasti rajatuissa käyttökonteksteissa. Tämän aihekokonaisuuden tutkimukset ovat pääosin melko tuoreita, alle viiden vuoden ikäisiä ja ne pyrkivät pääsääntöisesti vastaamaan aiemmassa tutkimuskirjallisuudessa esiin nousseisiin puutteisiin tai esitettyihin jatkotutkimusaiheisiin.

Ensimmäisenä ja samalla vanhimpana tutkimuksena toimii tutkijoiden Siponen, Vance sekä Willison (2012) organisaatioiden ohjelmistopiratismia käsittelevä tutkimus. Tutkimuksena tavoitteena on tuottaa ymmärrystä koskien neutralisaatiotekniikoiden roolia organisaation sisäisessä ohjelmistopiratismissa sekä selvittää, mitkä neutralisaatiotekniikoista vaikuttavat ilmiön taustalla. Neutralisaatiotekniikoiden lisäksi tutkimuksessa hyödynnettävä malli omaksuu peloteteoriasta häpeän, sanktiot sekä moraaliset uskomukset, mikä tarjoaa tutkijoille mahdollisuuden mitata kyseisten tekijöiden vaikutusta ohjelmistopiratismiin sekä verrata peloteteorian osien ja neutralisaatiotekniikoiden keskinäistä voimakkuutta ohjelmistopiratismin aikomusten ennustamisessa.

Siposen ym. (2012) tutkimuksen tulokset vahvistavat neutralisaatiotekniikoiden vaikuttavuudessa olevan eroavaisuuksia, mikä tukee tutkimuskirjallisuudessa esiintyvää käsitystä neutralisaatiotekniikoiden eriasteisista soveltuvuuksista yksittäisiin rikkomuksiin. Tulosten perusteella neutralisaatiotekniikoista vain tuomion tuomitseminen sekä vetoaminen korkeampiin velvollisuuksiin vaikuttivat työntekijöiden aikomuksiin toteuttaa ohjelmistopiratismia (Siponen ym., 2012). Saavutetut tulokset tarjoavat teoreettisen kontribuution ohella myös oleellista tietoa ohjelmistopiratismin ehkäisyn suhteen, tuottaen suosituksen painottaa piratismin vastaisessa koulutuksessa menetelmiä, jotka ehkäisevät edellä mainittujen neutralisaatiotekniikoiden käyttöä.

Toisena ohjelmistoihin liittyvänä käytännön tutkimuksena toimii Silic ym. (2017) varjo-ohjelmistoihin keskittyvä tutkimus, joka pyrkii selvittämään yksittäisten neutralisaatiotekniikoiden roolia kiellettyjen ohjelmistojen hyödyntämisessä. Tutkimuksen kontekstissa varjo-ohjelmistoilla tarkoitetaan organisaatioiden työntekijöiden lataamia ja hyödyntämiä ohjelmistoja, jotka ovat tietoturvaohjeistuksen vastaisia ja joita ei ole hyväksytty organisaation toimesta (Silic ym., 2017). Tärkeimpänä tutkimuskysymyksenä tutkijat pyrkivät selvittämään, mitkä yksittäiset neutralisaatiotekniikat ennakoivat varjo-ohjelmistojen käyttöä. Lisäksi tutkimus pyrkii myös vertaamaan aikomusten ennustamiseen esitettyjä neutralisaatiotekniikoita varsinaisiin hyödynnettyihin tekniikoihin (Silic ym., 2017).

Silic ym. (2017) tutkimuksen tulokset osoittavat, että neutralisaatiotekniikoista vain vetoaminen tilien pysymiseen tasapainossa vaikutti työntekijöiden aikomuksiin käyttää varjo-ohjelmistoja. Myöskään peloteteorian tekijät, kuten

häpeä, sanktiot sekä uskomukset eivät vaikuttaneet työntekijöiden aikomuksiin. Tuloksen perusteella organisaatioiden tulisi pyrkiä estämään vetoamista tilien pysymiseen tasapainossa käyttämistä työntekijöiden keskuudessa varjo-ohjelmistojen käytön estämiseksi.

Neutralisaatiotekniikoita koskevien tulosten ohella merkittävänä lisäyksenä tutkimuskirjallisuuteen toimivat myös Silic ym. (2017) tulokset koskien aikomusten sekä varsinaisten toimien suhdetta. Monet neutralisaatiotekniikoita hyödyntävät tutkimukset eivät suoraan mittaa varsinaista työntekijöiden toimintaa, vaan yleistävät erilaisilla skenaarioilla tuotetut tulokset vastamaan oikeaa reaalimaailman toimintaa. Tätä on perusteltu muun muassa kriminologian tutkimuskirjallisuudella, joka toteaa aikomusten ennakoivan vahvasti varsinaista toimintaa (Siponen & Vance, 2010). Silic ym. (2017) tutkimus tuottaa tälle väitteelle tukea myös tietoturvatutkimuksen sekä neutralisaatiotekniikoiden kontekstissa.

Ohjelmistojen ohella neutralisaatiotekniikoita on pyritty hyödyntämään tietoturvakoulutuksen sekä muiden tietoisuutta lisäävien ohjelmien suunnittelussa ja toteuttamisessa. Tutkijoiden Bauer, Bernroider ja Chudzikowski (2017) julkaisu käsittelee keskieurooppalaisten pankkien tietoturvakoulutukseen ja -tietoisuuteen kehitettyjä menetelmiä sekä niiden vastaanottoa organisaation jäsenten keskuudessa.

Aineiston perusteella Bauer ym. (2017) toteavat pankkien välillä olevan merkittäviä eroa tietoturvakoulutuksen kattavuudessa sekä yleisen tietoturvatietoisuuden välillä. Yksikään tutkimukseen osallistuneista pankeista ei hyödyntänyt neutralisaatiotekniikoiden torjumiseen suunniteltuja välineitä, vaikka tutkimuksen yhteydessä havaittiin neutralisaatiotekniikoiden olevan käytössä organisaatioiden jokaisella tasolla (Bauer ym., 2017). Neutralisaatiotekniikoiden monitasoisen käytön ohella tulokset osoittavat myös käytettyjen neutralisaatiotekniikoiden vaihtelevan organisaatioiden eri tasoilla. Esimerkiksi asiakaspalvelun kanssa työskentelevät työntekijät vaikuttaisivat hyödyntävän toiminnassaan vetoamista korkeampiin velvollisuuksiin, vetoamista toimimiseen pakon edessä sekä vahingon kieltämistä. Sen sijaan organisaation johto- sekä toimistotehtävissä työskentelevät henkilöt hyödynsivät vain vahingon kieltämistä (Bauer ym., 2017).

Bauer ym. (2017) tutkimuksella saavutetut tulokset tuottavat kaksi merkittävää lisäystä neutralisaatiotekniikoita käsittelevään kirjallisuuteen. Tulokset osoittavat, että neutralisaatiotekniikoiden hyödyntäminen ei ole yhtäläistä edes organisaatioiden sisällä, vaan niiden hyödyntäminen vaihtelee, esimerkiksi työtehtävistä riippuen. Tämän argumentin pohjalta tutkijat tuottavat toisen kontribuutionsa, jonka mukaan organisaation sisäinen tietoturvakoulutus tulisi räätälöidä entistä tarkemmin, eri työntekijäryhmien välillä (Bauer ym., 2017).

Pankkien ohella neutralisaatiotekniikoiden roolia tietoturvakoulutuksissa on tarkasteltu myös organisaatioiden salasanakäytäntöjen osalta. Tuoreessa vuonna 2020 julkaistussa tutkimuksessa tutkijat Siponen, Puhakainen ja Vance pyrkivät selvittämään voidaanko neutralisaatiotekniikoiden vastaisella koulutuksella ehkäistä näiden käyttöä, erityisesti salasanojen luomisen yhteydessä.

Tutkimuksen tavoitteena on neutralisaatiotekniikoiden ehkäisemisen ohella tarkastella, vaikuttaako räätälöity koulutus työntekijöiden käytäntöihin parempien salasanojen luomisen osalta.

Siponen ym. (2020) tulokset löytävät tukea hypoteeseille, joka ennustaa koulutuksella olevan vaikutusta yksilöiden todennäköisyyteen hyödyntää toiminnassaan neutralisaatiotekniikoita. Aineiston perusteella neutralisaatiotekniikoiden torjuntaan räätälöity koulutus vähensi selvästi työntekijöiden aikomuksia alkuperäisten neutralisaatiotekniikoiden hyödyntämiseen (Siponen ym., 2020). Neutralisaatiotekniikoiden ehkäisemisen ohella räätälöidyn koulutuksen saaneet työntekijät raportoivat selvästi korkeampia aikomuksia vahvempien salasanojen hyödyntämiseen verrattuna kontrolliryhmään.

Poikkeuksellisena piirteenä Siposen ym. (2020) tutkimuksessa on myös vaikutusten uudelleenarviointi vajaan kuukauden sisällä alkuperäisen koulutuksen jälkeen. Monet neutralisaatiotekniikoita hyödyntävät tietoturvatutkimukset pystyvät osoittamaan tuloksissa neutralisaatiotekniikoiden olevan vahva ennustaja tietoturvakäyttäytymiselle, mutta ne eivät pysty ottamaan kantaa vaikutusten kestoon tai tulosten yleistettävyyteen pidemmällä aikavälillä. Puutteen johdosta neutralisaatiotekniikoita käsittelevä tutkimus ei pysty tuottamaan käytännön suosituksia, esimerkiksi optimaaliselle koulutusten aikavälille. Siposen ym. tutkimus osoittaa koulutuksella saavutetun vaikutuksen kestävän vähintäänkin 3 viikon ajan (Siponen ym., 2020). Kyseinen havainto tuottaa tutkijayhteisölle ensimmäisen kerran tutkittua tietoa neutralisaatiotekniikoiden ehkäisemisen vaikutusten kestosta tietoturvan kontekstissa.

Viimeisen käytännön sovellutuksia tutkivan tutkimuksen osalta painopisteenä ovat neutralisaatiotekniikoiden ja työntekijöiden sukupuolen rooli osana tietoturvakäyttäytymistä ohjaavien pelotteiden ja palkintojen vaikutusta. Yhteisen vaikutuksen ohella Bansal, Muzatko ja Shin (2020) tutkimus tarkastelee myös neutralisaatiotekniikoita sekä sukupuolta itsenäisinä tekijöinä ja pyrkii arviomaan vaikuttavatko kyseiset tekijät työntekijöiden aikomuksiin rikkoa tietoturvaohjeistusta.

Tulosten osalta Bansal ym. (2020) tutkimus ei löydä tukea hypoteesille, joka ennustaa sukupuolen olevan suoraan vaikuttava tekijä tietoturvakäyttäytymisen osalta. Sen sijaan tutkimus löytää tukea hypoteesille, joka ennustaa neutralisaatiotekniikoiden lisäävän työntekijöiden aikomuksia poiketa tietoturvaohjeistuksesta. Tutkimusaineiston perusteella neutralisaatiotekniikoiden hyödyntäminen ja aikomukset rikkoa tietoturvaohjeistusta vaikuttaisivat olevan yhtä todennäköistä työntekijöiden sukupuolesta riippumatta.

Vaikka sukupuolen vaikutukselle tietoturvarikkomusten suhteen ei löydetty suoraa tukea, tutkimustulokset löytävät tukea hypoteesille, joka ennustaa sukupuolen ja neutralisaatiotekniikoiden vaikuttavan pelotteiden sekä palkintojen tehokkuuteen. Tutkimustulosten perusteella tutkimukseen osallistuneet naiset reagoivat vahvemmin palkintoihin ja miehet puolestaan rangaistuksiin. Näiden tulosten pohjalta tutkijat toteavatkin, että palkinnot ehkäisevät naisilla neutralisaatiotekniikoista vetoamista toimimiseen pakon edessä hyödyntämistä

ja pelotteet, kuten rangaistukset ehkäisevät miehillä vetoamista tilien pysymiseen tasapainossa sekä vahingon kieltämisen hyödyntämistä (Bansal ym., 2020).

4 TULOSTEN ARVIOIMINEN JA POHDINTA

Tässä pääluvussa käydään läpi tutkielman yhteydessä saavutetut tulokset ja vastataan tutkielman alussa esitettyihin tutkimuskysymyksiin. Tutkimuksen aineiston perusteella esitetään tutkielman tuloksia koskevat johtopäätökset ja arvioidaan näiden mahdollisia vaikutuksia. Tulosten esittelyn lisäksi luku tarkastelee aineistosta esiin nousseita puutteita, huomioita sekä muita rajoitteita kappaleen pohdinta osiossa. Pohdinnan yhteydessä otetaan myös kantaa sekä esitellään jatkotutkimusaiheita esiin nousseiden tulosten perusteella.

4.1 Tutkielman tulokset

Tutkielman tekoa ohjaavana tavoitteena oli tarkastella ja tuottaa katsaus neutralisaatiotekniikoiden asemaan organisaatioiden tietoturvaa käsittelevässä tutkimuksessa ja samalla vastata tutkielman ensimmäiseen tutkimuskysymykseen, miten neutralisaatiotekniikoita on hyödynnetty osana organisaatioiden tietoturvatutkimusta.

Kirjallisuuskatsauksen perusteella neutralisaatiotekniikat ovat vanhasta teoreettisesta taustastaan huolimatta melko tuore tutkimussuuntaus organisaatioiden tietoturvaa käsittelevässä tutkimuksessa, minkä seurauksena myös kirjallisuuden määrä on rajallista. Neutralisaatiotekniikat ovat saavuttaneet viimeisen kymmenen vuoden aikana jalansijaa tutkijoiden keskuudessa, mikä on näkynyt tutkimusten kasvaneena määränä. Tämän kirjallisuuskatsauksen osalta yli puolet käsitellyistä tutkimuksista ovat alle viiden vuoden ikäisiä ja merkittävä osa tutkimuksista on julkaistu viimeisen vuoden aikana.

Aihepiirin kasvaneen kiinnostuksen myötä myös aihetta tutkivien tutkijoiden joukko on kasvanut, mikä on lisännyt tutkimusten määrä sekä laajentanut tutkimusasetelmia. Tutkimusaiheen pioneeritutkijoiden joukko on melko rajallinen ja vanhemman kirjallisuuden yhteydessä esiin nousevat samat tutkijat usein eri tutkimusryhmien kombinaatioissa. Tuoreempien tutkimusten osalta pioneeritutkijoiden joukko on edelleen mukana merkittävässä roolissa uuden

tiedon tuottamisen osalta, mutta aihepiiri on kerännyt myös täysin uusia nimiä eri puolilta maailmaa. Tämä kehityssuunta on aihepiirin tutkimuksen kannalta positiivinen ensinnäkin siksi, että suuremman tutkijajoukon myötä tutkitun tiedon määrän kasvu on nopeampaa sekä myös siksi, että tutkimuksia on helpompi toteuttaa eri tutkimusympäristöissä, esimerkiksi eri maissa.

Itse tutkimusten aiheet ovat jaettu tämän tutkielman osalta neljään tunnistettuun pääryhmään tutkimuskysymysten sekä tutkimusten asettelun perusteella. Yhteenveto tutkimusten jaottelusta on alla olevassa taulukossa (taulukko 1). Tutkimusten jaon osalta voidaan karkeasti todeta vanhempien julkaisujen painottuvan enemmän teoreettisempiin kontribuutioihin sekä neutralisaatiotekniikoiden hyödyntämiseen osana eri komponenteista, kuten peloteteoriasta tai oikeudenmukaisuusteoriasta koostuvia malleja. Tuoreempien julkaisujen osalta tutkimusten painopiste on siirtynyt pääosin konkreettisempien aihepiirien käsittelyyn, joissa pyritään tuottamaan tietoa tarkemmin rajattuihin tutkimuskysymyksiin sekä tuottamaan myös suoria suosituksia tai ehdotuksia mahdollisille toimenpiteille.

TAULUKKO 1 Neutralisaatiotekniikoita hyödyntävien tutkimusten luokittelu aihepiireittäin

Tutkijat	**Aihepiiri**	**Tutkimuksen kohde**
Siponen & Vance, 2010	Aikeiden ennustaja	Organisaatioiden työntekijöiden tietoturvakäyttäytyminen ja neutralisaatiotekniikoiden rooli tietoturvarikkeiden ennustamisessa.
Willison ym., 2018	Aikeiden ennustaja	Oikeudenmukaisuusteorian ja neutralisaatiotekniikoiden keskinäinen suhde sekä näiden vaikutus aikomuksiin tietokoneiden väärinkäytölle.
Simola ym., 2020	Aikeiden ennustaja	Kadettien aikomukset hyödyntää neutralisaatiotekniikoita. Neutralisaatiotekniikoiden ja persoonallisuuden piirteiden keskinäinen suhde.
Barlow ym., 2013	Viestintä	Voidaanko neutralisaatiotekniikoiden käyttöä vähentää kohdennetulla viestinnällä? Ehkäiseekö neutralisaatiotekniikoiden vastainen viestintä tietoturvarikkeitä?
Barlow ym., 2018	Viestintä	Miten eri viestinnän keinot vaikuttavat työntekijöiden aikomukseen rikkoa tietoturvaohjeita? Ehkäiseekö antineutralisaatiota korostava viestintä tietoturvarikkeitä?
Lim, 2002	Osana mallia	Neutralisaatiotekniikoiden rooli organisaatioissa tapahtuvan tietokoneiden ja Internetin väärinkäytön suhteen. Miten oikeudenmukaisuusteoria vaikuttaa vetoamiseen tilien pysymiseen tasapainossa

		hyödyntämiseen?
Willison & Warkentin, 2013	Osana mallia	Syyt organisaatioiden työntekijöiden tietoturvarikkomusten taustalla. Neutralisaatiotekniikat osana Security Action Cycle:ä.
Cheng ym., 2014	Osana mallia	Neutralisaatiotekniikoiden ja peloteteorian rooli työpaikoilla tapahtuvan Internetin väärinkäytön selittämisessä.
Gwebu ym., 2020	Osana mallia	Miten organisaatioiden sisäiset arvot ja organisaation työkulttuuri vaikuttavat työntekijöiden todennäköisyyteen käyttää neutralisaatiotekniikoita?
Vance ym., 2020	Osana mallia	Miten tietoturvakäyttäytymistä ennustavat mallit toimivat eri kulttuureissa ja maissa?
Siponen ym., 2012	Käytännön sovellutus	Mitkä neutralisaatiotekniikoista vaikuttavat työntekijöiden aikomuksiin harrastaa ohjelmistopiratismia? Neutralisaatiotekniikoiden ja peloteteorian osien voimakkuuden vertailu ohjelmistopiratismin ennustamisessa.
Bauer ym., 2017	Käytännön sovellutus	Miten keskieurooppalaiset pankit toteuttavat tietoturvakoulutuksensa ja miten koulutukset ja niiden vaikutukset koetaan työntekijöiden keskuudessa?
Silic ym., 2017	Käytännön sovellutus	Mitkä neutralisaatiotekniikoista ennakoivat työntekijöiden aikomusta hyödyntää varjo-ohjelmistoja? Mitä neutralisaatiotekniikoita työntekijät käyttävät varjo-ohjelmistojen hyödyntämisen yhteydessä?
Bansal ym., 2020	Käytännön sovellutus	Miten neutralisaatiotekniikat ja sukupuoli vaikuttavat pelotteiden, kuten rangaistusten ja palkintojen toimivuuteen tietoturvarikkomusten ehkäisemisessä?
Siponen ym., 2020	Käytännön sovellutus	Voidaanko neutralisaatiotekniikoiden käyttöä ehkäistä räätälöidyllä koulutuksella ja muilla interventioilla?

Kokonaisuutena arvioiden neutralisaatiotekniikoiden rooli osana organisaatioiden tietoturvaa käsittelevässä tutkimuskirjallisuutta ei vielä ole johtava eikä valtavirtaistunut. Neutralisaatiotekniikat vaikuttaisivat kuitenkin olevan nouseva teoria tietoturvatutkimuksen osalta sekä omana teorianaan että myös osana moniulotteisia malleja. Kasvavan kiinnostuksen ja monipuolistuneen tutkimuskentän myötä voidaan olettaa neutralisaatiotekniikoiden saavuttavan aikaisempaa merkittävämmän roolin tietoturvaa käsittelevässä kirjallisuudessa ja tämän seurauksena neutralisaatiotekniikoiden roolia osana reaalimaailman tietoturvaa tullaan todennäköisesti hyödyntämään laajemmin, esimerkiksi tietoturvakoulutuksen yhteydessä.

Tutkielman toisena tavoitteena on tarkastella kirjallisuuskatsaukseen kuuluvien tutkimusten tuloksia sekä vastata tutkimuskysymykseen, minkälaisia

tutkimustuloksia neutralisaatiotekniikoita hyödyntävät tutkimukset ovat tuottaneet neutralisaatiotekniikoiden suhteen.

Yleisenä tutkielman johtopäätöksenä voidaan todeta neutralisaatiotekniikoiden tuottaneen rohkaisevia sekä hyvää ennakoivia tutkimustuloksia tietoturvaa koskien. Kirjallisuuskatsauksen tutkimukset löytävät käytännössä jokaisen julkaisun yhteydessä tukea hypoteeseille, jotka esittävät neutralisaatiotekniikoiden olevan merkittävä ennustaja tietoturvarikkomuksille tai neutralisaatiotekniikoiden olevan keskeisessä roolissa yksittäisten tietoturvarikkomuksen taustalla. Nämä havainnot vahvistavat neutralisaatiotekniikoiden kriittistä roolia osana organisaatioiden tietoturvaa ja tarvetta räätälöidyille neutralisaatiotekniikoihin kohdistuville turvallisuusmenetelmille. Tutkimusten tuloksia ja rajoituksia käsittelevä yhteenveto on tiivistettynä alla olevassa taulukossa (taulukko 2).

TAULUKKO 2 Neutralisaatiotekniikoita hyödyntävien tutkimusten neutralisaatiotekniikoita koskevat tulokset ja tutkimusten yleisiä rajoitteita

Tutkijat	**Tutkimuksen tulokset**	**Tutkimuksen rajoitteita**
Siponen & Vance, 2010	Neutralisaatiotekniikat ovat erittäin hyvä ennustaja aikomuksille rikkoa tietoturvaohjeistusta.	Kaikki tutkimukseen osallistuneet työntekijät olivat samasta maasta. Tutkimus mittasi aikomusta eikä toimintaa.
Willison ym., 2018	Koetulla proseduraalisella oikeudenmukaisuudella on vaikutus työntekijöiden todennäköisyyteen käyttää neutralisaatiotekniikoita tietoturvarikkomusten neutralisoimiseen.	Tutkimus mittasi työntekijöiden aikomusta eikä varsinaista käyttäytymistä tai toimintaa.
Simola ym., 2020	Tietyt persoonallisuuden piirteet vaikuttavat ihmisten todennäköisyyteen hyödyntää yksittäisiä neutralisaatiotekniikoita.	Tutkimus mittasi työntekijöiden aikomusta eikä varsinaista käyttäytymistä tai toimintaa.
Barlow ym., 2013	Neutralisaatiotekniikoista vetoaminen toimimiseen pakon edessä lisäsi työntekijöiden aikomusta jakaa salasanojaan tietoturvaohjeistuksen vastaisesti. Neutralisaatiotekniikoiden käyttöä voidaan vähentää koulutuksella ja viestinnällä.	Tutkimuksessa tarkasteltiin vain pienempiä tietoturvarikkomuksia, kuten salasanojen jakamista eikä koko luokaltaan suurempia rikkomuksia. Koulutuksen vaikutuksen kestoon ei voida ottaa kantaa.
Barlow ym., 2018	Neutralisaatiotekniikoiden ehkäisemiseen räätälöidyllä viestinnällä voidaan vähentää työntekijöiden aikomuksia poiketa tietoturvaohjeistuksista.	Viestinnän vaikutuksen kestoon ei voida ottaa kantaa. Tutkimus hyödynsi vain yhtä tietoturvarikkomusta ja kahta neutralisaatiotekniikkaa.
Lim, 2002	Oikeudenmukaisuusteorian tekijät vaikuttavat työntekijöiden aikomukseen käyttää vetoamista tilien pysymiseen tasapainossa. Vetoaminen tilien pysymiseen tasapainossa lisäsi	Tutkimuksessa hyödynnettiin vain yhtä neutralisaatiotekniikkaa. Tutkimus toteutettiin verkkopohjaisena kyselynä, mikä voi johtaa datan tahottomaan vääristymiseen.

	työntekijöiden harrastamaa tietokoneiden väärinkäyttöä.	
Willison & Warkentin, 2013	Esitetään laajennettu Extended Security Action Cycle malli, johon neutralisaatiotekniikat on integroitu.	Uutta mallia ei empiirisesti testata.
Cheng ym., 2014	Kaikkien alkuperäisten neutralisaatiotekniikoiden käyttö ennustaa työtietokoneiden väärinkäyttöä.	Tutkimuksen osanottajat edustivat pientä väestöryhmää ja toimivat samalla maantieteellisellä alueella.
Gwebu ym., 2020	Neutralisaatiotekniikat lisäävät aikomusta rikkoa tietoturvaohjeistusta. Organisaation korostamat arvot vaikuttavat neutralisaatiotekniikoiden käyttöön.	Merkittävä osa vastaajista edusti korkeakouluttuja työntekijöitä.
Vance ym., 2020	Neutralisaatiotekniikat ennustavat tietoturvarikkomusten aikeita kulttuurillisista tekijöistä riippumatta.	Kaikki tutkimukseen osaa ottaneet työntekijät edustivat samaa monikansallista organisaatioita.
Siponen ym., 2012	Yksittäiset neutralisaatiotekniikat lisäävät aikomusta ohjelmistopiratismin, mutta kaikki neutralisaatiotekniikat eivät.	Tutkimus mittasi työntekijöiden aikomusta eikä varsinaista käyttäytymistä tai toimintaa
Bauer ym., 2017	Kaikkien tutkimukseen osallistuneiden pankkien työntekijät hyödynsivät neutralisaatiotekniikoita. Neutralisaatiotekniikoiden valinta ja käyttäminen vaihtelee organisaatioiden eri tasoilla.	Tutkimuksen otanta oli pieni ja kaikki osallistuneet pankit toimivat samankaltaisessa kulttuurillisessa ympäristössä. Tutkimuksissa ei kysytty suoraan työntekijöiden toiminnasta vaan arvioitiin muiden työntekijöiden toimintaa.
Silic ym., 2017	Vetoaminen tilien pysymiseen tasapainossa hyödyntäminen lisäsi aikomusta ja varjo-ohjelmistojen varsinaista käyttöä.	Kaikki työntekijät eivät välttämättä olleet tietoisia varjo-ohjelmistoja koskevista kielloista, mikä voi vaikuttaa tuloksiin.
Bansal ym., 2020	Naiset ja miehet reagoivat eri tavoin palkintoihin ja rangaistuksiin, mikä johtaa eri neutralisaatiostrategioihin sukupuolten välillä.	Tutkimukseen osallistuneet henkilöt olivat kaikki yliopisto-opiskelijoita. Opiskelijat edustivat myös hyvin pientä alueellista otantaa.
Siponen ym., 2020	Räätälöidyllä koulutuksella voidaan vaikuttaa työtekijöiden neutralisaatiotekniikoiden käyttöön ja aikomuksiin noudattaa tietoturvaohjeistuksia.	Koulutuksen saanut ryhmä ja kontrolliryhmä ei ollut muodostettu sattumanvaraisesti. Lisäksi mitattiin aikomusta eikä varsinaista käytöstä.

Suurten linjojen ohella tutkimukset osoittavat, että neutralisaatiotekniikat ovat alttiita olosuhteista riippuville sekä inhimillisille tekijöille, minkä seurauksena neutralisaatiotekniikoiden tehokkuus ja käyttö vaihtelee. Tutkimukset ovat osoittaneet, esimerkiksi organisaatioiden eri tason työntekijöiden hyödyntävän eri neutralisaatiotekniikoita (Bauer ym., 2017), sukupuolen ja yksittäisten neutralisaatiotekniikoiden vaikuttavan pelotteisiin eri tavoin (Bansal ym., 2020) sekä neutralisaatiotekniikoiden vastaisen koulutuksen parantavan työntekijöiden salasanakäytäntöjä ja ehkäisevän neutralisaatiotekniikoiden käyttöä (Siponen

ym., 2020). Tutkimusten tuloksista huolimatta tutkimukset eivät kuitenkaan vielä pysty esittelemään laajasti yleistettäviä malleja sekä reaalimaailmassa sovellettavia menetelmiä.

Tutkimusten tulosten osalta oleellisena huomiona on myös neutralisaatiotekniikoiden tehokkuus verrattuna tietoturva-alan tutkimuksissa laajasti hyödynnettyyn peloteteoriaan. Useat katsauksen tutkimuksista löytävät tukea hypoteesille, joka ennustaa neutralisaatiotekniikoiden olevan vahvempi tietoturva rikkomusten ennustaja, kuin peloteteoria (Siponen & Vance, 2010; Silic ym., 2017). Vaikka teorioiden keskinäinen vertailu tai kilpailu ei itsessään ole itseisarvo tietoturvan parantamisen näkökulmasta, tarjoaa kyseinen tulos kuitenkin implikaatioita tulevaisuuden tietoturvan osalta. Organisaatioita koskeva tietoturvatutkimus nojaa yhä tänäkin päivässä vahvasti peloteteoriaan (D'arcy & Herath, 2011). Tutkitun tiedon varassa tätä näkemystä olisi perusteltua laajentaa hyödyntämällä neutralisaatiotekniikoita peloteteorian rinnalla.

4.2 Pohdinta ja tulevaisuuden tutkimusaiheita

Neutralisaatiotekniikoita hyödyntävä tietoturvatutkimus on viimeisten vuosien tuottanut merkittäviä kontribuutioita, jotka ovat paikanneet aikaisemmassa kirjallisuudessa esiintyviä puutteita sekä rajoituksia. Tämän ohella tutkijat ovat onnistuneet osoittamaan erilaisilla tutkimusasetelmilla neutralisaatiotekniikoiden olevan tärkeä osa vallitsevaa tietoturvan ymmärrystä. Saavutuksista ja lupaavista tutkimustuloksista huolimatta neutralisaatiotekniikoita hyödyntävä tutkimuskirjallisuus törmää edelleen kahteen keskeiseen ongelmaan, jotka aiheuttavat merkittävän osan tunnistetuista rajoituksista sekä puutteista.

Ensimmäinen neutralisaatiotekniikoissa korostuva ongelma koskee neutralisaatiotekniikoilla saavutettujen tulosten yleistettävyyttä. Jo alkuperäisessä neutralisaatiotekniikoita käsittelevässä julkaisussaan Sykes ja Matza (1957) esittävät neutralisaatiotekniikoiden soveltuvuuden ja valinnan olevan epäselvää henkilöiden iästä, sukupuolesta, etnisyydestä ja sosioekonomisesta asemasta riippuen. Tämän tiedon puute esiintyy edelleen yli 60 vuotta myöhemmin ja vieläkään tietoturvaa käsittelevä tutkimus ei pysty riittävästi yleistämään neutralisaatiotekniikoiden käyttöä kyseisten kriteerien osalta. Ongelman voidaan jopa katsoa laajentuneen, sillä tämä päivänä tietoa yleistettävyydestä tarvitaan myös, esimerkiksi organisaatioiden sisäisistä eroista sekä neutralisaatiotekniikoiden soveltuvuuksista eri kulttuureiden välillä.

Vaikka tuoreet tutkimukset ovat pyrkineet vastaamaan tunnistettuun ongelmaan ja tuottaneet tutkittua tietoa sukupuolen (Bansal ym., 2020), kulttuurillisten erojen (Vance ym., 2020) sekä organisaation eri tasojen eroista (Bauer ym., 2017) neutralisaatiotekniikoihin, sisältävät tutkimukset rajoituksia, jotka aiheuttavat haasteita yleistettävyyden kannalta. Muun muassa Vance ym. (2020) tutkimus kulttuurin vaikutuksista neutralisaatiotekniikoiden käyttöön ei löydä merkittäviä kulttuurin aiheuttamia eroja, mutta tutkimus on toteutettu yhteistyössä vain yhden monikansallisen organisaation kanssa ja on siten altis mah-

dollisille poikkeamille yleistämisen suhteen. Myös Bansal ym. (2020) tutkimus löytää eroja sukupuolten välillä neutralisaatiostrategioissa, mutta myös heidän tutkimuksessaan esiintyy ongelmia laajan yleistettävyyden osalta, sillä tutkimus ei pysty ottamaan kantaa vaikuttaako, esimerkiksi vastaajan ikä valittuun neutralisaatiostrategiaan. Tämän seurauksena saman sukupuolen, mutta eri ikäiset edustajat voivat hyödyntää neutralisaatiota eri tavoin.

Edellä mainitut esimerkit neutralisaatiotekniikoiden yleistettävyyden ongelmista eivät ole kattava listaus kaikista havaituista ongelmista, mutta ne havainnollistavat kirjallisuudessa esiintyvää ongelmaa. Tulevaisuuden tutkimuksen osalta onkin tärkeää pyrkiä vastaamaan yleistettävyyden aiheuttamiin ongelmiin jatkamalla tarkasti rajattujen käytännön tutkimusten tuottamista sekä pyrkimällä laajentamaan tutkimusten aineistoa, esimerkiksi monikansallisilla tutkimusten kohderyhmillä. Tämän lisäksi jatkotutkimukset, jotka tuottavat potentiaalisesti laajasti sovellettavia malleja olisivat arvokas lisä tutkimuskirjallisuuteen.

Toinen tutkimuksissa toistuva ongelma liittyy tutkimuksen aineiston hankintaan sekä tutkimusten varsinaisiin toteutuksiin. Merkittävä osa neutralisaatiotekniikoita hyödyntävistä tutkimuksista on toteutettu hyödyntämällä skenaariomallinnusta, minkä seurauksena aineiston avulla on jouduttu mittamaan ensisijaisesti tutkimusten osanottajien aikomusta rikkoa tietoturvaohjeistusta, eikä varsinaista toimintaa. Koska yksittäisten henkilöiden oikeaa tietoturvakäyttäytymistä on hankala mitata (Barlow ym., 2018), joudutaan useissa tutkimuksissa täten olettamaan, että tutkimuksissa raportoidut aikomukset ennakoivat vahvasti varsinaista käyttäytymistä.

Ongelmaa on pyritty tutkimuksissa paikkaamaan hyödyntämällä kriminologian tutkimuksesta saavutettuja tutkimustuloksia aikomusten ja varsinaisen toiminnan keskinäisestä suhteesta (Siponen & Vance, 2010; Siponen ym., 2012). Kyseiset tulokset esittävät, että aikomukset ja toiminta vastaavat toisiaan läheisesti, minkä seurauksena skenaariomallinnuksen avulla saavutetut tulokset voidaan yleistää vastaamaan reaalimaailman käytöstä (Pogarsky, 2004). Toisena ratkaisuna kirjallisuudessa esiintyy tutkimusmenetelmä, jossa tutkijat kysyivät vastaajilta muiden työntekijöiden toiminnasta (Bauer ym., 2017). Tämän menetelmän avulla tutkijat pyrkivät madaltamaan rehellisen vastaamisen kynnystä ja saamaan suoria vastauksia havaitusta toiminnasta, joka ei kuitenkaan ollut vastaajien itsensä suorittamaa. Vaikka menetelmän avulla voidaan tarkastella varsinaista toimintaa, on menetelmä altis esimerkiksi yksilöiden virheellisille subjektiivisille tulkinnoille muiden toiminnasta ja muille tarkoituksenhakuisille tutkinnoille.

Tutkielman kirjallisuuskatsauksen osalta tutkimuksista vain yksi mittasi skenaariomallinnuksen ja varsinaisen tietoturvakäyttäytymisen vastaavuutta. Kyseinen tutkimus löytää tukea kriminologiasta lainatulle argumentille, joka ennustaa aikomusten vastaavan varsinaista toimintaa (Silic ym., 2017), mikä vahvistaa argumentin soveltuvuutta osana tietoturvatutkimusta. Edellä mainitusta tutkimuksesta huolimatta aikomuksia hyödyntää neutralisaatiotekniikoita sekä varsinaisten neutralisaatiotekniikoiden käyttöä tulisi vertailla tulevaisuu-

dessa aiempaa enemmän, jotta skenaariomallinnuksen sopivuus organisaatioiden tietoturvakontekstissa voidaan tieteellisesti varmistaa. Optimaalisena jatkotutkimusten aiheena voidaankin pitää tutkimuksia, jotka pyrkivät kehittämään tutkimusmenetelmän, jonka avulla voidaan suoraan mitata neutralisaatiotekniikoiden käyttöä, mutta joka samalla mahdollistaa rehellisen datan keräämisen.

Rajoitusten ja haasteiden ohella neutralisaatiotekniikat tarjoavat myös runsaasti jatkotutkimuksen kohteita, joiden puuttuminen tunnistetaan tutkijayhteisön keskuudessa. Yksi oleellisimmasta neutralisaatiotekniikoita käsittelevän kirjallisuuden puutteista ovat pitkän aikavälin tutkimukset, jotka käsittelevät neutralisaatiotekniikoita sekä näiden vaikutuksia pidemmällä aikavälillä. Tämä puute tutkitun tiedon osalta on erityisen selkeä käytännön sovellutusten yhteydessä, jossa tutkimukset pyrkivät mittamaan, esimerkiksi tietoturvakoulutuksen vaikutusta lähes välittömästä koulutuksen jälkeen.

Tutkimuskirjallisuuden osalta vain yksi tutkimus tarkasteli tutkimuksensa yhteydessä neutralisaatiotekniikoita alkuperäisen koulutuksen jälkeen. Siposen ym. (2020) tutkimus käsittelee neutralisaatiotekniikoiden vastaisen koulutuksen tehokkuuden yhteydessä myös koulutuksen vaikutuksen kestoa, ja tutkijat toistavat kokeen kolme viikkoa alkuperäisen koulutuksen jälkeen. Tutkimuksen tulokset osoittavat koulutuksen vaikutuksen olevan selvästi läsnä vajaata kuukauden myöhemmin, mutta tuloksen perusteella ei voida sen tarkemmin ottaa kantaa, kuinka pitkään vaikutus on havaittavissa.

Tämän puutteen paikkaamiseksi neutralisaatiotekniikoita hyödyntävän jatkotutkimuksen tulisikin tarkastella erilaisten interventioiden, tietoiskujen sekä koulutuksen vaikutuksia riittävän pitkällä aikavälillä. Tämä tutkielma ei ota suoraan kantaa aikavälin riittävälle pituudelle, mutta tutkielma tunnistaa tarpeen ainakin jatkotutkimuksille, joiden tarkasteluvälit ovat vähintäänkin muutaman kuukauden tai jopa vuoden mittaisia. Aikapainotteisella jatkotutkimuksella voidaan katsoa olevan annettavaa luonnollisesti akateemisen kontribuution muodossa, mutta samalla myös suorana hyötynä tietoturvankoulutuksen suhteen. Tieteellisenä lisänä pitkäaikaistutkimus poistaisi tiedeyhteisön keskuudessa vallitsevan puutteen neutralisaatiotekniikoiden vastaisen koulutuksen kestosta ja samalla tuottaisi tarkempaa tietoa, kuinka pitkään työntekijöiden käyttäytymiseen voidaan vaikuttaa räätälöidyn koulutuksen avulla. Organisaatioiden osalta tutkimus mahdollistaisi entistä kattavamman ja tehokkaamman kouluttamisen, sillä tietoturvakoulutuksen syklit, olisi mahdollista ajoittaa optimaalisesti suhteessa koulutuksen vaikutuksen kestolle.

Ajallisten ulottuvuuksien lisäksi tärkeä ja tarpeellinen jatkotutkimuskohde on neutralisaatiotekniikoiden soveltaminen tapauksiin, joissa organisaatioiden tietoturvaa rikkovien henkilöiden toiminta on sekä tietoista että tahallista. Neutralisaatiotekniikoita hyödyntävien tutkimusten yhteydessä työntekijöiden toiminnan lähtökohtana on usein ajatus, jonka mukaan organisaatioiden työntekijät rikkovat tietoturvaohjeista tietoisesti, mutta heidän toimintansa ei ole pahantahtoista. Tämän lähtökohdan mukaan työntekijät tavoittelevat tietoturvarikkomuksilla, esimerkiksi organisaatiota osittain hyödyntäviä tavoitteita,

kuten ripeämpää asiakaspalvelua, eikä toiminnan tarkoituksena ole tarkoitus aiheuttaa tietoista vahinkoa organisaatioille.

Organisaatioiden riskienhallinnan kannalta potentiaalisena riskinä ovat myös pahantahtoiset työntekijät, joilla on pääsy organisaation kannalta arvokkaisiin tietoihin tai ohjelmiin. Tällä hetkellä neutralisaatiotekniikoita tutkiva kirjallisuus ei ota kantaa voidaanko neutralisaatiotekniikoita soveltaa edellä mainituissa tilanteissa. Tämän seurauksena tutkimuskirjallisuus ei pysty määrittelemään voidaanko pahantahtoisten työntekijöiden toimintaa ehkäistä neutralisaatiotekniikoiden vastaisella toiminnalla vai tarvitaanko kyseisten työntekijöiden torjuntaan muita menetelmiä. Potentiaalisena jatkotutkimuksena voisikin olla tutkimus, joka pyrkii tarkastelemaan, hyödynnetäänkö neutralisaatiotekniikoita ylipäätään tietoisten ja pahantahtoisten tietoturvarikkeiden yhteydessä.

Edellä mainittujen jatkotutkimusaiheiden ohella mahdollisena tutkimussuuntauksena voisi olla myös organisaation johdon rooli koskien työntekijöiden neutralisaatiotekniikoiden käyttöä. Aikaisempi tutkimuskirjallisuus on osoittanut neutralisaatiotekniikoiden hyödyntämisen olevan läsnä myös organisaation johdon toiminnassa (Bauer ym., 2017) sekä organisaation korostamilla arvoilla olevan vaikutusta työntekijöiden neutralisaatiotekniikoiden käyttöön (Gwebu ym., 2020). Näiden tulosten pohjalta potentiaalisena jatkotutkimuksen kohteena voisi olla organisaation johdon tai lähiesimiesten tuottaman esimerkin rooli työntekijöiden neutralisaatiotekniikoiden käytön suhteen.

Viimeisenä huomiona jatkotutkimusten osalta tämä tutkielma tunnistaa tarpeen edelleen kasvavalle ja entistä laajemmalle neutralisaatiotekniikoita tutkivien tutkijoiden joukolle. Vaikka aihepiirin tutkijoiden määrä on kasvanut viimeisten vuosien aikana, on tutkijoiden joukko edelleen suuressa mittakaavassa melko rajallinen. Laajemman tutkijoiden joukon voidaan katsoa tuottavan etuja jatkotutkimuksen suhteen ainakin kahdesta syystä. Ensinnäkin suurempi tutkijoiden joukko voi tuottaa useampia tutkimuksia nopeammalla aikavälillä ja täten tuottaa, esimerkiksi yleistämisen kannalta tärkeää tietoa.

Toisena laajemman tutkijajoukon etuna on myös laajempi tutkimuksen ulkopuolinen tarkastelu. Laajemman ulkopuolisen tarkastelun pohjalta on mahdollista, että tutkijat löytyvät uusia puutteita, virheitä, ristiriitaisia tuloksia tai muuta kritiikkiä, joka on aiemmin jäänyt tiedeyhteisön huomaamatta. Tämän lisäksi mahdollisimman avoin ja laaja dialogi tutkimusten luotettavuudesta, validiteetista ja tuloksista on oleellista ylipäätään tieteellisestä näkökulmasta. Mahdollisten ongelmien havaitsemisen ohella ulkopuolisten tutkijoiden näkemykset voivat myös tarjota valtavirrasta poikkeavia tutkimusaiheita tai menetelmiä, jotka voivat tuottaa merkittävää lisäarvoa neutralisaatiotekniikoita hyödyntävälle tietoturvatutkimukselle.

5 YHTEENVETO

Tässä tutkielmassa tarkasteltiin neutralisaatiotekniikoita, niiden teoreettista taustaa sekä soveltuvuutta osana tietoturvan tutkimuskirjallisuutta. Tutkielman tavoitteena oli tuottaa kuvaileva kirjallisuuskatsaus neutralisaatiotekniikoita hyödyntäviin organisaatioiden tietoturvaa tutkiviin julkaisuihin ja selvittää miten neutralisaatiotekniikoita on sovellettu aihepiirin osalta. Lisäksi tutkielman toisena tavoitteena oli tarkastella kirjallisuuskatsaukseen valikoituneiden tutkimusten saavuttamia tutkimustuloksia, erityisesti neutralisaatiotekniikoiden osalta. Tutkimuksen tavoitteiden ohella tutkielman tekoa ohjasi rajoitus tuoreiden lähteiden hyödyntämisestä ja tämän seurauksena tutkimuksen lähdeaineisto oli muutamaa poikkeusta lukuun ottamatta julkaistu 2000-luvulla. Edellä mainittujen kriteerien pohjalta tutkielman tutkimuskysymyksiksi muodostuivat seuraavat:

- Miten neutralisaatiotekniikoita on hyödynnetty osana organisaatioiden tietoturvatutkimusta?
- Minkälaisia tutkimustuloksia neutralisaatiotekniikoita hyödyntävät tutkimukset ovat tuottaneet koskien neutralisaatiotekniikoita?

Tutkielman toisessa luvussa suorettiin katsaus neutralisaatiotekniikoiden historialliseen kehitykseen, teoreettiseen taustaan sekä määriteltiin tarkemmin keskeisimmät neutralisaatiotekniikat. Luvun yhteydessä määriteltiin myös alkuperäisten neutralisaatiotekniikoiden ulkopuolisia tekniikoita, joista tutkielmaan valikoituivat tietoturvakirjallisuuden kannalta relevanteimmat. Kokonaisuutena arvioiden tutkielman teoreettisen taustan pohjalta voidaan todeta neutralisaatiotekniikoiden noudattavan edelleen monilta osin Sykesin ja Matzan (1957) esittämää teoreettista kehystä ja neutralisaatiotekniikoiden olevan tiedeyhteisön keskuudessa varsin vakiintuneesti määritelty. Yleisen määritelmän sijaan neutralisaatiotekniikoiden yksittäiset määritelmät, neutralisaatiotekniikoiden määrä ja neutralisaatiotekniikoiden soveltaminen vaihtelee tutkimuskirjallisuudessa.

Tutkielman kolmannessa luvussa tarkasteltiin organisaatioiden tietoturvaa tutkiva julkaisuja, jotka hyödynsivät neutralisaatiotekniikoita itsenäisesti tai vaihtoehtoisesti osana laajempaa kokonaisuutta. Tutkielmassa tunnistetaan julkaisujen jakautuvan aihepiiriensä perustella neljään ryhmään, jotka ovat neutralisaatiotekniikat aikeiden ennustamisessa, neutralisaatiotekniikat viestinnässä, neutralisaatiotekniikat osana malleja sekä käytännön tutkimukset. Jaon perusteella suosituimmiksi aihepiireiksi nousivat neutralisaatiotekniikoiden hyödyntäminen osana moniulotteisia malleja sekä neutralisaatiotekniikoiden soveltaminen osana käytännön tutkimuksia.

Tutkielman neljäs luku käsittelee kerätyn aineiston perusteella saavutettuja keskeisiä löydöksiä ja vastaa tutkielman alussa määriteltyihin tutkimuskysymyksiin. Neutralisaatiotekniikoita organisaatioiden tietoturvan yhteydessä käsittelevä tutkimuskirjallisuus on melko tuoretta, mikä näkyy kirjallisuuden rajallisena määränä. Julkaisujen määrä on kuitenkin ollut viimeisten vuosien aikana kasvussa, mikä viittaisi aihepiirin lisänneen houkuttelevuuttaan. Kuten aiemmin jo mainittu, organisaatioiden tietoturvaa käsittelevät ja neutralisaatiotekniikoita hyödyntävät tutkimukset voidaan jakaa neljään keskeiseen aihepiiriin, joiden suosio on vaihdellut viimeisen vuosikymmenen aikana. Tutkimusten aihepiirien painopiste on siirtynyt yhä enemmän teoreettisista sovellutuksista käytännön tutkimuksiin sekä soveltuvuuksiin.

Kirjallisuuskatsauksessa esiintyvien tulosten perusteella voidaan todeta, että neutralisaatiotekniikat ovat vahvasti olosuhde riippuvaisia, mikä näkyy esimerkiksi eri neutralisaatiotekniikoiden soveltumisena eri tietoturvarikkomusten yhteydessä. Neutralisaatiotekniikoiden olosuhde riippuvuus on rajallisen kirjallisuuden ohella yksi tärkeimmistä tekijöistä neutralisaatiotekniikoiden yleistettävyyden ongelmien osalta. Yleistettävyyden haasteista huolimatta tutkimusten tulokset löytävät vahvaa tukea ajatukselle, joka ennustaa neutralisaatiotekniikoiden olevan vahva ennustaja sekä merkittävä tekijä tietoturvarikkomusten taustalla. Tämän toistuvasti vahvistetun argumentin perusteella neutralisaatiotekniikoiden roolia osana tietoturvatutkimusta tulisi laajentaa entisestään ja neutralisaatiotekniikat tulisi nähdä kriittisenä osana tietoturvakäyttäytymistä.

Tulevaisuuden jatkotutkimuskohteiden osalta neutralisaatiotekniikat tarjoavat useita tutkimusaiheita sekä suuntauksia. Neutralisaatiotekniikoiden soveltamisen keskeisenä ongelmana on puuttuva ymmärrys niiden laajasta yleistettävyydestä, minkä seurauksena tulevaisuuden jatkotutkimuksia voidaan suunnata ainakin kahteen tutkimussuuntaukseen. Ensimmäisenä suuntauksena ovat jo kirjallisuudessa esiintyvien tutkimusten kaltaiset käytännön sovellutukset, jotka tuottavat lisätietoa nykyisin tuntemattomista aiheista, kuten neutralisaatiotekniikoiden vastaisen koulutuksen tehokkuuden kestosta tai neutralisaatiotekniikoiden soveltamisesta eri ikäryhmien kohdalla. Toisena suuntauksena ovat tutkimukset, jotka pyrkivät vertailemaan neutralisaatiotekniikoiden osa-alueiden soveltuvuutta, esimerkiksi eri demografisten tekijöiden osalta tai eri kulttuuriympäristöissä ja täten tuottamaan yleistettävämpiä tuloksia.

Edellä mainittujen jatkotutkimussuuntausten ohella neutralisaatiotekniikoita käsittelevä tutkimuskirjallisuus tunnistaa myös puutteen suorille yksittäisille tutkimusaiheille. Yhtenä potentiaalisena jatkotutkimuksen aiheena on neutralisaatiotekniikoiden soveltuvuus organisaatioiden työntekijöihin, joiden toiminta on tietoista sekä samalla myös pahantahtoista. Kyseistä aihetta tutkiva jatkotutkimus tuottaisi tietoa tulisiko neutralisaatiotekniikoita tutkia tulevaisuudessa myös tarkemmin tästä näkökulmasta vai edellyttääkö asetelma jotakin muuta teoreettista kehystä. Lisäksi tarpeellisena jatkotutkimuksen aiheena ovat tutkimukset, jotka tutkivat työntekijöiden neutralisaatiotekniikoiden käytön aikomusten ja varsinaisen käytön keskinäistä suhdetta.

LÄHTEET

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33(3),* 237-248.

Bansal, G., Muzatko, S., & Shin, S. I. (2020). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology & People*.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security*, *39*, 145-159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems, 19(8),* 3.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *computers & security*, *68*, 145-159

Chatzidakis, A., Hibbert, S., & Smith, A. P. (2007). Why people don't take their concerns about fair trade to the supermarket: The role of neutralisation. *Journal of business ethics*, *74*(1), 89-100.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, *38*, 220-228.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20(6),* 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research, 20(1),* 79-98.

De Bock, T., & Van Kenhove, P. (2011). Double standards: The role of techniques of neutralization. *Journal of Business Ethics, 99(2),* 283-296.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *computers & security, 28(3-4),* 189-198.

Fritsche, I. (2005). Predicting deviant behavior by neutralization: Myths and findings. *Deviant Behavior*, *26*(5), 483-510.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal, 30(2),* 220-269.

Kaptein, M., & Van Helvoort, M. (2019). A model of neutralization techniques. *Deviant Behavior*, *40*(10), 1260-1285.

Klockars, C. B. (1974). The professional fence (pp. 7899-7899). New York: Free Press.

Lim, V. K. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of organizational behavior: the international journal of industrial, occupational and Organizational Psychology and Behavior, 23(5),* 675-694.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research?. *Crime and justice, 32*, 221-320

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of research in crime and delinquency, 18(2),* 295-318.

Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity. *Criminology, 42(1),* 111-136.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management, 54(8),* 1023-1037.

Simola, P., Virtanen, T., & Sartonen, M. (2020). Information Security, Personality, and Justifications for Norm Violation. *Journal of Information Warfare, 19(2),* 62-IV

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security, 88,* 101617.'

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly,* 487-502.

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49(7-8),* 334-341.

Sutherland, E. H. (1945). Is" white collar crime" crime?. *American sociological review, 10(2),* 132-139.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security, 72,* 212-233.

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management, 57(4),* 103212

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49(3-4),* 190-198.

Vendrell-Herrero, F., Bustinza, O. F., Parry, G., & Georgantzis, N. (2017). Servitization, digitization and supply chain interdependency. *Industrial Marketing Management, 60,* 69-81.

Versteeg, G., & Bouwman, H. (2006). Business architecture: A new paradigm to relate business strategy to ICT. *Information systems frontiers, 8(2),* 91-102.

Vestman, T. (2020). *Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä* (Väitöskirja, Jyväskylän yliopisto). Haettu osoitteesta http://urn.fi/URN:ISBN:978-951-39-8174-7

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18(2),* 101-105.

Williams, K., Chatterjee, S., & Rossi, M. (2008). Design of emerging digital services: a taxonomy. *European journal of information systems, 17(5),* 505-517.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly,* 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293.