Eettinen hakkerointi systeemiteoreettisessa tarkastelussa

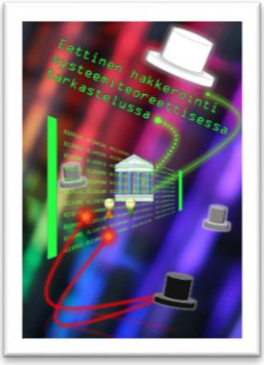
TAMPEREEN YLIOPISTO

Eettinen hakkerointi systeemiteoreettisessa tarkastelussa

Yksikkö
Luonnontieteiden tiedekunta

Raporttityyppi
Pro gradu -tutkielma
Valmistumispäivämäärä
4.3.2018

Tutkija
Santeri Taskinen, hall. kand.
Ohjaaja
Erkki Mäkinen, professori



Tampereen yliopisto, Luonnontieteiden tiedekunta
Tietojenkäsittelytieteiden tutkinto-ohjelma
TASKINEN, SANTERI MIKAEL
Eettinen hakkerointi systeemiteoreettisessa tarkastelussa
Pro gradu -tutkielma
61 sivua + 2 liitesivua
Filosofian maisterin tutkinto
Maaliskuu 2018

Tämä tutkimus vastaa kysymykseen, miten eettisen hakkeroinnin menettelytavoilla voidaan parantaa organisaatioiden kyberturvallisuutta.

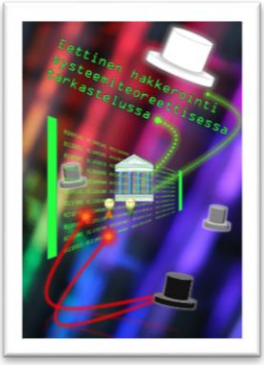
Tutkimus on metodologialtaan **kvalitatiivinen** asiantuntijoiden teemahaastatteluihin perustuva analyysi. Teemahaastattelut toteutettiin talvella 2016 Jyväskylän kyberturvallisuusmessuilla. Haastateltavat olivat eettisen hakkeroinnin ja kyberturvallisuuden asiantuntijoita. Tutkimuksen aineistona on käytetty laajasti kirjallisia lähteitä.

Teoreettinen tausta perustuu vuonna 1968 esiteltyyn **yleisen systeemiteoria**n (GST) malliin, jossa kaikille systeemeille voidaan osoittaa samankaltaisia ominaisuuksia. Tutkimus tarkastelee organisaatioita kybermaailmassa **avoimina vuorovaikuttavina systeemeinä**. Organisaatiot ovat kokonaisvaltaisia vakaaseen tilaan pyrkiviä monista elementeistä koostuvia vuorovaikuttavia systeemejä, joiden hierarkia muuttuu tulevaisuusriippuvaisesti uusia systeemejä luoden.

Kyberturvallisuus on eri toimijoiden ja toimintojen digitaalisuudesta ja verkottuneisuudesta aiheutuva turvallisuuden tila. **Kyberturvavalmius** tarkoittaa systeemin kompleksiseen kybertoimintaan valmistautumisen tasoa turvallisuusnäkökulmasta. **Eettinen hakkerointi** tarkoittaa tässä tutkimuksessa kyberturvavalmiuden selvittämistä – ei automaattisesti parantamista – testaamalla jonkin systeemin, kuten organisaation, kyberturvallisuutta pahaa tahtovien hakkerien käyttämillä menetelmillä luvallisesti ja laillisesti. Tutkimuksessa analysoidaan hakkeroinnin **käsite**, hakkeroinnin **menetelmät** ja organisaatioiden **toimet** kyberturvallisuuden testauksen jälkeen. Tärkeimpänä osana tutkimusta on selvitetty eettisen hakkeroinnin mahdollistamat menettelytapojen muutokset.

Hakkerointi voi olla hyvää tai pahaa ja teknistä tai sosiaalista. Eettisen hakkeroinnin vaiheet ovat tiedustelu, skannaus, haltuunotto, hallussapito ja raportointi. Sen vaikutukset kohdeorganisaatiossa perustuvat eettisen hakkeroinnin jälkeen valmistellussa raportissa ilmoitettujen kehitysehdotusten - haavoittuvuuksien ja menettelytapojen - muuttamiseen. Mahdolliset menettelytapojen muutokset ovat esimerkiksi kokonaiskuvan parantuminen, tavoitteellinen kehittäminen, prosessien laadun parantuminen, perusteet riittäville resursseille, kriittisten kohteiden tunnistaminen, mahdollisuuksien ja haavoittuvuuksien kartoittaminen, häiriötiloista toipuminen, yhteistyön kehittäminen, innovatiivisuus ja oppiminen sekä organisaatiokulttuurin ja toimijoiden asenteiden muutos.

Nykyään kyberturvallisuus on läsnä lähes kaikilla organisaatioiden toiminnan alueilla. Tämän takia ehdotetaan kyberturvallisuuden parantamiseksi **toimenpideohjelmaa**, johon kootaan edellä esitettyjen menettelytapojen avulla selkeät ja laaja-alaiset kyberturvavalmiutta parantavat keinot. Näin toimiva organisaatio olisi aiempaa kyberturvavalmiimpi ja hyödyttäisi itsensä lisäksi ympäröivää kyberriippuvaista yhteiskuntaa.



University of Tampere, Faculty of Natural Sciences
Degree Program in Computer Sciences
TASKINEN, SANTERI MIKAEL
Systems theory approach to ethical hacking
Master's thesis
61 pages + 2 pages of appendices
Master of Science degree
March 2018

This study answers the question of how ethical hacking practices can improve cyber security of organizations.

The research is based on a **qualitative** methodology theme interviews analysis of the cybersecurity professionals. The theme interviews were carried out in Winter 2016 at the Jyväskylä Cyber Security Convention. The interviewees were experts in ethical hacking and cyber security. Furthermore, research material has been widely collected from written sources.

The theoretical background is based on the **General System Theory** (GST) model presented in 1968, according to which all systems can be shown to have similar properties. The study views organizations in cyberspace as **open-interactive systems**. Organizations are holistic, multi-element interacting systems, which hierarchy is changing depending on the future and creating new systems at the same time.

Cybersecurity is a state of security derived from digital and networked nature of different actors and activities. **Cyber readiness** means the level of preparation for a complex cyber-based system from a security perspective. **Ethical hacking** means testing lawfully system cybersecurity - such as organizations - with the same methods used by evil-seeking "black hat" hackers. This study analyzes the concept of hacking, hacking methods, and organizational actions after cyber security testing. The most important part of the study is the means with which ethical hacking can change processes and bad practices in organizations.

Hacking can be good or bad and technical or social. The ethical hacking's five phases are reconnaissance, scanning, gaining access, maintaining access and reporting. Ethical hacking improvements on the target organization are based on the changes written in the development proposal (vulnerabilities and policies) reported in the last stage of ethical hacking. Possible changes in procedures include, for example, an overall image improvement, goal-oriented development, improved process quality, sufficient resources, identifying critical sites, mapping opportunities and vulnerabilities, faster recovering from disturbances, developing co-operation, innovating and learning, and changing organizational culture and attitudes.

Currently cybersecurity issues are present in all areas of virtual activity of organizations. As a result, is proposed a **program** to improve cybersecurity of organizations, which, by means of the above procedures, combines clear and wide-ranging means and ways to improve overall cyber readiness. The organization, as described above, would have better comprehensive view of cyberspace security and would benefit not only itself, but also surrounding cyber-dependent society.

Sisällysluettelo

1. Kybermaailma on hakkerien kehittelemä ... 1
2. Tutkimuksen menetelmävalinnat ... 5
3. Hakkeroinnin eettisyys ... 8
4. Eettinen hakkerointi kohdistuu systeemeihin ... 16
4.1. Yleinen systeemiteoria on työkalu eettisen hakkeroinnin tarkasteluun ... 16
4.1.1. Vakautuvuus ... 18
4.1.2. Tulevaisuusriippuvuus ... 19
4.1.3. Hierarkia ... 19
4.1.4. Kokonaisvaltaisuus ... 20
4.1.5. Jatkuva keskittyminen ... 20
4.1.6. Kasvaminen ja haje ... 21
4.1.7. Edistyvä segregaatio ... 21
4.1.8. Kilpaileminen ... 22
4.1.9. Itsenäistyminen ... 22
4.2. Systeemiteorian konsepti eettisessä hakkeroinnissa ... 23
4.3. Tutkimusteorian lähiteoriat ... 25
5. Eettinen hakkerointi käytännössä ... 26
5.1. Tutkimuksen empiiriset valinnat ... 26
5.2. Eettinen hakkerointi on turvallisuustestausta ... 27
5.3. Eettisen hakkeroinnin vaiheet ja menetelmät ... 27
5.3.1. Tiedustelu – tietojen kerääminen kohdesysteemistä ... 28
5.3.2. Skannaus – tiedon jäsentely ja jatkojalostus ... 30
5.3.3. Haltuunotto – systeemiin hyökkäys ... 31
5.3.4. Hallussapito – tavoitteiden saavuttaminen ... 33
5.3.5. Jälkien peittäminen tai raportointi ... 34
6. Aineistoanalyysi ... 36
6.1. Asiantuntijahaastattelut ... 36
6.2. Eettisen hakkeroinnin luonteesta ... 37
6.3. Eettisen hakkeroinnin menettelytavat organisaatioissa ... 39
6.4. Hakkeroinnin vaikutukset organisaatioihin ... 47
7. Tutkimustulokset ... 49
8. Johtopäätökset ... 53
8.1. Kybervalmis organisaatio on nykypäivää ... 53
8.2. Yhteiskunnan kyberturvallisuus koostuu systeemien kybervalmiuksista ... 54
8.3. Eettisen hakkeroinnin menettelytapojen tulevaisuus ... 55
Lähdeluettelo ... 57
Liitteet ... 62
Liite 1. Kvalitatiivinen teemahaastattelurunko asiantuntijoille ... 62
Liite 2. Haastattelussa käytetty teemaympyrä ... 63

1. Kybermaailma on hakkerien kehittelemä

Maapalloistuminen eli globalisaatio muuttaa käsitystämme maailman tilasta. Teknologisen kehittymisen nopeus näkyy jokaisen ihmisen henkilökohtaisessa elämässä. Globaali Internet, sähköiset palvelut ja nopea kommunikaatio ovat siirtäneet perinteisiä fyysisen maailman rakenteita ja prosesseja tietoverkkojen maailmaan. Uusi digitaalinen maailma poikkeaa monella tavalla totutusta fyysisestä maailmasta. Digitaalisen maailman toiminnot ovat aika- ja paikkariippumattomia. Maailman toisella puolella fyysisesti sijaitseva verkkokauppa on suomalaiselle avoinna ympäri vuorokauden, veroilmoituksen voi palauttaa kotona keskiyöllä ja töihin ei tarvitse välttämättä lähteä kotikonetta kauemmaksi. Ihmissuhteitakin voi kehittää virtuaalisesti ilman toisen ihmisen fyysistä tapaamista. Kaikki edelliset tapahtumat on mahdollistanut alun perin tehokkuuden parantamista varten kehitetty laaja ja nopea bittien maailma. Tätä uutta systeemien vuorovaikuttavaa kerrosta kutsutaan *kybermaailmaksi* ja sen aikaansaamaa prosessia *digitalisaatioksi*.

Kybermaailma ei kuitenkaan ole fyysisestä maailmasta erillinen kokonaisuus, vaan ne ovat limittyneet toisiinsa monin tavoin. Erilaiset kyber-fyysiset systeemit (engl. *cyber-physical systems*, *CPS*) ovatkin jatkuvassa vuorovaikutuksessa ja riippuvuussuhteissa keskenään (National Science Foundation 2016). Ajoneuvo- ja joukkoliikenteen, lääketieteen, terveydenhuollon, älykotien ja -rakennusten sekä sosiaalisten verkostojen ja pelaamisen järjestelmät ovat kaikki tällaisia. Edelleen kybermaailman kautta voidaan ohjata nykyisin suuriakin fyysisen maailman prosesseja. Älykkäät sähköverkot, datakeskukset, lämmönjaon ja kulunvalvonnan systeemit mahdollistavat nykyisin ihmisten arjen sujuvuuden. Toisaalta fyysisen maailman prosessit ovat yhä riippuvaisempia kybermaailman tapahtumista. Tällöin turvallisuuteen, häiriönsietokykyyn, luotettavuuteen, tietoliikenteen priorisointiin ja reaaliaikaisuuden vaatimuksiin kiinnitetään entistä enemmän huomiota. Tätä kompleksista teknologiseen kehittymiseen keskeisesti liittyvää ilmiötä voidaan kuvata ja ymmärtää yleisen systeemiteorian avulla. (Khaitan, McCalley 2015 ss. 4-10)

Globaali kybermaailma mahdollistaakin tehokkuuden kasvattamisen lisäksi täysin uusia toimintatapoja. Hyvämieliset hakkerit kehittelevät jatkuvasti kybermaailmaan uusia sovelluksia ja innovaatioita, jotka antavat elämällemme lisäarvoa. Alan Turing kehitteli vuonna 1937 laskennan matemaattisen mallin eli Turingin koneen (Lavington et al. 2012 s. 6, Cooper, van Leeuwen 2013 ss. 481-483).

Saksalainen Konrad Zuse puolestaan rakensi vuosina 1938-1941 maailman ensimmäisen Turing-täydellisen ohjelmoitavan Z3-tietokoneen (Rojas 1997 s. 6). Myöhemmin vuonna 1983 Richard Stallman kehitteli vapaan lähdekoodin periaatteen ja vuonna 1991 GNU-käyttöjärjestelmäkokonaisuuden yhdessä suomalaisen Linus Torvaldsin Linux-ytimen kanssa (Stallman 1983, Torvalds 1992, Canonical Ltd. 2016). Ydintä käyttävät jokaisen arjesta tutut Linux-, Android- ja Chrome-käyttöjärjestelmät (Zhou, Jiang 2012 s. 101, Google 2009). Kaikkien uusien sovelluksien käyttötavat eivät kuitenkaan ole kaikille systeemeille hyödyksi tai moraalisesti hyviä. Vallitsevat käsitykset oikeasta ja väärästä määrittelevät, millainen toiminta on moraalisesti hyväksyttävää. Vuoden 1988 marraskuun 2. päivänä yhdysvaltalainen Robert Tappan Morris ohjelmoi yhden ensimmäisistä Internetissä levinneistä madoista eli tietokonehaittaohjelmista nimeltään ”Morris-mato” (Rochlis, Eichin 1989). Madon aiheuttamista taloudellisista tappioista ja sekaannuksesta havaittiin kybermaailman synkempi puoli (Seeley 1989 ss. 696-698). Toisaalta kybermaailmassakin helpoimmat hakkeroinnin kohteet ovat yleensä ihmisiä. Tätä tietoa käytti hyväkseen Kevin Mitnick, joka tunnetaan sosiaalisen hakkeroinnin eli ihmismielen huijaamisen taidokkaasta käyttämisestä (Gots 2016). Etiikka voi antaa vastauksia siihen, millainen toiminta uudessa kybermaailmassa on hyvää ja mikä pahaa – oikeaa ja väärää. Tästä hakkeroinnissa on eettisesti tarkasteltuna kysymys.

Kuten edellä esitettiin, kaikki kybermaailman tapahtumat eivät ole organisaatioille myönteisiä. Organisaatiot koostuvat ihmisistä. Motivoitumisen ja organisaatioiden toiminnan edellytyksenä ovat ihmiselle ominaiset psykologiset tarpeet. Maslow’n tarvehierarkia järjestää psykologiset perustarpeet tärkeimmästä vähiten tärkeimpään. Teorian mukaan jokainen edeltävä perustarpeiden taso on täytettävä ennen mahdollisuutta siirtyä seuraavalle tasolle. Ensimmäinen perustaso sisältää ihmiselle ominaiset fysiologiset perustarpeet, kuten aineenvaihdunnan, ruoan, veden, unen ja seksuaaliset mielihalut. Jo toinen perustaso käsittää turvallisuuden tarpeet ja pitää sisällään fyysisen ja henkisen turvallisuuden eli uhkien ja vaarojen poissaolon sekä mahdollisuudet kehittymiseen (Virta 2011 s. 121). Vasta kolmannella tasolla on organisoitumisen ja organisaatioiden olemassaolon edellytyksen täyttyminen: yhteenkuuluvuuden, ryhmään kuulumisen ja rakkauden tarpeet. Ihmisen turvallisuuden tarpeiden onkin täytyttävä organisaatioiden syntymisen edellytyksenä. Myös organisaation tapaisilla ihmisistä koostuvilla systeemeillä on olemassaolonsa turvaamiseksi tarve turvalliseen toimintaympäristöön. Edellä esitelty kybertoimintaympäristö ei tee tästä kyber-fyysisenä systeeminä poikkeusta. (Maslow 1943 ss. 372-385)

Pahaa tahtovat hakkerit pyrkivät hyödyntämään nopeaa kybermaailman kehittymistä omien tavoitteidensa täyttämiseen. Motivoivia tekijöitä voivat olla esimerkiksi näyttämisen halu, rahallinen hyöty tai poliittinen ideologia (Manion, Goodrum 2000 s. 17). Pahamieliset hakkerit eivät toimi aina yksin. Erilaiset verkostot, organisaatiot ja jopa valtiolliset toimijat saattavat tukea pahamieleisiä hakkereita ja käyttää Internetiä aseenaan. Esimerkiksi Yhdysvalloilla, Kiinalla, Venäjällä ja monilla muilla mailla on oma kyberarmeijansa, joka valmistautuu tarvittaessa käyttämään kaikkia mahdollisia kybermaailman keinoja tavoitteidensa täyttämiseen (National Security Agency 2016, Clarke, Knake 2011 s. 6). Toisaalta organisaatioiden toimintaedellytyksiä heikentävistä tekijöistä kaikki eivät ole suoraan ihmisen aiheuttamia. Esimerkiksi luonnonkatastrofit, fyysiset laiterikot ja koneiden tekemät virheet ovat tällaisia. Edellä mainitut ovat organisaatioiden vakaata tilaa eli hyviä toimintaedellytyksiä horjuttavia uhkia tekijätahosta riippumatta. Niiden hallitseminen ja ennaltaehkäisy muodostavat systeemien turvallisuusmenettelytavat. Kyberuhkien tunnistamisen yksi keino on eettinen hakkerointi, mutta se ei yksinään riitä. Tarvitaan uusia prosesseja ja rakenteita, joilla kyberturvavalmiuden taso paranee tehtyjen eettisten hakkeroinnin selvitysten jälkeen. Muutokset organisaatioiden menettelytavoissa ratkaisevat kyberturvavalmiuden todellisen tason (Beaver 2013 s. 23).

Eettisen hakkeroinnin menettelytapojen tutkimuksen ajankohtaisuus näkyy myös ihmisten arkipäiväisessä elämässä. Syyskuussa 2016 laskettiin liikkeelle Mirai-haittaohjelma, joka muutti kuluttajien omat etäohjattavat kamerat ja reitittimet osaksi isoa hajautettuihin palvelunestohyökkäyksiin (DDoS) käytettävää kaapattujen tietokoneiden verkkoa eli bottiverkkoa. Toisaalta samaa haittaohjelmaa käytettiin myös Internetin kriittistä puhelinluetteloa eli nimipalvelujärjestelmää vastaan tehdyissä iskuissa. Tämän seurauksena Twitterin, Netflixin, Spotifyn ja useiden verkkosivustojen käyttö oli ajoittain mahdotonta myös Euroopassa. Kuluttajaelektroniikan uhkakuvat ovat olleet tiedossa jo pitkään. Miksi puutteita ei kuitenkaan ole todellisuudessa korjattu? (Kerola 2016)

Otetaan esimerkiksi teknologiateollisuuden yritys, jonka keskeinen liiketoiminta-alue on ohjelmistojen myynti ja digitaalinen palvelutoiminta. Mitä tapahtuisi, jos kyberuhka toteutuisi ja yrityksen liiketoiminnan perusta eli ohjelmakoodit tai tärkeät dokumentit varastettaisiin tai vuodettaisiin? Millaisia vaikutuksia olisi muutaman päivän tietojärjestelmien alasajolla? Salailtaisiinko tapahtunutta? Kuinka suuret taloudelliset tappiot olisivat? Millainen imago- ja luottamustappio tällaisesta

yksittäisestä mediassa vellovasta tapauksesta aiheutuisi? Tällaisiin kysymyksiin voidaan joutua vastaamaan, mikäli organisaation kyberturvallisuudesta ei ole huolehdittu tarpeeksi ja menettelytapoja kehitetty toimintaympäristön muuttuessa.

Kybermaailma onkin hyvin kompleksinen systeeminen kokonaisuus, jossa kyberturvallisuuden kokonaisvaltaisia keinoja tarvitaan kyberturvavalmiuden parantamiseksi. Jatkuva tutkimus luo uusia käsitteitä, jotka voivat olla aiheeseen perehtymättömälle vaikeita ymmärtää. Tämän tutkimuksen tavoitteena onkin käsitellä aihetta selkeästi käsitteidenmäärittelyiden, esimerkkien ja ratkaisukeskeisen aiheen jäsentelyn keinoin.

2. Tutkimuksen menetelmävalinnat

Tietojenkäsittelytieteelliselle tutkimukselle on tyypillistä pyrkiä löytämään uutta tietoa systeemien toimintatavoista (March, Smith 1995 s. 251). Uuden tiedon tuottamiseksi on täytynyt tutkimuksen aihe operationalisoida tutkimuskysymykseksi (Saukkonen 2011). Tässä tutkimuksessa tutkimuskysymyksen muodostamisessa on käytetty apuna eettisen hakkeroinnin aiheanalyysia ja kirjallisuuskatsausta, joiden pohjalta on muotoutunut eettisen hakkeroinnin menettelytapoja ja vaikutuksia korostava tutkimuskysymys:

Miten eettisen hakkeroinnin menetelmillä vaikutetaan organisaatioiden kyberturvallisuuteen?

Tutkimuskysymys koostuu kahdesta osasta: 1. eettisen hakkeroinnin menetelmistä eli keinoista tuottaa eettistä hakkerointia ja 2. organisaation menettelytavoista eli muutoksista prosesseissa ja rakenteissa eettisen hakkeroinnin pohjalta. Tutkimuskysymyksen selvittämiseksi on välttämätöntä tietää, mitä eettisen hakkeroinnin menetelmiä on olemassa ja miten niitä voidaan käyttää. Menetelmä tarkoittaa tässä tutkimuksessa toimia ja tapoja jäljitellä pahamielisten hakkerien toimintaa sekä löytää kyberturvallisuuden kehityskohteita. Edelleen on ymmärrettävä, mihin menetelmiä käytetään ja mihin niillä pyritään. Lisäksi on ensiarvoista tietää, vaikutetaanko saaduilla tiedoilla organisaation kyberturvallisuuden tasoon.

Tutkimuksen tavoite on tuottaa uutta tietoa eettisen hakkeroinnin menettelytapojen vaikutuksista organisaatioissa. Tähän on pyritty analysoimalla aiempaa lähdekirjallisuutta ja tuottamalla omaa tutkimusaineistoa. Uutta tietoa on pyritty löytämään järjestelemällä jo olemassa olevaa aineistoa ja jäsentelemällä organisaatioiden eettisen hakkeroinnin menettelytapoja.

Turvallisuus- ja kybertutkimuksen aihealueen laajuuden vuoksi tutkimuksen *rajaaminen* on ollut välttämätöntä. Tämä tutkimus ei syvenny minkään erillisen organisaatiotyypin kyberturvallisuuden menettelytapoihin. Pyrkimyksenä on ollut käsitellä kyberturvallisuutta yleisesti ja systeemilähtöisesti konkreettisia esimerkkejä käyttäen. Esimerkkien tarkoitus on auttaa lukijaa ymmärtämään kompleksista kybermaailmaa. Tässä tutkimuksessa ei myöskään syvennytä yksittäisiin hakkeroinnin teknologisiin menetelmiin, sillä se ei olisi tutkimuksen laajuuden kannalta mahdollista. Teknisiä menetelmiä kuitenkin esitellään tarpeen mukaan asioiden konkretisoimiseksi yleisellä ja ymmärrettävällä tasolla. Tämän tutkimus keskittyy kaikkiin organisaatioihin yleistettävien eettisen hakke-

roinnin menettelytapojen tutkimiseen ja niiden hyötyjen tai haittojen selvittämiseen. Tarkoitus onkin osittain nähdä jatkuvasti muuttuvan teknologisen kuoren läpi ja ymmärtää kybermaailmassa vaikuttavien systeemien toimintaa ja kyberturvallisuuden ominaisuuksia.

Tieteenfilosofialtaan tämä tutkielma on tietojenkäsittelytieteiden ja yhteiskuntatieteiden filosofioiden mukainen. Tämä johtuu tutkimuksen aiheesta, joka yhdistää organisaatioiden, eettisen hakkeroinnin ja ihmisten toiminnan tutkimusta. Tietojenkäsittelytieteiden perinteinen filosofinen näkökulma on ollut loogisen sovelletun päättelyn mukaiset ajattelutavat. Tässä tutkimuksessa tieteenfilosofinen pohja on kuitenkin tietojenkäsittelytieteissä uudemman eli tietojenkäsittelyn etiikan sovelluksien, kuten kyberturvallisuuden, hakkeroinnin ja yhteiskunnan muodossa. Edellä esitellyn filosofisen suuntauksen kehittymiseen ovat vaikuttaneet muun muassa yhteiskunnan kyberriippuvuuden kasvaminen ja ubiikin laskennan eli kaikkialle sulautuvan tietotekniikan yleistyminen (Tietotekniikan termitalkoot 2000). (Colburn 2015 ss. 3-4)

Tässä tutkimuksessa on käytetty *päättelymallina* loogista induktiota (*lat. in+duco*, johtaa tai ohjata sisään) eli yleistämistä, jossa yksittäisistä havainnoista voidaan tehdä rajallisia johtopäätöksiä (Korkman, Yrjönsuuri 1998, s. 449). Lisäksi tutkimus on pääosiltaan deskriptiivinen eli kuvaileva tutkimus, joka näkyy muun muassa esimerkkien määrässä. Tutkimuksen päättelymalli koostuu tietojen kokoamisesta ja niiden analysoinnista. Toisaalta mukana on myös uutta tietoa ja päätelmiä, joiden tarkoituksena on parantaa ja kehittää organisaatioiden kyberturvallisuuden tasoa. Tästä näkökulmasta tutkimuksessa on myös hieman normatiivisia eli ohjaavia analyyseja. Tieteellisillä käsitteillä ja väittämillä voidaan selittää jonkin ilmiön olemusta. Tieteellistä selittämistä puolestaan tarvitaan, sillä halutaan saada vastauksia tieteellisiin kysymyksiin. Selittämisen tarkoituksena on tuottaa tutkimuskohteesta tietoa ja ennustaa sen kehitystä. (Routio 2006)

Menetelmätieteellisesti eli metodologisesti ja *aineistollisesti* tämä tutkimus on kvalitatiivinen puolistrukturoituihin teemahaastatteluihin perustuva sitaattianalyysi. Lisäksi aiempaa tutkimuskirjallisuutta on käytetty teoreettisen ja empiirisen aineiston keräämiseen. Teemahaastattelut on valittu tutkimuksen tiedonkeruumenetelmäksi, sillä eettisen hakkeroinnin kirjoittamattomista säännöistä ja vaikutuksista organisaatioihin on suhteellisen vähän aiempaa tutkimusta. Teemahaastattelu sopii

tutkimusmenetelmänä aihealueisiin, joiden ilmiöistä ja asioista on vähemmän tunnettua tietoa. Tutkimuksessa viitattu kirjallisuus on koostunut pääasiassa vertaisarvoiduista tieteellisistä julkaisuista, kirjoista ja verkkosivuista. Lähteiden valinnassa on noudatettu lähdekritiikkiä.

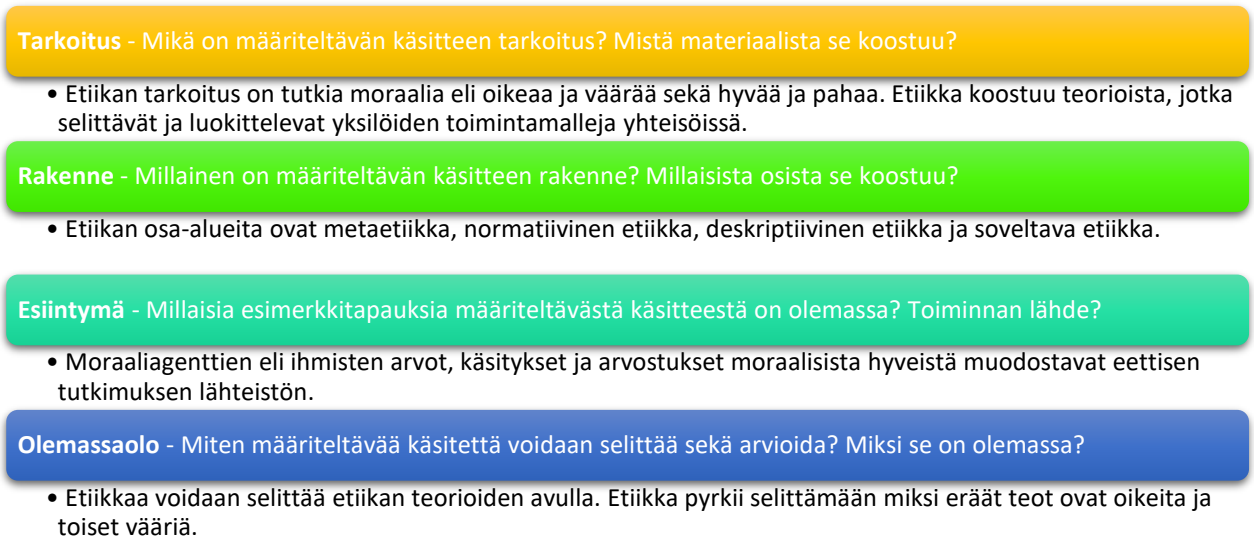
Tutkimuksen kvalitatiivinen eli laadullinen tutkimusmenetelmä on perusteltu aihealueen laajuuden ja vaikean määrällisen mitattavuuden vuoksi. Kvalitatiivisen menetelmän laajuus ja monimuotoisuus on asettanut haasteen, joka on otettu huomioon tutkimusprosessin aikana selkeillä metodologisilla ja aineistollisilla valinnoilla. Aineiston analyysiä ja tulkintoja korostamalla on voitu tutkimuksen uutta tietoa ja tuloksia tuottavia osia käsitellä enemmän (Saaranen-Kauppinen, Puusniekka 2006).

Teoreettinen viitekehys pohjautuu tässä tutkimuksessa yleiseen systeemiteoriaan, jota käytetään jäsentelemään ja selkeyttämään eettisen hakkeroinnin menettelytapojen tarkoitusta, tarvetta ja toimintaperusteita. Yleisellä systeemiteorialla tuetaan havaintoja, joita tutkimuksen aineistonhankintamenetelmillä on löydetty. Yleistä systeemiteoriaa on käytetty aiemminkin tietojenkäsittelytieteissä esimerkiksi tietokonejärjestelmien informaatioturvallisuuden matemaattisessa tutkimuksessa (Bell, LaPadula 1973 s. IV). Teorian valintakriteerinä on ollut laaja soveltuvuus systeemeihin, monitieteellisyys sekä avoimien ja vakaata tilaa tavoittelevien systeemien periaate, joka sopii hyvin organisaatioiden eettisen hakkeroinnin menettelytapojen tutkimukseen. (von Bertalanffy 1968 s. 39,48,54)

Tutkimuksen ensimmäisen osan (luku 1) muodostaa johdanto, jossa johdatellaan lukija aihealueeseen. Tutkimuksen toinen osa (luku 2) sisältää tutkimustehtävän, metodin, aineistonhankintamenetelmät ja tutkimusfilosofian. Kolmas osa (luku 3) esittelee tutkielmassa käytetyt keskeiset käsitteet ja pohtii hakkeroinnin eettisyyttä laajasti eri näkökulmista. Neljännessä luvussa (luku 4) syvennytään tutkimuksen teoreettiseen taustaan ja selitetään eettisen hakkeroinnin menettelytavat yleisen systeemiteorian avulla. Viidennessä luvussa (luku 5) käsitellään empiirinen tutkimustieto eettisen hakkeroinnin vaiheittaisista teknisistä ja sosiaalisista menetelmistä kirjallisuuslähteiden mukaan. Asiantuntijahaastatteluiden analyysi esitetään tutkimuksen kuudennessa osassa (luku 6). Tutkimuksen seitsemäs osa (luku 7) sisältää yhteenvedon koko tutkimuksen tuloksista ja tarkastelee teorian sopivuutta tutkimuksen aihepiiriin. Johtopäätöksiin, pohdintaan ja tietojenkäsittelytieteelliseen sekä yhteiskunnalliseen lisäarvoon keskitytään tutkielman päättävässä osassa (luku 8). Samalla pohditaan eettisen hakkeroinnin kiinnostavia uusia tutkimuskohteita.

3. Hakkeroinnin eettisyys

Käsitteitä on käytetty tiedon jäsentämiseen jo kauan (Tieteen termipankki 2014). Aristoteles (*Aristotélēs*, 384-322 eaa.) esitti aikanaan näkemyksen, jonka mukaan tietämyksen lisäämiseksi on kyettävä vastaamaan neljästä näkökulmasta ”miksi?”-kysymykseen (Falcon 2016). Kysymyksen vastauksella on kyettävä selittämään ilmiön, tiedon tai olion tarkoitusta, rakennetta, esiintymiä sekä olemassaoloa (Ross 2014 ss. 634-636, Sachs, Aristotle 1995 ss. 53-56). Tietämyksen lisäämiseksi on ilmiötä, tietoa tai oliota jäsentelevää käsitettä selitettävä edellä mainittujen käsitepiirteiden – näkökulmien ja syiden – kautta (Lavonen, Meisalo 2013, Tieteen termipankki 2014). Määrittelyprosessissa on tiedostettu teleologinen käsitteiden muutoksen mahdollisuus: millainen tila käsitteellä on nykyhetkessä (aktuaalisuus) ja millaiseksi se voi muuttua tulevaisuudessa (potentiaalisuus). Esimerkiksi nykyinen hakkeri (aktuaalisuus) voi tulevaisuudessa olla verkkorikollinen tai laillinen penetraatiotestaaja (potentiaalisuus). Tämän tutkimuksen käsitteenmäärittelyissä on käytetty edellä esitettyä ja tieteellisesti koeteltua käsitteiden määrittelymallia. Kuvassa 1 on esitetty etiikan käsitteen määrittelyn näkökulmat. Samaa määrittelymallia on käytetty kaikkien käsitteiden osalta. Seuraavaksi operationalisoidaan tutkimuksen aiheen kannalta keskeisimmät käsitteenmäärittelyt.



Kuva 1. Etiikka-käsitteen määrittely neljän näkökulman avulla mukaellen Aristotelesta.

Etiikkaa (kreik. ἠθική ēthos = vakiintuneet tavat, luonne (Tieteen termipankki 2016a 'etiikka')) on käsitelty tutkimuskirjallisuudessa karkeasti neljästä eri näkökulmasta. Yhtäältä etiikalla tarkoitetaan erilaisia arvojen järjestelmiä – arvoja loogisina kokonaisuuksina (Haarala et al. 2016, moraali) – yk-

silöiden muodostamissa yhteisöissä. Toisaalta etiikalla voidaan viitata myös moraalisuuteen eli yhteen yhteisöjen monista arvojärjestelmistä. Tällöin etiikka tarkoittaisi yhteisöissä vallitsevia käsityksiä, arvostuksia ja käyttäytymissääntöjä (Haarala et al. 2016, etiikka). Kolmannesta näkökulmasta etiikka on synonyymi **moraalille** eli yksilön eri elämäntilanteissa tekemille käytännön valinnoille tai toimintamalleille, jotka voivat olla hyviä tai pahoja – oikeita tai vääriä. Teko on moraalinen vain, jos sen tekijällä eli niin sanotulla **moraaliagentilla** on kyky ja mahdollisuus harkintaan erilaisten vaihtoehtojen välillä, eikä yksilö ole pakkotilanteessa (Opetushallitus 2009). Neljänneksi etiikka on filosofian osa-alue ja tiede, joka tutkii moraalia ja etiikan suhteita muihin filosofian osa-alueisiin. (Crisp 1998)

Aristoteles esitti, että eettisen tutkimuksen tarkoituksena on selvittää ihmisen luonnetta ja sen hyveitä (Aristotle 1999, 1098a). Sen mukaan jokainen ihminen pyrkii järkevien ja hyvien johtopäätösten avulla onnellisuuteen. Tämä näkyisi esimerkiksi hyvien hakkerien onnellisempana elämänä pahoihin hakkereihin verrattuna. Länsimaalaisen filosofian tutkimuksessa etiikka on kuitenkin pikemminkin oppia moraalisista hyveistä. Tämän käsityksen mukaan etiikan tehtävänä olisi tutkia moraalia ja selittää moraalisia ilmiöitä teorioiden avulla. Tätä filosofista suuntausta kutsutaan myös nimellä **moraalifilosofia** (Pietarinen 2015). (Crisp 1998, Tieteen termipankki 2016a 'etiikka')

Nykyään etiikka on jaettu neljään eri osa-alueeseen, suuntaukseen tai tavoitteeseen: metaetiikkaan, normatiiviseen etiikkaan, deskriptiiviseen etiikkaan ja soveltavaan etiikkaan (Kimppa 2016). **Metaetiikka** tutkii etiikan teoreettisia perusteita ja käsitteitä, eikä niinkään käytännön sovelluksia, kuten eettisen hakkeroinnin oikeita menettelytapoja. Metaetiikalla on perinteisesti voitu määritellä esimerkiksi käsitteitä hyvä, paha ja moraali. (Blackburn 2016, Martin 2016)

Normatiivinen etiikka puolestaan perustuu teorioihin, joiden mukaan on olemassa yksittäinen sääntö tai joukko periaatteita, joiden mukaan kaikkien ihmisten ja systeemien tulisi elää ja toimia. Tämän pääperiaatteen avulla voitaisiin ratkaista kaikki moraalifilosofian kysymykset siitä, onko jokin teko – esimerkiksi murtautuminen toisen tietojärjestelmään sen turvallisuuden parantamiseksi – eettisesti oikea vai väärä menettelytapa. Eettinen ajattelu on normatiivista, jos pyritään ratkaisemaan, onko jokin teko moraalisesti oikein vai väärin. Eräs erittäin tunnettu esimerkki normatiivisen etiikan periaatteesta on niin sanottu *Kultainen sääntö* (Fieser 2016, Wattles 1996 s. 3):

Tee toisille niin, kuin haluaisit itsellesi tehtävän.

Tätä sääntöä ovat opettaneet lähes kaikki maailman uskonnot muodossa tai toisessa. Periaate sopii myös maallisen normatiivisen etiikan perusajatukseksi (Wattles 1996 s. 4). Toisaalta Kultaisen säännön soveltaminen käytännön tilanteisiin on ollut ajoittain vaikeaa ja jopa moraalisesti ristiriitaista (Neusner, Chilton 2008 s. 4). Tästä huolimatta hakkeroinnin eettisyyttä voidaan vähintään arvioida erilaisten normatiivisten teorioiden avulla. Normatiivisen etiikan teoriat luokitellaan velvollisuusetiikkaan, seurausetiikkaan ja hyve-etiikkaan (Fieser 2016). Kaikilla näistä suuntauksista on oma käsityksensä hakkeroinnin hyvyyden ja pahuuden rajoista.

Deskriptiivinen etiikka kuvailee ihmisten oikeaa ja väärää koskevia erilaisia käsityksiä ja ajatuksia moraalista. Eräs deskriptiivisen etiikan kysymys on: Mikä on sinun mielestä oikein ja mikä väärin? Tässä etiikan haarassa on kyse moraaliagenttien eli ihmisten omien moraalisten valintojen tutkimisesta. Eettisen hakkeroinnin menettelytapojen osalta voi jokaisella organisaation muodostavalla ihmisellä olla oma käsitys oikeista ja vääristä toimintatavoista. Nämä käsitykset yhdessä muodostavat eettisen hakkeroinnin toimintatavat organisaatioissa. (Kärkkäinen 2016)

Soveltava etiikka tarkoittaa moraalisesti kiistanalaisen asian analysoimista etiikan teorioiden avulla. Jotta tapaus, teko tai toiminta kuuluisi soveltavan etiikan tutkimusalueeseen, tulee kaksi seuraavaa ehtoa täyttyä (Fieser 2016):

1. Moraalinen kiistanalaisuus: asiaa pitävät hyvänä sekä huonona merkittävät ihmisjoukot.
2. Moraalikysymys: sama kysymys on eri näkökulmista moraalisesti oikein ja väärin.

Sovelletussa etiikassa pyritään normatiivisen etiikan teorioilla selittämään arkipäivän tilanteiden moraalista puolta (Pietarinen 2015, Fisher 2014 ss. 1-2). Seuraavassa käsiteltävä hakkerointi on tästä hyvä esimerkki: hakkeroinnin tavoite määrää sen hyvyyden tai pahuuden. Toisaalta ensimmäisen ehdon mukaan eettisesti hyvää tavoitteleva hakkerointi ei edes olisi eettinen kysymys, koska luvallista hakkerointia pidetään laajasti ja yleisesti hyvänä asiana. Tässä tutkimuksessa etiikka tarkoittaa tiedettä, joka tutkii hyvää ja pahaa sekä oikeaa ja väärää. Tutkimuksessa etiikkaa tarkastellaan soveltavan etiikan näkökulmasta.

Hakkerointi (engl. *hacking*) on käsitteenä monimuotoinen ja sillä on ollut historiansa aikana erilaisia käyttötarkoituksia (Haarala et al. 2016, hacking). Hacking-sana on todennäköisesti johdettu *hack*-sanasta, joka 1300-luvulla on tarkoittanut paloitteluun tarkoitettua työsuoritetta tai työkalua, kuten kuokkaa tai hakkua (Oxford English Dictionary 2016).

1600-1700-luvuilla englannin kielessä *hack*-sanalla on viitattu *hackney*-sanaan, joka on tarkoittanut keskikokoista ja tavallista vuokravaunujen vetämiseen tarvittavaa hevosta. 1800-luvulla *hack*-sanalla alettiin tarkoittaa vuokrattavien hevoskärryjen sijasta vuokrattavaa ajoneuvoa yleisesti. Nykyenglannissa *hack*-sanalla on monia merkityksiä. Sitä käytetään edelleen englannin slangisanana taksille tai taksinkuljettajalle, mutta se voi viitata myös kehen tahansa tavallista vuokratyötä tai rutiinityötä tekevään tai itse rutiinityöhön. Erään käsityksen mukaan se viittaisi myös kirjoituskoneen kirjoittajan painikkeita ”hakkaavaan” eli rutiininomaisen leipätyön tekemiseen. *Hack*-sanan määritelmä viittaakin tässä yhteydessä usein perusideaan, rutiiniin tai normaaliin menettelytapaan. Tämä ei kuitenkaan tarkoita, että *hack* olisi alkuperäinen tapa toimia, vaan pikemminkin amatöörimäinen, kömpelö ja suorittava menettelytapa. Tällä on voinut olla vaikutusta hakkerointi-sanan kehityksessä. (Merriam-Webster 2016a)

Tietojenkäsittelyn näkökulmasta todennäköisempi selitys hakkerointi-sanan kehittymiselle on tapahtunut 1950-luvulla Massachusettsin teknillisessä korkeakoulussa (MIT). Koulun paikallinen pienoisrautatiekerho (TMRC) sai laitelahjoituksen, joka sisälsi vanhoja lankapuhelinlaitteistoja. Kerhon jäsenet rakensivat niistä monimutkaisen ohjausjärjestelmän, jonka avulla useampi henkilö kykeni samaan aikaan kontrolloimaan monta pienoisrautatien rataosaa soittamalla eri rataosien numeroihin. Kerhon jäsenet kutsuivat työtään hakkeroinniksi. Kerho esittikin vuonna 1959 humoristisen standardiluettelon, jossa *hack* määriteltiin toiminnaksi, jolla A) ei ole rakentavaa loppua B) johon on ryhdytty itsenäisesti tai C) joka lisää epäjärjestyksen määrää systeemissä (Samson 1959). Moni TMRC-pienoisrautatiekerhon jäsen siirtyi 1960-luvulla ohjelmoimaan reikäkorteille tai lennätinnauhoille ensimmäisten tietokoneiden avulla. Todellisina hakkereina pidettiin henkilöitä, jotka pystyivät toteuttamaan ohjelmallisesti saman toiminnallisuuden pienemmällä reikäkorttimäärällä tehokkaammin ja paremmin. Tällä perusteella ratkaisu (*hack*) on tarkoittanut normaalista poikkeavaa me-

nettelytapaa tai kokeilua, jonka hakkeri (*hacker*) on tehnyt. Hakkerointi (*hacking*) puolestaan on tarkoittanut teknisen laitteen tai menetelmän – esimerkiksi ohjelmiston – muuntelua taidokkaalla tai fiksulla normaalista poikkeavalla tavalla. (Erickson 2003 ss. 1-2)

Mediassa on jo pitkään käytetty hakkeri (vrt. krakkeri) sanaa moraalisesti paheksuttavissa yhteyksissä, jolloin sanalle on muodostunut automaattisesti negatiivinen konnotaatio: ”Näin hakkeri murtautui ja miten sen olisi voinut estää – 3 tositapausta” (Helsingin Sanomat 2014). Tässä yhteydessä hakkerilla on viitattu murtautujaan tai rikolliseen ja sitä on käytetty krakkeri-sanan sijasta, jolloin termit ovat sekoittuneet. **Krakkeri** (engl. *cracker*) tarkoittaa murtautujaa, joka tunkeutuu luvatta suojattuun systeemiin – esimerkiksi tietojärjestelmään. Tässä tutkimuksessa **hakkeri** voi olla myös ainoastaan innokas järjestelmien ja systeemien tutkija tai harrastaja, joka keksii erilaisia ratkaisuja asioihin ja nauttii niiden tekemisestä. (Valtionvarainministeriö 2009 s. 31,53, Malkin, Parker 1993 s. 11,21, Shirey 2000 s. 45,78, Taylor 1999 ss. 15-16)

Edellä osoitettu tapa käyttää hakkeri-sanaa moraalisesti paheksuttavin keinoin toimivasta systeemien tuntijasta ei ole täysin väärä, sillä hakkereita jaetaan nykyisessä tutkimuksessa monin eri tavoin. Tutkimuskirjallisuudessa ”hakkeri” on laaja yleiskäsite, joka kuvaa enemmänkin taitoa tai innostuneisuutta erilaisten systeemien toiminnasta kuin syyllisyyttä rikoksiin tai eettisesti ja laintulkinnallisesti arveluttaviin tekoihin. Hakkerointi voi olla keino uusien tavoitteiden saavuttamiseen. Tavoitteet määräävät, onko hakkerointi hyvää vai pahaa. Hakkereita voidaan jakaa esimerkiksi seuraavalla tavalla (aluksi moraalisesti kiistanalaisimmat) (Graves 2010 s. 4):

- **Harmaahattu** (*engl. grey hat*): hakkeri, joka käyttää taitojaan tahtonsa mukaan tilannekohtaisesti. Harmaahattu ei toimi aina luvallisesti tai laillisesti, mutta toimii moraalisesti oikein. Etiikan tehtävä on selvittää, mikä on missäkin tilanteessa oikein ja väärin. Esimerkiksi systeemeistä kiinnostunut amatööri tai harrastelija voi olla harmaahattu.
- **Mustahattu** (*engl. black hat*): hakkeri tai krakkeri, joka toimii ilkeästi tai pahamielisillä tarkoitusperillä, hyökkäävästi. Toimintaan kuuluu haitan aiheuttaminen, tiedon tuhoaminen ja palvelunestot ilman kohteen lupaa tai laillisuutta.
- **Valkohattu** (*engl. white hat*): hakkeri, joka käyttää taitojaan puolustaviin tarkoituksiin. Valkohattu hakkeroi systeemiä aina luvallisesti ja laillisesti. Esimerkiksi organisaation turvallisuusasiantuntija voi olla valkohattu.

Hakkerin määrittelyssä on otettava huomioon kolme asiaa: tavoite, luvallisuus ja motivaatio (Engebretson 2013 s. 3). *Harmaahattuhakkerin* toiminta on eettisen pohdinnan kannalta kaikkein kiinnostavinta, sillä päätökset tehdään itsenäisesti ja moraalilla on suuri rooli päätöksenteossa. Harmaahatun tavoitteet ovat lähtökohteisesti moraalisesti hyviä, mutta eivät välttämättä laillisia, luvallisia tai kohdeorganisaation näkökulmasta hyväksyttäviä. Harrasteleva hakkeri, joka testaa oman paikallispankkinsa kyberturvamekanismeja pitääkseen omat ja muiden rahat paremmin tallessa, on eräs esimerkki harmaahatuille tyypillisestä toiminnasta.

Mustahattuhakkeri, joka hyökkää johonkin systeemiin, ei välttämättä ole eettisesti tarkasteltuna paha. Kybertaistelija eli kybermaailmassa toimiva sotilas on tästä hyvä esimerkki: hyve-etiikan näkökulmasta isänmaallisuus ja oman valtion puolesta toimiminen olisi moraalisesti oikein ja hyvä asia, vaikka keinot olisivatkin hyökkääviä tai toisille haittaa aiheuttavia. Mustahattuhakkeri voidaankin tavoitteiden ja kontekstin avulla määritellä yleisesti tuomituista keinoistaan huolimatta moraalisesti hyväksi toimijaksi. Toisaalta seurausetiikkaan kuuluvan utilitarismin näkökulmasta teon moraalinen hyvyys määräytyy teon vaikutuspiirissä olevien tahojen hyötyjen perusteella. Tällöin sama kybertaistelija toimisi moraalisesti väärin tehdessään pahaa vastaosapuolelle. Monet etiikan periaatteista ovatkin hieman ristiriitaisia keskenään. Yleinen esimerkki mustahattuhakkerista on verkkorikollinen, joka hakkeroimalla tavoittelee omaa hyötyä muiden kustannuksella tuhoista välittämättä. (Mill 1863 s. 16)

Valkohattuhakkerit ovat laillisia systeemien kehittäjiä ja turvallisuusasiantuntijoita. Valkohattujen asiantuntemus on haluttua työmarkkinoilla (Caldwell 2011). Tämä johtuu verkottuneisuuden ja tietoteknistymisen lisääntymisestä, jolla on voitu kasvattaa globaalia tuottavuutta. Samalla myös riskit kybermaailmassa ovat kasvaneet, kun mustahatut ovat oivaltaneet verkkohyökkäyksien arvon. Toisaalta myös tietoisuus mustahatuista on kasvanut yleisen kyberkiinnostuksen kasvaessa. (Libicki, Senty & Pollak 2014 ss. 1-7)

Eettinen hakkerointi (engl. *ethical hacking*) tarkoittaa tässä tutkimuksessa kyberturvavalmiuden selvittämistä – ei automaattisesti parantamista – testaamalla jonkin systeemin, kuten organisaation, kyberturvallisuutta pahamielisten hakkerien käyttämillä menetelmillä luvallisesti ja laillisesti. Kä-

sitteen sana ”eettinen” viittaa moraalisesti hyvään ja oikeaan toimintaan, vaikka etiikka tieteenä tutkii myös pahaa ja väärää. Eettinen hakkerointi ei ole tosiasiassa etiikan kannalta mielenkiintoinen kysymys, sillä sitä pidetään yleisesti hyväksyttävänä ja hyvänä kyberhaavoittuvuuksien kartoitusmenetelmänä.

Hyvän hakkeroinnin eli eettisen hakkeroinnin päämääränä on löytää systeemien rakenteista eli osista ja prosesseista kehityskohteita ja haavoittuvuuksia. Eettinen hakkerointi on kuitenkin vain tarkistus: eettinen hakkerointi ei itsessään korjaa mitään rakenteita tai prosesseja systeemeissä. Eettisen hakkeroinnin voikin rinnastaa selvitykseen, jonka tekemisen päämääränä on tulevien toimenpiteiden suunnittelu ja kartoitus. Varsinaisia vaikutuksia kohdesysteemeissä saadaan aikaan vasta testauksen tulosten hyödyntämisen jälkeen. Näitä hyödyntämisen menettelytapoja ja eettisen hakkeroinnin käsitettä on analysoitu lisää luvussa 4.

Kyberturvavalmius (engl. *cyber readiness*) tarkoittaa systeemin kompleksiseen kybertoimintaan valmistautumisen tasoa turvallisuusnäkökulmasta. Kyberturvavalmiuden tasoa ei voida arvioida täydellisesti, sillä systeemien avoin luonne ja kompleksiset vuorovaikutussuhteet muuttuvat jatkuvasti. Tämä tukee luvussa 4 esiteltäviä systeemien yleisiä toimintaperiaatteita, jotka antavat mahdollisuuden kyberturvavalmiuden kokonaisvaltaiseen parantamiseen. (Taskinen 2015 s. 11)

Kyberturvallisuus (engl. *cyber security*) on eri toimijoiden ja toimintojen kyberkokonaisuudesta aiheutuva turvallisuuden tila. Kyberturvallisuuteen kuuluvat tietoturvallisuuden ja kyber-fyysisten systeemien turvallisuuden kaikki osa-alueet. Tietoturvan osa-alueita ovat fyysinen tietoturva, hallinnollinen tietoturva, tietoaineisto-, tietoliikenne- ja ohjelmistoturvallisuus sekä yksityisyyden suojan asiat. Kyberturvallisuuteen kuuluvat lisäksi kriittisten järjestelmien turvallisuus, kybersota, tiedustelutoiminta sekä kyberterrorismi. Myös fyysisen maailman ohjaaminen tietoverkkoja tai -tekniikkaa hyväksi käyttäen kuuluu kyberturvallisuuden käsitteen piiriin. **Kyberuhka** on kyberturvallisuutta heikentävä tekijä. (Taskinen 2015 s. 10, Harju 2015)

Organisaatio (engl. *organisation*) on rakenteita ja prosesseja, joita ihmiset muodostavat olemassaolon ja tarkoituksen perusteella. Rakenteet ovat organisaation olemassaolon ja toiminnan perusta. Organisaation rakenne on aina tietyssä määrin hierarkkinen, joka käy ilmi myös luvussa 3 esiteltävän

yleisen systeemiteorian näkökulmasta. Käytännössä rakenne muodostuu työnjaosta, erikoistumisesta, osastojaosta, auktoriteeteistä, komentoketjuista, valvontasuhteista, päätöksentekovallasta sekä muodollisuuksista eli säännöistä ja määräyksistä. Tämän tutkimuksen kannalta on keskeistä ymmärtää, että organisaation prosessit – eli esimerkiksi eettisen hakkeroinnin menettelytavat – määrittävät organisaation rakenteet, jotka ovat pohjimmiltaan periaatteiden yhdistelmiä. Esimerkiksi yrityksen eettisen hakkeroinnin menettelytapoihin voisi kuulua prosessien muuttaminen valkohattujen ja harmaahattujen suositusten mukaisesti paremman kyberturvallisuuden saavuttamiseksi. Tällöin myös yrityksen rakenteessa väistämättä tapahtuu muutoksia. (Harisalo 2008 s. 74,76,77)

Organisaatio voidaan määritellä karkeasti neljästä eri näkökulmasta: tavoitteen ja tehokkuuden, säilymisen, avoimien systeemien ja ihmisten omien tulkintojen näkökulmista (Harisalo 2008 ss. 17-29). Tässä tutkimuksessa organisaatiot käsitetään avoimiksi systeemeiksi eli kyber- ja fyysisestä ympäristöstään riippuvaisiksi vuorovaikuttaviksi kokonaisuuksiksi.

Menettelytapa tarkoittaa tässä tutkimuksessa systeemin tapoja toimia päämäärän saavuttamiseksi. Selvittäminen tai suunnittelu eivät riitä, vaan tarvitaan toimia, jolla päämäärä saavutetaan. Käytännössä on kyse siitä, mitä eettisen hakkeroinnin eli kyberturvavalmiuden selvittämisessä aikaan saaduilla tiedoilla tehdään organisaatiossa. Pelkkä dokumenttien kirjoittaminen harvemmin johtaa toivottuihin parannuksiin. Monissa organisaatioissa kuitenkin toimitaan näin jatkuvasti. (Beaver 2013 s. 23)

4. Eettinen hakkerointi kohdistuu systeemeihin

Systeemi tulee latinan kielen sanasta *systēma*, joka tarkoittaa tiettyjen periaatteiden mukaista toiminnallista vuorovaikuttavien elementtien kokonaisuutta (Haarala et al. 2016, systeemi, Merriam-Webster 2016b, Scott, Liddell & Jones 1940). Esimerkiksi viranomainen, yritys ja yhdistys ovat systeemejä. Systeemin sisäisiä osia kutsutaan tässä tutkimuksessa elementeiksi. Tässä luvussa esitetään teoria systeemien yhteistoiminnasta ja vuorovaikutussuhteista. Teoriaa sovelletaan eettisen hakkeroinnin menettelytapojen kuvaamiseen organisaatiossa.

4.1. Yleinen systeemiteoria on työkalu eettisen hakkeroinnin tarkasteluun

Itävaltalainen biologi ja filosofi Ludwig von Bertalanffy (1901-1972) esitteli vuonna 1968 organisaatioita ja kokonaisuuksia käsittelevän **yleisen systeemiteorian (GST)**, jonka mukaan maailma tulisi hahmottaa systeemeinä ja niiden välisinä vuorovaikutussuhteina. Tieteenaloja yhdistävän teorian mukaan systeeminen kokonaisuus voi olla enemmän tai vähemmän kuin osiensa summa. Tämä holistinen näkemys on seurausta systeemien vuorovaikutussuhteiden ja rakenteiden kompleksisuudesta, joka ilmenee systeemien toimintatapojen vaikeana mitattavuutena ja jatkuvana muutoksena. Ymmärtääksemme nykyisiä komplekseja systeemejä tulisi teorian mukaan keskittyä enemmän systeemien ja niiden aliosasten, elementtien, väliseen vuorovaikutukseen eli prosesseihin ja osiin eli rakenteisiin. Nykyisessä monimutkaisessa ja kehittyvässä maailmassa GST:n monitieteisyys on auttanut ymmärtämään ja jäsentelemään systeemien hakkeroinnin laajuutta. (von Bertalanffy 1968)

Mitä hyötyä teoriasta on kyberturvallisuuden ja eettisen hakkeroinnin tutkimuksen kannalta? Hyötynä on selkeä jäsennys siitä, mitä yksittäiseltä kyberturvallisuuttaan pohtivalta organisaatiolta voi odottaa, millaiset vaikutukset kybermaailmalla on organisaatioon ja kuinka näitä vaikutuksia voisi hallita parhaiten. Toiseksi teorian avulla voidaan perustella, miksi eettinen hakkerointi on ylipäätään järkevää. Kolmanneksi teorialla voidaan selittää, miksi eettinen hakkerointi ei yksinään riitä ongelmien ratkaisemiseksi. Neljänneksi eettisen hakkeroinnin tuottaman tiedon avulla voidaan luoda menettelytapoja, jolla eettisen hakkeroinnin tulokset implementoidaan osaksi systeemin toimintaa kokonaisvaltaisesti.

GST jakaa systeemit avoimiin ja suljettuihin systeemeihin. Suljettu systeemi on täydellisesti eristetty muista systeemeistä, eli sillä ei ole vuorovaikutusta muiden systeemien kanssa. Päinvastoin avoin systeemi on jatkuvassa vuorovaikutuksessa ympäristönsä kanssa.

Suljetuilla systeemeillä on yhteisiä ominaisuuksia, jotka ovat peräisin *termodynamiikan* laeista: systeemin tasapaino, energian säilyminen, entropian kasvu ja entropian nollapiste. Termodynamiikan säännöt eivät kuitenkaan sovellu avoimien eli vuorovaikuttavien systeemien tutkimukseen kovin hyvin. Tämä johtuu yhtäältä lakien vaikeasta sovellettavuudesta avoimiin ja kompleksisiin systeemeihin, toisaalta termodynamiikan toisen säännön vaikeasta selitettävyydestä. Sen mukaan luonnon systeemeissä tapahtuu jatkuvaa rappeutumista ja entropia kasvaa, kunnes saavutetaan täydellinen tasapaino eli hajaannus (ei rakenteita). Entropia on hajeen määrän mitta systeemissä. Avoimissa systeemeissä tapahtuu kuitenkin organisoitumista eli entropia on negatiivista. Avoimien systeemien kuvaamiseksi yleinen systeemiteoria onkin hyödyllinen ja auttaa ymmärtämään paremmin keskenään vuorovaikuttavia systeemejä. Suljettuja systeemejä ei esiinny luonnossa, vaan ne ovat lähinnä teoreettisia ideaalimalleja, eivätkä siten ole kyberturvallisuuden kannalta oleellisia.

A**voimilla systeemeillä** on yhteisiä ominaisuuksia suljettujen systeemien kanssa. Jatkuvasta ympäristön kanssa käytävästä vuorovaikutuksesta johtuen niillä on myös poikkeavia lisäominaisuuksia. Jokainen ominaisuus käydään läpi seuraavissa alakohdissa erikseen. Kooste ominaisuuksista on esitetty kuvassa 2.

Vaikka yleistä systeemiteoriaa on sovellettu kyberturvallisuuden tutkimiseen yleensä, ei ole tiedossa, että sitä olisi aikaisemmin sovellettu eettisen hakkeroinnin mallintamiseen ja tutkimiseen.

Vakautuvuus	• Systeemi pyrkii vakaaseen tilaan, vaikka ei saavutakaan sitä täydellisesti koskaan.
Tulevaisuusriippuvuus	• Systeemin toiminta riippuu sen tavoitteista (vakaan tilan olemuksesta)
Hierarkia	• Järjestystä on systeemien rakenteissa (osat) ja toiminnoissa (prosessit).
Kokonaisvaltaisuus	• Muutos systeemin yhdessä elementissä vaikuttaa koko muuhun systeemiin.
Jatkuva keskittyminen	• Systeemin tietyt osat ovat keskeisempiä kokonaisuuden kannalta.
Kasvaminen ja haje	• Systeemit voivat kasvaa ja elementtien lisääntyminen systeemissä merkitsee kasvua.
Edistyvä segregaatio	• Elementit erkanevat toisistaan itsenäisyyden kasvaessa. Tämä luo pohjan kasvulle.
Kilpaileminen	• Systeemit voivat kilpailla keskenään.
Itsenäistyminen	• Systeemin elementit voivat olla enemmän tai vähemmän itsenäisiä, eivät kokonaan.

Kuva 2. Kaikkien avoimien systeemien yhteiset ominaisuudet mukaellen von Bertalanffyä (1968).

4.1.1. Vakautuvuus

Avoimien systeemien ”tila” on riippuvainen systeemin ympäristön vuorovaikutussuhteista. Tila tarkoittaa systeemin toimintaa tietyllä ajanhetkellä. Yleisen systeemiteorian mukaan kaikki systeemit – esimerkiksi organisaatiot – pyrkivät omaan *vakaaseen tilaan* eli vakaan toiminnan määriteltyyn tasoon, vaikka eivät saavuta sitä koskaan täydellisesti. Tämä johtuu jatkuvasti käynnissä olevasta vuorovaikutuksesta systeemin ympäristön kanssa. Vakaa tila tarkoittaa esimerkiksi organisaation strategisten tavoitteiden tai päämäärän tasoa. Epävakaiden systeemien kehittyminen ei ole optimaalista ja niiden toimintaedellytykset ovat heikompia muihin organisaatioihin verrattuna. Tästä syystä vakaa tila on kaikkien organisaatioiden tavoitteena.

Avoin ja vuorovaikuttava systeemi on aina alttiina erilaisille ulkoisen ja sisäisen vuorovaikutuksen luomille poikkeavuuksille. Tällöin systeemin vakaa tila saattaa vaarantua ja systeemin toimintakyky heiketä. Nykyään yhä harvempi tietojärjestelmä on täysin eristynyt Internetistä. Vuorovaikutusta tapahtuu muihin systeemin ulkopuolisiin tietojärjestelmiin. Tähän perustuu eräs nykypäivänä esiintyvä systeemien vakaata tilaa horjuttava tekijä eli pahamielinen hakkerointi. Se käyttää systeemien haavoittuvuuksia ja kehittämättömiä menettelytapoja hyödykseen. Näitä haavoittuvuuksia voidaan havaita ja korjata eettisen hakkeroinnin tulosten perusteella (Engebretson 2013 s. 54). Tästä syystä

eettisen hakkeroinnin käyttäminen on avoimien systeemien kannalta perusteltua. Eettisen hakkeroinnin kokonaisvaltaisilla ja holistisilla koko systeemin huomioon ottavilla luvussa 4 esiteltävillä menettelytavoilla voidaan parantaa systeemin vakaan tilan todennäköisyyttä eli resilienssiä ja kykyä sopeutua sekä kohdata kyberturvallisuuteen vaikuttavia vuorovaikutussuhteita.

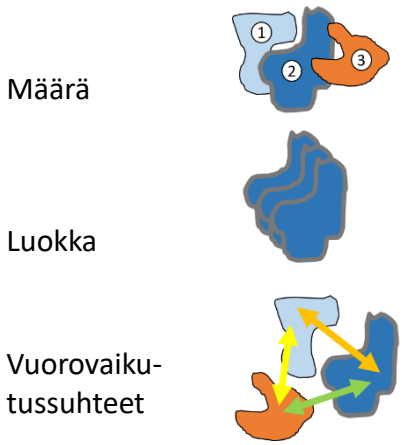
4.1.2. Tulevaisuusriippuvuus

Avoimen systeemin vakaan tilan määritelmä on *tulevaisuusriippuvainen*. Tulevaisuudelle asetetut tavoitteet määräävät systeeminkohtaisen vakaan tilan. Systeemi määrää itse tavoitteet, joiden perusteella se muuttaa toimintaansa ja tavoittelee uutta vakaata tilaa. Toteuttaakseen tulevat tavoitteensa systeemi tarvitsee turvallisuutta. Se saavutetaan, jos 1. systeemeillä on vapaus arvioida omaan menestymiseen, arvoihin tai hyvinvointiin kohdistuvia riskejä ja uhkia, 2. mahdollisuus ilmaista itseensä kohdistuvat riskit sekä resurssit uhkien poistamiseksi, lieventämiseksi tai niihin sopeutumiseksi. Turvallisuuden saavuttamisessa tulevaisuudessa onkin kysymys uhkien ennaltaehkäisemisestä ja tulevaisuuden tapahtumien epävarmuuden vähentämisestä.

Edellä ensimmäinen ehto on määritelmä negatiiviselle turvallisuudelle. Hakkeroinnissa tällaisia ovat systeemiin kohdistuvat kyberuhkat, joita on esitelty lisää kohdassa 5.3. Toinen ehto on puolestaan positiivista turvallisuutta eli eettistä hakkerointia. Siinä on kyse haavoittuvuuksien kartoituksesta ja mahdollisuudesta systeemin tulevaisuuden epävarmuustekijöiden poistamiseen korjaamalla rakenteita ja prosesseja. (Gunhild 2012 ss. 835-839)

4.1.3. Hierarkia

Hierarkia tarkoittaa systeemien luokittelutapaa ja rakenne. Perustaso on systeemi, joka koostuu rakenteista eli osista ja prosesseista eli toiminnoista. Luokittelussa systeemin alapuolella ovat systeemin sisäiset elementit. Elementit ovat omia systeemejään, joiden sisällä on uusia systeemejä. Perustason systeemin yläpuolella on vuorovaikutussuhteiden verkosto, joka muodostaa ylemmän tason systeemin. Kaikki systeemit vuorovaikuttavat toimintojensa avulla keskenään, jol-



Kuva 3. Rakennetta voidaan luokitella hierarkkisesti monella eri tavalla.

loin systeemien rakenteet eli osat muuttuvat. Kaikilla systeemeillä on hierarkia. Systeemejä voidaan määritellä luokittelemalla niitä eri tavoin. Kuvassa 3 on esitetty kolme tapaa luokitella systeemejä.

Kuvassa 3 ylhäällä systeemien määrä voi tarkoittaa esimerkiksi yrityksen liiketoimintayksiköiden määrää, esimies- ja tiimisuhteiden määrää, tietojärjestelmien määrää, henkilöstön tai käyttäjätunnusten määrää, fyysisten rakennusten määrää ja niin edelleen. Systeemin luokka (kuvassa 3 keskellä) voi olla käytännössä vaikkapa markkinointiosasto, turvallisuusosasto, kesätyöntekijät, tietokannat, palomuuri tai mikä tahansa systeemiä luokittelemalla jäsentelevä rakenne. Vuorovaikutussuhteita (kuvassa 3 alimpana) voivat olla tietoliikenneyhteydet, esimiehen työnmääräysvalta, tiedotuskanavat ja logistiikka. Hierarkia onkin näkökulmariippuvainen systeemin rakenteita ja prosesseja kuvaava kokonaisuus, joka liittyy varsinkin hakkeroinnin tiedusteluvaiheeseen, erityisesti sosiaaliseen tiedusteluun.

4.1.4. Kokonaisvaltaisuus

Avoimessa systeemissä voidaan saavuttaa sama vakaa tila eli tavoite monella eri tavalla ja monesta eri lähtötilanteesta. Tätä systeemin ominaisuutta kutsutaan **ekvifinaliteetiksi** eli samatavoitteisuudeksi (Ihanus 2010). Tämä eroaa termodynamiikan perusperiaatteista, sillä suljetussa systeemissä alkutilanteen tai tavan muutos muuttaa välttämättä myös systeemin lopputilaa termodynamiikan lakien mukaisesti. Käytännössä avoimissa systeemeissä kyse on siitä, että keinot tavoitteisiin pääsemiseksi voivat olla erilaisia tuloksen ollessa sama. Avoimet systeemit ovatkin epälineaarisia, kokonaisvaltaisia ja jokainen elementti vaikuttaa koko systeemin tilaan.

Käytännössä tämä ilmenee esimerkiksi systeemin tavassa tavoitella kyberturvallisuutta. Saman kyberturvallisuuden tason voi saavuttaa kouluttamalla henkilöstöä oikeisiin toimintatapoihin, kehittämällä yhteistyötä muiden systeemien kanssa tai parantamalla johtamista ja tilannekuvaa. Tämä johtuu systeemin kompleksisesta kokonaisvaltaisuudesta. (Taskinen 2015)

4.1.5. Jatkuva keskittyminen

J*atkuva keskittyminen* tarkoittaa systeemin rakenneosasten eriarvoisuutta. Keskeisillä elementeillä on enemmän tai tärkeämpiä vuorovaikutussuhteita. Toisaalta muilla elementeillä on suurempi riippuvuus niistä. Haitallinen vakaata tilaa horjuttava vuorovaikutus keskeiseen elementtiin saattaa johtaa koko systeemin kriisitilaan. Toisaalta toiset systeemin elementeistä ovat kokonaisuuden kannalta

vähemmän tärkeitä, mutta niihin kohdistuva vakaata tilaa horjuttava vuorovaikutus vaikuttaa aina koko systeemin toimintaan jollain tavalla.

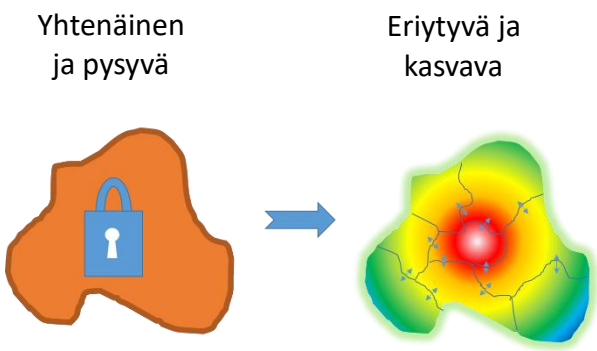
Hakkeroinnin näkökulmasta tämä ilmenee käyttöjärjestelmien suojauskehien muodossa. Suojauskehän numero ilmaisee, kuinka paljon kyseisellä kehällä olevalla prosessilla on oikeuksia koko järjestelmässä. Käyttöjärjestelmän ydin sijaitsee suojauskehällä 0. Sillä on pääsy kaikkiin tietojärjestelmän elementteihin ja se myös ohjailee käyttöoikeuksien antamista muilla kehillä oleville ohjelmille. Hakkerin pääsy tällaiselle kehälle antaisi täydet hallintaoikeudet kaikkiin toimintoihin systeemissä. (Krutz 2008 ss. 117-119)

4.1.6. Kasvaminen ja haje

Avoimen systeemin entropia eli hajeen määrä voi olla negatiivista tai positiivista. Käytännössä tämä tarkoittaa, että kaaoksen sijaan systeemissä voi syntyä järjestystä, organisoitumista ja kasvua jatkuvasti. Myös hajeen suureneminen ja rakenteiden tuhoutuminen on mahdollista. Tästä hyvä esimerkki on evoluutio, sillä kaikki luonnossa esiintyvät elävät organismit ovat avoimia systeemejä. Yritysorganisaation kasvaminen, Internetin laajentuminen sekä kyberavaruuden kehittyminen ovat myös esimerkkejä negatiivisesta entropiasta. Hakkerit voivat käyttää jatkuvaa muutosta hyödykseen, sillä muutoksessa syntyy haavoittuvuuksia, kuten ohjelmointivirheitä.

4.1.7. Edistyvä segregaatio

Systeemi tarvitsee kasvaakseen *edistyvää segregaatiota* eli systeemin elementtien eriytymistä. Tämä prosessi on kuvattu kuvassa 4 vasemmalla, jossa lukkiutunut, yhtenäinen ja pysyvä systeemi ei kehity, mutta voi olla hallittavampi. Kuvassa 4 oikealla eriytyvä, itsenäistyvä ja kasvava systeemi muodostuu kompleksisemmaksi prosessin edetessä. Uusia elementtejä ei voi syntyä, jos organisaatiossa ei tapahdu eriytymistä. Toisaalta eriytyminen vaatii energiaa systeemin ympäristöstä. Segregaatio lisää systeemin kompleksisuutta ja riippuvuutta ympäristöstä. Tällöin sen toiminnan ymmärtäminen on entistäkin haastavampaa.



Kuva 4. Vasemmalla olevan yhtenäisen ja pysyvän systeemin muutos eriytyväksi ja kasvavaksi systeemiksi mahdollistaa kasvun.

Esimerkiksi jatkuvasti muuttuvista ja kasvavista informaatiojärjestelmistä tulee hetki hetkeltä kompleksisempia. Mustahattujen tekniikat ovat yleensä askeleen edellä valkohattuihin verrattuna. Koko ajan järjestelmiä ja prosesseja päivitetään vastaamaan paremmin erilaisia kyberuhkia vastaan. Tätä resilienssiä eli kykyä vastata vuorovaikutussuhteiden muutoksiin korjataan esimerkiksi ohjelmistopäivityksillä, uusilla haittaohjelmatunnisteilla ja täysin uusilla laitteiston sekä tekniikan innovaatioilla. Tämä kaikki vaatii työtä eli energiaa organisaatioon ulkopuolisilta tahoilta. (Beaver 2013 s. 24)

4.1.8. Kilpaileminen

Systeemeille on ominaista myös *kilpaileminen*. Laajoissa vuorovaikutussuhteiden verkostoissa, kuten markkinatalousjärjestelmässä on olemassa kilpailua. Se tarkoittaa systeemien välistä vuorovaikutussuhteiden ohjailua siten, että systeemin oma vakaa tila ja kasvu säilyisi mahdollisimman optimaalisena. Kaikkien vuorovaikutukselle avointen systeemien pyrkimys samaan tilaan ilmenee kilpailuna. Eettinen hakkerointi luo etuja kilpailijoihin nähden muun muassa vähentämällä liiketoiminnalle aiheutuvia riskejä ja parantamalla ennustettavuutta.

4.1.9. Itsenäistyminen

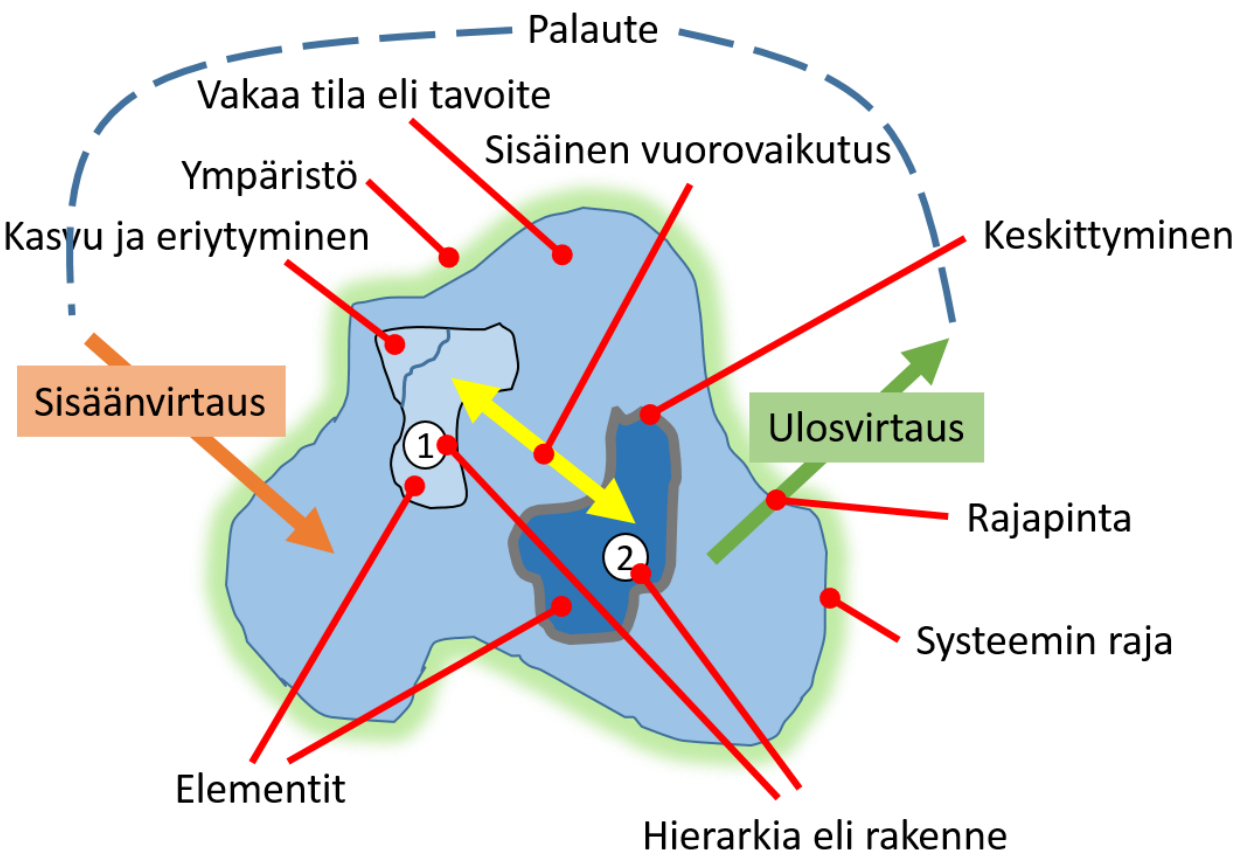
Yksilö voidaan määritellä keskittyneeksi systeemiksi. Itsenäistymistä tapahtuu vuorovaikutussuhteiden vähentymisen seurauksena. Uusia systeemejä syntyy tällöin systeemien alemmille hierarkiatasoille samalla, kun ylemmät systeemit muodostuvat kokonaisuutena kompleksisemmiksi. Ilman systeemien eriytymistä ei kasvua ja kehitystä voi tapahtua.

Käytännössä tämä näkyy tietojärjestelmien tehtävissä. Jokainen järjestelmä on oma kokonaisuutensa ja räätälöity tuottamaan tietynlaisia palveluita, prosesseja ja toimintoja mahdollisimman tehokkaasti. Jokaisella toimijalla on järjestelmille omat tarpeensa ja halu parantaa prosesseja. Yksi yhteinen järjestelmä on mahdollinen, mutta tällöin siihen täytyy rakentaa valtava määrä jokaisen toimija huomioon ottavia osia tai moduuleita. Vastaava toiminnallisuus voidaan saavuttaa myös yhdellä pienellä vain asiakkaan tarpeisiin räätälöidyllä tietojärjestelmällä. Tällöin ei kuitenkaan saavuteta sisäisen vuorovaikutuksen hyötyjä, kuten synergiaetuja ja sujuvaa vuorovaikutusta elementtien välillä. Mitä suurempi ja kompleksisempi järjestelmä on, sitä haastavampaa on huolehtia sen kyberturvallisuudesta. (Ives, Learmonth 1984)

4.2. Systeemiteorian konsepti eettisessä hakkeroinnissa

Miksi eettistä hakkerointia tehdään? Teorian ymmärrettävyyden kannalta on välttämätöntä tarkastella asiaa esimerkin ja systeemiteorian visualisoinnin (kuva 5) avulla. Systeemi voi olla esimerkiksi yritys, viranomainen tai yhdistys. Systeemin sisällä voi olla IT-järjestelmä, joka on myös systeemi. Tarkastellaan systeeminä yritystä, jolla on toimintoja kybermaailmassa ja fyysisessä maailmassa (**ympäristö)**. Yrityksessä on työntekijöitä, fyysistä ympäristöä ja digitaalisia järjestelmiä (**elementit**). Kybermaailma on vuorovaikuttavien systeemien verkosto (**vuorovaikutussuhteet**). Yritys pyrkii toimintaansa itsenäisesti ohjailemalla saavuttamaan tavoitteitaan, kasvamaan ja kilpailemaan muiden yritysten kanssa (**tulevaisuusrippuvuus**). Yrityksen tavoite on saavuttaa **vakaa tila**, jossa toiminnan tuotot, edellytykset ja kehittymismahdollisuudet ovat parhaimmat.

Voidakseen toimia näin yrityksen on oltava vuorovaikutuksessa ympäristönsä eli muiden yritysten (kilpailijoiden toimet), viranomaisten (viranomaispäätökset) ja asiakkaiden (kysyntä) kanssa (**palaute**). Samalla yrityksen on kehitettävä nykyisiä, luotava uusia ja lopetettava kannattamattomia liiketoimintamahdollisuuksia selviytyäkseen tulevasta (**kasvaminen ja eriytyminen**). Pienenkin liiketoiminta-alueen epäonnistunut toiminta voi vaikuttaa koko yrityksen tulokseen, ilmapiirin ja toimintamahdollisuuksiin (**kokonaisvaltaisuus**). Yrityksen keskeisten strategisten tavoitteiden – eli vakaan tilan – saavuttamatta jääminen voi merkitä pahimmassa tapauksessa koko yrityksen konkurssia (**jatkuva keskittyminen**). Haasteen yrityksen toiminnalle asettaa jatkuva muutos yrityksen sisäisissä toimintatavoissa (**edistyvä segregaatio**). Tästä syystä yritys pyrkii jatkuvasti ja kokonaisvaltaisesti tarkastelemaan omia toimintamahdollisuuksia heikentäviä tekijöitä ja ennalta ehkäisemään niitä. Yritykset luovat rakenteita ja prosesseja tunnistamaan tällaisia vakaata tilaa heikentäviä vuorovaikutussuhteita ja pyrkivät mahdollistamaan vakaan toiminnan (**hierarkia**).



Kuva 5. Kaikille systeemeille yhteiset prosessit ja rakenteet esitettynä visuaalisesti mukaellen von Bertalanffyä (1968).

Eettinen hakkerointi on eräs keinoista, jolla voidaan sekä tunnistaa toimintamahdollisuuksia heikentäviä että parantavia vuorovaikutussuhteita ja rakenteita menettelytavoista riippuen. Eettisen hakkeroinnin menettelytavoilla tavoitellaan parempaa resilienssiä ja vakautta systeemille, kuten yritykselle, julkiselle viranomaiselle tai yhdistykselle. Kuten edellä esitettiin, kaikkien kybermaailmassa toimivien systeemien prosesseihin ja rakenteisiin on löydettävissä eettisen hakkeroinnin tulosten sovelluksia. Niillä voidaan parantaa systeemin toimintamahdollisuuksia laaja-alaisesti: epävarmuus tulevasta vähenee, riskit pienenevät ja resilienssi vastata uusiin uhkiin kasvaa. Samalla voidaan mahdollistaa toimintaa, joka aiemmin oli liian riskialtista. Toisaalta on myös tilanteita, joihin eettisen hakkeroinnin menettelytavat eivät ole ensisijainen keino. Tällainen tilanne on esimerkiksi hyvin pienissä organisaatioissa, joiden resurssit ovat vähäiset. Kaikki systeemien tapahtumat voidaan kuitenkin selittää yleisen systeemiteorian avulla.

4.3. Tutkimusteorian lähiteoriat

Tässä tutkimuksessa teoriapohjana on yleinen systeemien teoria. Teoriasta on kuitenkin useita sovelluksia tai lähiteorioita, joita ovat muun muassa kompleksisuusteoria, peliteoria, informaatioteoria ja kybernetiikka. Esimerkiksi kybernetiikan mukaan tavoitteellinen toiminta systeemeissä pohjautuu saatuun palautteeseen ja sen perusteella toiminnan ohjailemiseen. Informaatioteoria puolestaan esittelee informaation mitattavaksi yksiköksi ja perustelee sen liikkeitä systeemeissä (von Bertalanffy 1968). Kaikki edelliset sopivat hyvin eettisen hakkeroinnin tarpeellisuuden ja vaikutusten selittämiseen, mutta eivät välttämättä ole yhtä monitieteisiä, kuin yleinen systeemiteoria GST.

Hieman erilaisen näkemyksen antaa kompleksisten adaptiivisten systeemien teoria (engl. Complex Adaptive Systems, CAS). Tämän tyyppisille järjestelmille on ominaista itseorganisoituminen ja ilmaantuminen, oppiminen, mukautuminen ja yhteisevoluutio. Kompleksisilla adaptiivisilla systeemeillä voidaan selittää organisaatioiden kaltaisia sosiaalisia systeemejä ja niiden kompleksisuutta sekä kyberturvallisuuden kokonaisvaltaisuutta. (Mitleton-Kelly 2003, Taskinen 2015)

5. Eettinen hakkerointi käytännössä

Tässä tutkimuksessa pidetään teoriaa ja empiriaa toisiaan täydentävinä ja myös selittävinä vastinpareina. Kokemuksemme ympäröivästä maailmasta voivat täydentää ajatusrakenteitamme siitä, kuinka maailma toimii. Toisaalta ajattelumallimme rakenteet voivat tuottaa oivalluksia, joita kokemusperäisesti emme olisi aiemmin havainneet. Näin ollen teoria ja empiria kulkevat yhdessä myös kokemuksien analysoinnissa. (Taskinen 2015)

5.1. Tutkimuksen empiiriset valinnat

Seuraavassa käsitellään empiirisen aineiston hankintamenetelmiä. Tutkimuksen menetelmällisistä perusteista ja aineiston keruusta prosessina on kerrottu jo aikaisemmin luvussa 2. Monipuolisilla kirjallisuuslähteillä voi antaa tutkimuksessa esille nousevista ilmiöistä erilaisia ja jopa vastakkaisia näkökulmia käsiteltäviin teemoihin ja aiheisiin. Tutkimuksen kirjallisuusaineisto perustuu aiempaan eettisen hakkeroinnin kirjallisuuteen ja tutkimukseen. Edellisiä voi rajoitetusti soveltaa tämän tutkimuksen osaksi antamaan tutkimukselle lisäarvoa. Sekä suomeksi että englanniksi tuotettu kirjallisuus antaa erilaisia näkökulmia lähestyä aihealuetta. Lisäksi on laajasti käytetty lähteinä vertaisarvioituja akateemisia aikakauslehtiä ja kansainvälisten standardointiorganisaatioiden näkemyksiä käsitteiden käytössä. Näin on saatu selville eettiseen hakkerointiin liittyviä ajankohtaisia ja yleisiä kehityskohteita ja kehityksen suuntaa. Myös erilaiset viranomaislähteet ja raportit ovat tärkeä osa tämän tutkimuksen empiiristä lähteistöä, sillä julkisessa turvallisuussuunnittelussa tuotetaan erilaisia viranomaisraportteja ja strategioita, joiden haluttaisiin ohjaavan käytännön toimintaa. Kirjallisuus on kuitenkin vain täydentämässä tutkimuksen empiiristä osuutta ja tuomassa sille lisäarvoa ja vastakkaisia käsityksiä asioista. Tämä tutkimus ei siis ole ainoastaan kirjallisuusanalyyttinen, vaan aineistoa on kerätty myös teemahaastatteluilla.

Tämän tutkimuksen keskeisin tutkimusaineisto on tuotettu eettisen hakkeroinnin menettelytapojen teemahaastattelulla. Teemahaastattelurunko on tutkimuksen liitteenä 1. Teemahaastattelun kysymykset on valittu tutkimusongelman ratkaisemiseksi. Jokaista kysymystä on harkittu tarkasti ja ne pyrkivät ilmentämään eettisen hakkeroinnin menettelytapojen vaikutusta organisaatioin kyberturvallisuuteen. Kysymyksiä on analysoitu syvällisemmin luvussa 6. Kysymysten reliabiliteettia ja validiteettia tarkastellaan lisää tutkimuksen johtopäätöksissä luvussa 8.

5.2. Eettinen hakkerointi on turvallisuustestausta

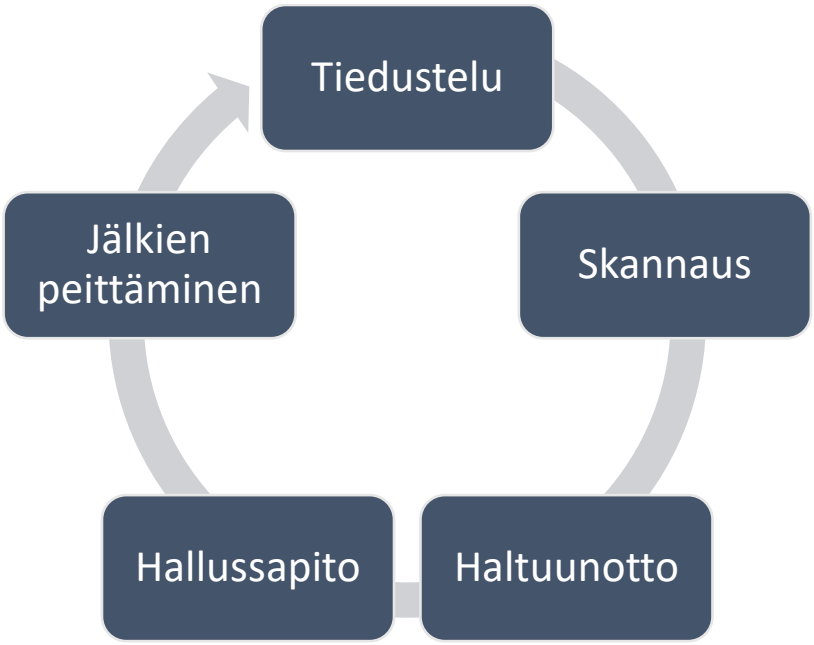
Eettistä hakkerointia kutsutaan erilaisissa asiayhteyksissä penetraatiotestaukseksi (engl. *penetration testing*), haavoittuvuustestaukseksi (engl. *vulnerability testing*) ja turvallisuusauditoinniksi (engl. *security auditing*). Kaikki käsitteet liittyvät samaan asiaan eli systeemien testaamiseen tai arviointiin, mutta niiden merkitys vaihtelee kirjallisuudessa.

Monissa alan teoksissa penetraatiotestausta pidetään täysin samana asiana kuin eettistä hakkerointia (Engebretson 2013 ss. 1-2). Toisissa lähteissä edellinen väite kumotaan esittämällä, että penetraatiotestaus on kapeampi ja vähemmän ammattimaisempi näkökulma kybertestaukseen (Tutorialspoint 2016, Khan 2010 ss. 15-16). Tässä tutkimuksessa penetraatiotesti tarkoittaa järjestelmän, verkon tai laitteen haavoittuvuuksien testausta, eikä se mittaa ihmisten toimintatapoja (Henry 2012 s. 12).

Turvallisuusauditointi (engl. *security auditing*) on tarkastus auditointikriteeristön täyttymisestä. Auditointikriteeristö voi olla lista tai standardi, jonka mukaan systeemin toiminta tulee tarkastaa (Harris 2016). Turvallisuusauditoinnin tarkoituksena on tarkastaa, että turvallisuus- ja riskienhallinta on otettu toiminnassa huomioon (Beaver 2013 s. 12). Auditointi onkin huomattavasti määrämuotoisempi ja rajoitetumpi tarkastusmuoto eettiseen hakkerointiin verrattuna, joka on kokonaisvaltainen kyberturvavalmiuden tarkastus ja koostuu teknisistä ja inhimillisistä keinoista.

5.3. Eettisen hakkeroinnin vaiheet ja menetelmät

Pahamielinen hakkerointi on jaettu viiteen vaiheeseen: tiedustelu, skannaus, haltuunotto, hallussaspito ja jälkien peittäminen (Krutz 2008 s. 9, Engebretson 2013 s. 14). Vaiheet ovat peräkkäisiä ja ne on esitetty kuvassa 6. Jälkien peittelyvaiheen jälkeen hakkeroinnin kehä palaa takaisin tiedusteluvaiheeseen, jossa tarkastellaan systeemin uudet prosessit ja osat eli edistyvän segregaation aikaansaamat muutokset. Valkohattuhakkerit käyttävät mustahattuhakkerien menetelmiä, joten samat vaiheet pätevät eettisen hakkeroinnin menetelmiin. Poikkeuksen tekee kuitenkin alussa tarvittavat luvat ja toimeksianto sekä lopuksi toteutettava raportointi kohteen testaustuloksista. Seuraavassa esitellään vaiheet ja menetelmät lyhyesti.



Kuva 6. Mustahattuhakkerin eli krakkerin menetelmät pätevät myös eettisessä hakkeroinnissa. Jälkien peittäminen korvataan kuitenkin tyypillisesti raportointivaiheella.

5.3.1. Tiedustelu – tietojen kerääminen kohdesysteemistä

Eettisen hakkeroinnin prosessi alkaa kohteen toimeksiannolla. Toimeksiannolla varmistetaan valkohattuhakkerille lailliset ja moraalisesti oikeat toimintaperusteet. Varsinaisen hakkeroinnin kohteen tiedot voivat vaihdella toimeksiannosta riippuen. Vaihtoehtoehtoiset toimeksiannot ovat musta laatikko, harmaa laatikko ja valkoinen laatikko. Musta laatikko tarkoittaa toimeksiantoa, jossa kohdesysteemistä ei saada mitään alkutietoja – kohteen nimeä lukuun ottamatta. Valkoinen laatikko on puolestaan hyvin paljon valmista dataa sisältävä toimeksianto. Kohdeorganisaatio eli systeemi antaa valkoisen laatikon toimeksiannossa itsestään paljon valmista tietoa valkohattuhakkeroinnissa käytettäväksi. Tällöin eettinen hakkerointi on hieman helpompaa aloittaa. Tiedot voivat olla esimerkiksi kohdesysteemin teknisten järjestelmien verkkokaavioita, käytettyjen teknologisten ratkaisujen luettelo, organisaatiokaavio ja jopa lupa haastatella kohdesysteemin ihmisiä, johtajia ja IT-vastaavia. Harmaan laatikon toimeksianto on valkoisen ja mustan laatikon toimeksiantojen sekoitus. Siinä voidaan esimerkiksi antaa lupa haastatella ihmisiä, mutta ei anneta mitään tietoja yrityksen verkoista. (Engebretson 2013 ss. 4-5)

Tiedustelu voi olla aktiivista tai passiivista. **Passiivisen** tiedustelun aloituskeinoina ovat GST:n mukaiset ainoastaan ulosvirtaavat vuorovaikutukset, jotka sisältävät tietoa kohdeorganisaatiosta. Näitä ovat esimerkiksi tiedot kohteesta julkisessa Internetissä. Julkisista lähteistä saatavia tiedustelutietoja lyhennetään akronyymillä OSINT (Open-Source Intelligence). Passiivinen tiedustelu tarkoittaakin

kohdesysteemin seuraamista ja monitoroimista ilman kiinnijäämisen pelkoa. Teknologisena välineenä saavuttaa OSINT-tietoja käytetään muun muassa nuuskimia (engl. *sniffer*), www-sivujen kopioijia, google-hakua hakuehtojen kanssa, metadatan keräimiä ja whois-palveluja. Hieman arkipäiväisempi menetelmä on roskisdyykkaus, jossa kohdesysteemin pois heittämiä dokumentteja ja tarvikkeita analysoidaan tiedon saamiseksi kohdesysteemin prosesseista ja rakenteista. Tätä keinoa käytti muun muassa kuuluisa hakkeri Kevin Mitnick 12 vuoden iässä huijaamalla hyväntahtoisen linja-autonkuljettajan kertomaan ”kouluprojektiaan” varten Los Angelesissa käytössä olleiden julkisen liikenteen vaihtolippujen rei’ityslaitteen ostopaikan. Mitnick lainasi tarvittavat 15 taalaa laitteen ostoon äidiltänsä ja kaivoi paikallisen linja-autovarikon jäteastiat, jotka olivat täynnä rei’ittämättömiä vaihtolipukkeita. Näin hän pystyi rei’ittämään itselleen käyttämättömiä vaihtolipukkeita ja matkustamaan ilmaiseksi kaikilla Los Angelesin linja-autoilla. (Gots 2016, Krutz 2008 s. 10, Engebretson 2013 s. 21)

Aktiivisella tiedustelulla testataan kohteen reagointia antamalla kohteelle impulssi sisään virtaavien vuorovaikutussuhteiden välityksellä samalla seuraamalla ulosvirtauksen muutoksia erilaisilla antureilla. Tällöin kohdesysteemi myös huomaa uuden sisään virtaavan vuorovaikutusyrityksen, jolloin systeemi voi tehdä ennaltaehkäiseviä toimia hakkeria vastaan. Tällaiseen toimintaperiaatteeseen nojautuvat esimerkiksi kohdesysteemin DNS-palvelinten tietojen kaivaminen, kohteen sähköpostipalvelimen hyödyntäminen tietojen keräämisessä ja sosiaalinen tiedustelu (engl. *social engineering*). Sosiaalinen tiedustelu tarkoittaa kohdesysteemissä olevien ihmisten psyykkistä taidokasta manipuloimista tiettyjen tapahtumien aikaansaamiseksi (Hadnagy 2010 s. 10). Ihmiset ovat systeemien, kuten organisaation, informaatioturvaamisen heikoin lenkki, mikä tarkoittaa mustahattujen näkökulmasta helpointa tapaa hakkeroida systeemi (Beaver 2013 s. 65). Esimerkiksi tietojenkalastelu (engl. *phishing*) on eräs menetelmistä, jossa mustahattu väittää olevansa esimerkiksi IT-tukihenkilö ja pyytää lähettämään sähköpostin välityksellä erilaisia tietoja, kuten käyttäjätunnuksen ja salasanan. Sosiaaliseen tiedusteluun ei välttämättä tarvita kovinkaan syvällisiä tietojenkäsittelyllisiä taitoja, vaan syvällistä, tieteellistä ja taidokasta ymmärrystä ihmisten käyttäytymisestä ja psyykestä. Sen tekniikoita ovat tietojenkalastelun lisäksi tekosyyt eli sepitetykset, syötit, seuraaminen ja fyysinen tunkeutuminen. (Engebretson 2013 ss. 48-49, Hadnagy 2010 ss. 78, 351-352)

Tiedusteluvaiheen jälkeen valkohattuhakkerilla on käsitys kohdesysteemistä ja analyysi systeemin rajapintojen eli IP-osoitteiden (engl. *Internet Protocol*) määrästä ja tiedoista. Aktiivisin ja passiivisin

keinoin hankittujen tietojen syventäminen ja jatkojalostaminen jatkuu skannausvaiheessa. (Engebretson 2013 ss. 53-54)

5.3.2. Skannaus – tiedon jäsentely ja jatkojalostus

Eettisen hakkeroinnin toisen vaiheen menetelmän eli skannauksen tarkoituksena on selvittää kohdesysteemin hierarkia, elementtien rajapinnat, keskeiset elementit ja hyödynnettävät haavoittuvuudet. Skannausvaihe on kokonaisuus, mutta käytännössä se koostuu **kaikuluotauksesta** (engl. ping sweep), porttiskannauksesta, skriptauksesta ja haavoittuvuusskannauksesta. Kaikkien edellisten toteuttamiseen löytyy valmiita ratkaisuja ja ohjelmistoja ilmaiseksi. Kaikuluotaus on keino selvittää, mitkä systeemin elementit reagoivat sisään virtaaviin vuorovaikutussuhteisiin eli mitkä elementeistä ovat aktiivisia ja toiminnassa. Teknisenä menetelmänä käytetään esimerkiksi ICMP-pakettien (engl. Internet Control Message Protocol) lähettämistä skannattavalle kohde-elementille eli laitteille. ICMP pakettien tehtävänä on kertoa verkkoon kytkettyjen laitteiden tilasta. Tällaisia ovat erilaiset virhetilanteet datagrammien prosessoinnissa: esimerkiksi kohdeverkon, -laitteen tai portin saavuttamattomuus (Ince 2013, Postel 1981a s. 1, 4). (Engebretson 2013 s. 54, 57)

Skannauksen toinen osa on **porttiskannaus** (engl. *port scan*), jonka tarkoituksena on selvittää, mitkä systeemin elementtien väliset vuorovaikutussuhteet ovat avoimia systeemin ulkopuolelle, tai yleisemmin, mitkä portit ovat avoimia hyökkäykselle ja mitkä ovat kiinni. Teknisesti tämä onnistuu käyttämällä hyväksi Internetin kuljetuskerroksen TCP-kehyksiä (engl. Transmission Control Protocol). TCP mahdollistaa tietoliikenteen eli vuorovaikutukset elementtien ja muiden systeemien välillä. Eräs mustahattujen menetelmä on lähettää TCP-protokollaan kuuluva aloituspaketti eli vuorovaikutussuhteiden synkronointipaketti (SYN) kohdeporttiin. TCP-kolmiotiekättelyn periaatteen mukaan kohdesysteemin saadessa tällaisen sisään virtaavan impulssin vastaus on jokin seuraavista. Ulos virtaa RST-paketti, joka merkitsee portin olemista kiinni. Tällöin mikään elementti ei käytä porttia vuorovaikutussuhteisiinsa systeemin ulkopuolelle. Ulos voi myös virrata TCP-SYN-ACK-paketti, jolloin portti on auki ja valmis avaamaan mustahatulle yhteyden elementin prosessille tai toiminnolle, joka käytännössä on ohjelmisto. Kolmas vaihtoehto on, että kohde ei reagoi mitenkään. Tällöin kohde-elementti ei vuorovaikuta systeemin ulkopuolelle kyseisestä portista. (Postel 1981b ss. 1-5, 7-8)

Skannauksen kolmas ja neljäs osa ovat **skriptaus** ja **haavoittuvuusskannaus**, jotka limittyvät yhteen. Skriptauksella musta- tai valkohattu kykenee automatisoimaan käyttämiään komentoja ja räätälöimään hyökkäyksen kohdesysteemin haavoittuvuuksien mukaan. Skriptaus on käytännössä erilaisten komentojen tai tietojenkeruun automatisointia pienillä ohjelmilla. Tämä säästää hakkerin aikaa muihin tehtäviin, kuten haavoittuvuusskannaukseen (Simpson 2012 ss. 112-118). Haavoittuvuuksia pyritään löytämään ohjelmistoista ja asetuksista, joita hyödynnetään suoraan kohteiden haltuunottovaiheessa. Ohjelmistoihin liittyvät haavoittuvuudet ovat yleensä korjaamattomia ohjelmointivirheitä tai vääriä asetuksia. Tunnisteiden kerääminen (engl. *fingerprinting*) on osa haavoittuvuustestausta, jossa kerätään tietoa kohde-elementin käyttöjärjestelmistä ja näin saavutetaan tietoa erilaisista hyökkäysmahdollisuuksista. (Krutz 2008 ss. 109-111, Engebretson 2013 s. 72)

Skannaus päättyy **luettelointiin** (engl. *enumeration*) ja **kartoitukseen** (engl. *mapping*), joissa hakkeri etsii käyttäjätunnustietoja, lokitietoja, systeemin ryhmiä ja rooleja, salasanoja ja suojaamattomia jaettuja tiedostoja sekä hakemistoja käyttöjärjestelmäkohtaisesti. Tällaisella luetteloinnilla pyritään saamaan kuva kohdesysteemin hierarkiasta ja kartoittamaan sen turvallisuussegmentit. Keskeisin systeemin elementti on yleensä kiinnostavin, koska sillä on tyypillisesti pääsy kaikkiin systeemin muihin sisäisiin elementteihin. Eräs tekninen luetteloinnin menetelmä on käyttää Ethernetin SNMP-ohjausprotokollaa (engl. Simple Network Management Protocol) hyväksi. SNMP on tehty verkkoon kiinnitettyjen laitteiden hallintaan ja valvontaan. Se on käyttöjärjestelmäriippumaton reitittimien, kytkimien, palvelinten, kirjoittimien ja työasemien hallintaan yleisesti käytetty menetelmä. Tämän vuoksi se on hakkerille mielenkiintoinen hyökkäyskohde. Hakkeroinnin menetelmä perustuu tässäkin muuttamatta jätettyihin tehdasasetuksiin. Niiden avulla hakkeri voi ohjata SNMP-kohdekonetta suhteellisen helposti. (Engebretson 2013 s. 72, Krutz 2008 s. 132)

5.3.3. Haltuunotto – systeemiin hyökkäys

Skannausvaiheen jälkeen alkaa hakkeroinnin kolmas vaihe eli haltuunotto, joka on riippuvainen tiedustelussa ja skannauksessa saaduista tiedoista kohteesta. Tämän vaiheen tarkoituksena on saada kohdesysteemi hyökkääjän hallintaan ja hyödynnettäväksi. Käytännössä tämä onnistuu saamalla täydet järjestelmänvalvojan oikeudet systeemissä, mutta muukin tavoite on mahdollinen. Tämän saavuttamiseksi hakkeri käyttää esimerkiksi salasanakrakkereita (engl. *password cracking*), väsytyshyökkäyksiä (engl. *brute force*), sanakirjahyökkäyksiä (engl. *dictionary attack*), näppäinlokitusta (engl. *keylogger*) ja eskalaatiohyökkäyksiä (engl. *privilege escalation*). Haltuunotto on vaiheista laajin,

monipuolisin ja jatkuvasti muuttuva. Haltuunotto voidaan jakaa neljään kategoriaan, jotka ovat käyttöjärjestelmätaso, sovellustaso, verkkotaso ja palvelunesto. (Beaver 2013 s. 123,197,249, Krutz 2008 ss. 145-164, Engebretson 2013 ss. 79-82)

Käyttöjärjestelmätasolla hakkeroinnissa käytetään kohdesysteemin käyttöjärjestelmää eli ohjelmien toiminta-alustaa haavoittuvuuksien hyödyntämiseksi. Vuonna 2016 tammikuusta maaliskuuhun mitatulla aikavälillä työpöytäkäyttöjärjestelmistä markkinaosuuksiltaan suosituimpia koko maailmassa olivat Windows 7 (49,16 %), Windows 10 (18,39 %) ja Windows XP (10,2 %). Mobiilikäyttöjärjestelmistä samana tarkasteluajanjaksona suosituimmat olivat Android (68,67 %) ja Ios (25,71 %). Internetiin kytkettyjen kotisivujen ylläpitoon käytettävistä käyttöjärjestelmistä arviolta 2/3 on Unix-pohjaisia käyttöjärjestelmiä, joista Linux noin 55 % osuudella on suurin. Loput 1/3 on valtaosaltaan Windows-pohjaisia käyttöjärjestelmiä. Hakkeroinnin mielenkiintoisimmat kohteet ovatkin Linuxiin ja Windowsiin pohjautuvat käyttöjärjestelmät. (Netmarketshare 2016a, Netmarketshare 2016b, W3Techs 2016a, W3Techs 2016b)

Sovellustasolla hakkeroinnin kohteena ovat sovellukset eli systeemien prosessit, jotka hoitavat erilaisia tehtäviä. Näitä ovat esimerkiksi vuorovaikutussuhteiden muodostaminen ja ylläpito systeemin ulkopuolelle sekä rakenteiden tietovarantojen ylläpito. Käytännössä sovellustason hakkeroinnissa käytettäänkin tietoliikenneohjaimien, sähköpostin, IP-puheluiden, applikaatioiden ja tietokantojen heikkouksia hyväksi. Nämä sovellukset mahdollistavat osaltaan Internetin toiminnan ja ovat siksi kytkettyinä maailmanlaajuiseen verkkoon. Eräs tekninen menetelmä on käyttää vanhan SMTP-sähköpostiprotokollan heikkouksia, jossa kohdejärjestelmän porttiin 25 lähetetään telnet-yhteydellä vahvistuspyyntö erilaisille sähköpostiosoitteiden olemassaoloille. Mikäli vahvistus tulee kohdesysteemistä ulosvirtauksena, voidaan se lisätä käyttäjätunnuslistaan ja jatkaa haltuunottoa muilla menetelmillä. (Beaver 2013 ss. 251-252, 258-259)

Verkkotasolla toimivat systeemin rakenteet, jotka luovat pohjan kaikelle vuorovaikutukselle ja toiminnalle systeemin sisällä. Siksi ne ovat kiinnostavia kohteita mustahatuille ja eettisille hakkereille tai penetraatiotestaajille. Haltuunotto voi tapahtua esimerkiksi Man-in-the-Middle -menetelmällä (MitM), salakuuntelemalla langatonta radiotietä, SQL-injektiolla (engl. *SQL injection*) ja XSS-hyökkäyksillä (engl. *Cross-site scripting*) (Wilhelm 2013 s. 340-346). Eräs MitM-menetelmä on ARP-väärennös. ARP (engl. Address Resolution Protocol) on tarkoitettu IP-pakettien välittämiseen oikealle

Ethernet-verkon kohdelaitteelle. Protokollan avulla voidaan selvittää IP-osoitetta vastaava laiteuniikki MAC-osoite eli yksinkertaisemmin selvittää, mikä on laitteen osoite Ethernet-verkossa. Tyypillisesti laite A kysyy verkon eri laitteilta MAC-osoitteita, jolloin ARP-väärennöksessä hakkeri palauttaa samassa aliverkossa olevan hakkerin laitteen MAC-osoitteen, jolloin kaikki tietoliikenne ohjautuukin hakkerin koneelle. Näin hakkeri pystyy salakuuntelemaan verkkoliikennettä MitM-menetelmällä ja saamaan tarvittavat tiedot kohteen haltuunottoon. ARP-väärennöstä käytetään myös istunnon kaappaamisten ja palvelunestohyökkäysten aloituskeinona. (Ramachandran, Nandi Dec 19, 2005 s. 239, Beaver 2013 ss. 146-149)

Haltuunoton viimeinen, erittäin ajankohtainen ja yleisin hyökkäysmuoto on palvelunestot, (engl. *denial of service*), jolla tavoitellaan palvelun saatavuuden estymistä sen laillisilta käyttäjiltä. Tämä tehdään sisään virtaavien vuorovaikutuskanavien kautta suurella määrällä pyyntöjä kohdesysteemiin. Tällöin systeemin kapasiteetti käsitellä pyyntöjä ylittyy ja sen seurauksena vuorovaikutussuhteet tavanomaisiin käyttäjiin vähenevät tai loppuvat kokonaan. Näin palvelunesto on saavutettu. Menetelminä käytetään ICMP-, UDP- ja SYN- pakettien suurien massojen lähetyksiä. Hyökkäys voidaan tehdä yhdeltä koneelta (DoS) tai useammalta koneelta (DDoS). Laajat useilta kaapatuilta tai saastuneilta bottikoneiden verkostoilta tehdyt palvelunestohyökkäykset ovat hajautettuja palvelunestohyökkäyksiä (engl. Distributed Denial of Service). (Beaver 2013 s. 150, Krutz 2008 ss. 208-211)

Isojen nettihyökkäysten ja varsinkin hajautettujen palvelunestohyökkäysten kokoluokka on jatkuvasti kasvanut. Samalla myös Internetissä olevien laitteiden määrän arvioidaan kasvavan tulevaisuudessa nykyisestä 17 miljardista laitteesta noin 26 miljardiin laitteeseen vuoteen 2020 mennessä. Hajautetut palvelunestohyökkäykset voivat olla tulevaisuudessa vieläkin vakavampia kyberuhkia ubiikin yhteiskunnan kehittyessä, mikäli laitteiden kyberturvallisuutta ei systemaattisesti paranneta. (Pulliainen 2016)

5.3.4. Hallussapito – tavoitteiden saavuttaminen

Hakkeroinnin tavoitteena on neljännessä hallussapitovaiheessa hyödyntää kohdejärjestelmän haltuunottovaiheessa saavutettua hallintaa. Tämä toteutetaan muuttamalla systeemin rakenteita ja prosesseja, jolloin myös vuorovaikutussuhteet muuttuvat. Käytännössä hallussapito koostuu ohjelma-

koodin viemisestä, tuomisesta ja muuttamisesta. Ohjelmat voivat olla troijalaisia (engl. *Troijan*), viruksia (engl. *virus*) ja matoja (engl. *worm*). Esimerkiksi troijalaiset muokkaavat ja tuottavat prosesseja kohdesysteemin tietämättä siitä. Troijalainen toimii itsenäisesti ja aktivoituu esimerkiksi erilliseksi taustaprosessiksi käyttäjän poistuttua työasemalta. Tällainen toiminta vaatii troijalaisen pääsyä systeemin keskuselementteihin. Troijalainen tuottaa aktiivisesti ulos virtaavaa vuorovaikutusta kohdesysteemistä ilman tarvetta antaa käskyjä, jolloin sen toiminta on huomaamattomampaa. Ulos virtaavia vuorovaikutussuhteita rajoitetaan yleisesti vähemmän kuin sisään virtaavia vuorovaikutussuhteita. Troijalaiselle ei ole tyypillistä monistua itsestään, vaan madot ja virukset toimivat näin. (Engebretson 2013 s. 54, Krutz 2008 ss. 169-200)

Valkohattuhakkerin tavoitteena ei ole viruksien tai matojen levittäminen. Tavoitteena on vain saavuttaa hallussapito, joka riittää tavoitteeksi. Hallussapitovaiheen saavuttaminen merkitsee käytännössä mahdollisuutta koko järjestelmän toiminnan ja vuorovaikutussuhteiden ohjailuun. Monesti varsinainen tekninen osuus eettisessä hakkeroinnissa päätyy tähän ja alkaa raportointivaihe (Engebretson 2013 ss. 187-188). Tarkastellaan silti viimeinen eli mustahattuhakkerien tavoite olla jättämättä todisteita rikollisista toimista. Tämä tehdään, jotta voidaan ymmärtää, miten todisteiden keruu systeemissä kannattaa järjestää.

5.3.5. Jälkien peittäminen tai raportointi

Systeemien hakkerointi on muuttunut vuosien varrella. Aiemmin mustahattuhakkerien operaatiot olivat kertaluonteisia systeemeihin kohdistuvia hyökkäyksiä. Nykyään yhä useamman pahamielisen hakkerin tavoitteena on pitää pääsy järjestelmään tarvittaessa myös hyökkäyksen jälkeen, eikä hyökkäyksestä saa jäädä mitään jälkiä. Tämä onnistuu luomalla systeemiin takaovi eli rakenne, joka ylläpitää vuorovaikutussuhteiden mahdollisuutta systeemiin sisään ja ulos. Takaovi mahdollistaa hyökkääjän palaamisen kohdejärjestelmään myöhemmässä vaiheessa tarpeen vaatiessa. Eräs tekninen keino toteuttaa takaovia systeemeihin on piilohallintaohjelmistot (engl. *rootkit*), jotka luovat systeemien tärkeisiin keskuselementteihin prosesseja ja rakenteita, joilla systeemin ulkopuolinen taho voi päästä systeemiin sisälle ja tehdä mitä vain, milloin vain. (Engebretson 2013 ss. 167-168)

Jälkien peittäminen tarkoittaa käytännössä kaikkien hakkeroinnin olemassaolon todisteiden tuhoamista. Keinoja ovat tiedostojen tuhoaminen, piilottaminen, lokitiedostojen tyhjentäminen tai muok-

kaaminen, virustorjuntaohjelmistojen kiertäminen ja eheystarkistusten manipulointi. Huomaamattomuus takaa pääsyn systeemiin myös myöhemmässä vaiheessa ja riski kiinni jäämisestä pienenee. (Wilhelm 2013 s. 78)

Eettisen hakkeroinnin toimeksiannosta riippuen jälkien peittämisen vaihe tyypillisesti korvataan **raportointivaiheella**, joka on eettisen hakkeroinnin tärkein vaihe. Raportoinnin tavoite on kirjata löydetyt havainnot kyberturvallisuutta heikentävistä tekijöistä selittää, kuinka hyökkäys tehtiin ja antaa ohjeita haavoittuvuuksien korjaamisesta. Edelliset tavoitteet yhdessä antavat toimeksiantajan eettiseen hakkerointiin käyttämille rahoille vastinetta. Raporteista voidaan tehdä monta versiota, jotka tieteellisen artikkelin tavoin vertaisarvioidaan ja tarkastetaan ennen toimittamista toimeksiantajalle. Ilman raportointia kaikki edelliset toimet ovat turhia, sillä asiakas eli kohdesysteemi ei voi tietää löydettyjä haavoittuvuuksia eikä myöskään korjata puutteita rakenteissa ja prosesseissa. (Wilhelm 2013 ss. 358-367, Beaver 2013 ss. 319-324)

Raportti koostuu testauksen perustiedoista, haavoittuvuuksien tyypeistä, vakavuusluokituksista ja toimenpide-ehdotuksista ongelmien korjaamiseksi. Perustiedot sisältävät eettisen hakkeroinnin menetelmät, toteutusajan, toteuttajan tiedot ja kohteet. Haavoittuvuudet luokitellaan sosiaalisiin ja teknisiin löydöksiin. Sosiaaliset perustuvat sosiaalisen tiedustelun, fyysisen turvallisuuden ja operatiivisen toiminnan puutteisiin esimerkiksi turvattomien toimintatapojen muodossa. Tekniset haavoittuvuudet puolestaan liittyvät verkkoihin, laitteisiin, ohjelmiin ja asetuksiin. Kaikki edelliset luokitellaan vakavuusasteikolle, jonka perusteella voidaan suunnitella haavoittuvuuskorjauksien priorisointia. Toimenpide-ehdotukset ovat konkreettisia keinoja kyberturvallisuuden tason parantamiseksi kohdesysteemissä. (Beaver 2013 ss. 319-324)

6. Aineistoanalyysi

Tämän tutkimuksen keskeisimmän aineiston muodostavat kyberturvallisuuden asiantuntijoille tehdyt teemahaastattelut. Tässä osiossa analysoidaan tutkimusaineistoa sitaattianalyysin keinoin teemoittelemalla tuloksia erillisiin osa-alueisiin. Tutkimustuloksista on kerrottu erikseen luvussa 7.

6.1. Asiantuntijahaastattelut

Teemahaastattelun kahdeksan keskustelua ohjaavaa kysymystä on laadittu tutkimuskysymyksen pohjalta. Kysymysten tarkoituksena on ollut käsitellä eettisen hakkeroinnin menettelytapoja laajasti erilaisista näkökulmista. Kysymykset ovat tutkimuksen liitteenä 1. Tutkijan tekemien haastattelukysymysten validiteetti ja reliabiliteetti on tarkastutettu tutkimuksesta riippumattomalla kyberturvallisuuden asiantuntijalla hyvissä ajoin ennen haastattelutilannetta. Lomakkeet tarkastaneella asiantuntijalla oli pitkä kokemus tieto- ja kyberturvallisuuden alan turvallisuustoiminnasta sekä eettisestä hakkeroinnista. Asiantuntija johtaa tiimiä, joka tekee kyberturvallisuus- ja penetraatiotestauksia turvallisuuskriittisiin järjestelmiin. Tehdyt haastattelukysymysten korjaukset ovat liittyneet lähinnä kysymysten selkeyteen ja käsitteiden määrittelyihin.

Haastateltavat kyberturvallisuuden asiantuntijat valittiin etukäteen tehdyn organisaatioanalyysin perusteella. Analyysissa selvitettiin tutkimuskysymyksen kannalta mielenkiintoisimmat organisaatiot pisteyttämällä jokainen nollasta viiteen yritysten Internet-sivuilta löytyneiden tietojen perusteella. Parhaimmat pisteet saaneiden organisaatioiden edustajat valittiin haastateltaviksi erikseen selvitetyn eettisen hakkeroinnin ja kyberturvallisuuden asiantuntijuuden ja tietotaidon perusteella. Tutkimukseen haastateltiin viittä asiantuntijaa Jyväskylän kyberturvallisuusmessuilla 4. marraskuuta 2016. Haastateltaviksi valikoitui suurten ja pienten suomalaisten kyberturvallisuusalan organisaatioiden edustajia. Haastateltavien joukossa oli niin yksityisten kuin myös julkisten organisaatioiden edustajia – yrittäjiä ja tutkijoita.

Tutkimushaastatteluihin valittiin kaksi kyberturvallisuuden liiketoiminta-alueena ja kokonaisvaltaisemmin tuntevaa asiantuntijaa, jotka olivat molemmat toimitusjohtajia. Tämän lisäksi haastatteluun valittiin kaksi ”hands on” -asiantuntijaa, joilla oli pitkä kokemus eettisestä hakkeroinnista käy-

tännössä. Toinen eettisistä hakkereista oli investoija ja start-up -yritysten konsultti eettisen hakkeroinnin alalla. Viidenneksi asiantuntijaksi valittiin yliopiston kyberturvallisuuden tutkija, jolla oli pitkä tutkimushistoria kyberturvallisuuden alalta. Haastateltavien profiilit on esitetty taulukossa 1.

Tunniste	Profiili	Sukupuoli	Lisätiedot
Haastateltava 1	Toimitusjohtaja	mies	Diplomi-insinööri
Haastateltava 2	Toimitusjohtaja	mies	Ohjelmoija, arkkitehti ja konsultti
Haastateltava 3	Eettinen hakkeri	nainen	Turvallisuusasiantuntija
Haastateltava 4	Eettinen hakkeri	mies	Startup-neuvoja ja investoija
Haastateltava 5	Yliopistotutkija	nainen	Projektitutkija ja projektipäällikkö

Taulukko 1. Teemahaastatteluun valittujen asiantuntijoiden profiilit.

Haastattelut on nauhoitettu ja litteroitu. Haastattelujen keskimääräinen kesto oli 31 minuuttia ja litterointiaineistoa kertyi keskimäärin viisi sivua haastateltavaa kohden. Litterointimateriaalia on analysoitu tuottamalla tiheä kuvaus tutkimuksen kannalta relevanteista havainnoista ja lausumista. Tiheän kuvauksen perusteella on löydetty 11 erilaista kyberturvallisuuteen vaikuttavaa menettelytapaa, jotka ovat seurausta eettisen hakkeroinnin antamista tiedoista.

6.2. Eettisen hakkeroinnin luonteesta

Teemahaastattelun ensimmäinen kysymys eli eettisen hakkeroinnin määritteleminen on ollut koko tutkimuksen kannalta keskeinen. Haastateltujen asiantuntijoiden vastaukset olivat odotetusti toisiaan tukevia ja samankaltaisia, mutta eroavaisuuksiakin löytyi. Poikkeavuudet johtuivat kyberturvallisuuden ja eettisen hakkeroinnin käsitteiden monitulkintaisuudesta. Asiantuntijahaastatteluiden litterointien perusteella saatuja puheenvuoroja on lainattu osana tätä analyysiosuutta. Lainaukset on merkitty sitaatteina kursiivilla tekstistä erilleen helpottamaan lukemista. Lainaukset on valittu koko litterointiaineistosta tutkimuskysymyksen perusteella.

Usean haastateltavan mukaan eettinen hakkerointi tarkoittaa systeemien tai järjestelmien kyberturvallisuuden testausta. Tämä määrittely tukee hyvin yleisen systeemiteorian mukaista systeeminäkökulmaa. Systeemit tavoittelevat vakaata tilaa ja pyrkivät myös ennaltaehkäisemään sitä horjuttavia

tekijöitä. Eettinen hakkerointi mielletään järjestelmien tai menettelytapojen tarkastamiseksi ja havaittujen puutteiden raportoimiseksi.

"Eettisen hakkeroinnin päämäärä on pyrkimys parantaa tietoturvaa löytämällä heikkouksia olemassa olevista järjestelmistä tai menettelytavoista." "Se on postiviinen asia."

Asiantuntijoiden mukaan hakkerointia voidaan kohdistaa ihmisiin ja tietojärjestelmiin. Tämä tukee kirjallisuuden ja yleisen systeemiteorian näkemystä eettisen hakkeroinnin kokonaisvaltaisuudesta. Tällöin otettava huomioon ihmisistä koostuvan organisaation menettelytavat.

"Eettinen hakkerointi voidaan kohdistaa sekä tietojärjestelmille että ihmisille."

Eettisen hakkeroinnin menettelytavat ovat mustahattuhakkerien eli pahamielisten hakkerien käyttämiä. Samanlaisilla tavoilla toimia pyritään saavuttamaan samanlaisia vaikutuksia kohdesysteemissä. Näin voidaan kerätä tietoa oman systeemin haavoittuvuuksista ja korjata menettelytapoja.

"Käytetään luvallisesti samoja tekniikoita, työkaluja ja lähestymistapoja tietoturvahaavoittuvuuksien tunnistamiseen ja löytämiseen kuin pahamieliset hakkerit."

Edellinen asiantuntijakommentti tukee aiemman kirjallisuuden näkemystä eettisestä hakkeroinnista. Erään asiantuntijan mukaan toiminta on eettistä hakkerointia, mikäli se täyttää jokaisen toimintaa kuvaavista ehdoista: kontrolli, kommunikaatio ja yhteistoiminta.

"Eettisessä hakkeroinnissa ollaan "white hat" -hakkereita ja pyritään tunnistamaan haavoittuvuudet, dokumentoimaan ne ja auttamaan asiakasta korjaamaan ne."

Asiantuntijat jakoivat eettisen hakkeroinnin pääasiassa kahteen luokkaan: **tilattuihin** ja **spontaaneihin** hakkerointeihin. Tilatut hakkeroinnit ovat ostettuja tai muuten erikseen kysyttyjä valkohattuhakkerien suorittamia tietoturva-auditointeja vapaamuotoisempia tai kokonaisvaltaisempia organisaation kyberturvallisuuden tason testejä. Tilatut hakkeroinnit ovat luvallisia ja kohteen hyväksymiä. Spontaanit eettiset hakkeroinnit ovat odottamattomia harmaahattuhakkerien toteuttamia kyberturvallisuuden testauksia, joille ei tyypillisesti ole organisaation hyväksyntää. Harmaahattuhakkerien toiminta ei kuitenkaan välttämättä ole organisaation kannalta haitallista, vaan jopa hyödyllistäkin.

"Yritykset maksavat palkkioita sellaisille hakkereille, jotka löytävät heidän järjestelmistään aukkoja."

Osa organisaatioista on kääntänyt asian hyödykseen ja järjestänyt kaikille avoimia eettisen hakkeroinnin tapahtumia, joissa annetaan lupa kaikille hakkereille käyttää taitojaan ja yrittää löytää järjestelmistä heikkouksia.

> *"Jonkinlaista eettistä hakkerointia ovat myös "bug bounty" -ohjelmat, jossa firmat tarjoavat omia tekeleittään yleisesti testattavaksi."*

Kaikki organisaatiot eivät ole asiantuntijoiden mukaan yhtä kypsiä toteuttamaan eettistä hakkerointia. Sellaisille organisaatioille, joiden toimintaan ei juurikaan liity tietotekniikkaa tai kybermaailman ulottuvuuksia, eivät välttämättä hyödy eettisen hakkeroinnin toteuttamisesta. Toisaalta tällaisten toimijoiden osuus on nykyään varsin pieni. Kaikkein pienimmillä organisaatioilla ei välttämättä ole resursseja tilata tai toteuttaa eettistä hakkerointia. Halutessaan jokainen organisaatio kuitenkin kykenee sellaisen toteuttamaan, vaikkapa juuri "bug bounty" -tyyppisellä edullisemmalla ratkaisulla.

6.3. Eettisen hakkeroinnin menettelytavat organisaatioissa

Systeemit pyrkivät vakaaseen tilaan. Eräs tämän tavoitteen mahdollistavista keinoista on eettinen hakkerointi. Sen menetelmät tuottavat uutta tietoa ja mahdollistavat uudenlaisia menettelytapoja organisaatioissa. Näiden menettelytapojen avulla voidaan parantaa organisaation kyberturvallisuutta. Eettinen hakkerointi ei ilman menettelytapoja vaikuta juurikaan organisaation kyberturvallisuuden tasoon. Vaikutus kyberturvallisuuteen saavutetaan vasta, kun eettisellä hakkeroinnilla selville saatujen havaintojen muutokset menettelytapoihin on toteutettu. Kuvassa 7 on esitetty 11 mahdollista menettelytapojen muutoksilla saavutettavaa tilannetta. Näillä keinoilla kokonaisvaltainen organisaation kyberturvallisuuden taso paranee.

Kuva 7. Eettisen hakkeroinnin mahdollistamat menettelytavat organisaatioiden kyberturvallisuuden parantamiseksi tämän tutkimuksen perusteella.

Kokonaiskuva ongelmista

Eettistä hakkerointia voivat hyödyntää erilaiset systeemit: yritykset, viranomaiset, yhdistykset ja yksityishenkilöt. Mitä suuremmasta toimijasta on kyse, sitä perustellumpaa ja yleisempää eettisen hakkeroinnin tilaaminen usein on. Tämä johtuu suurten systeemien kyberulottuvuuksien kompleksisuudesta ja halusta parantaa kokonaisvaltaisesti organisaation kybertoimintaa.

"Maailman järjestäytyessä näin tulee eettistä hakkerointia ajatella suhteessa moneen – ei suhteessa yhteen. Organisaation sisäiset ja ulkoiset osat ovat eri tavoilla verkottuneita."

Eettisellä hakkeroinnilla voidaan ymmärtää kybermaailmaa paremmin. Sen avulla voidaan innovoida ja nähdä kybermaailman mahdollisuuksia laajentamalla systeemin käsityksiä kybermaailmasta. Kokonaiskuvan muodostaminen parantaakin organisaation kyberturvavalmiutta ja vaikuttaa siten kyberturvallisuuden tasoon. Tätä havaintoa tukee myös yleisen systeemiteorian kaikille systeemeille yhteinen kokonaisvaltaisuuden periaate. Organisaatiot ovat kokonaisuuksia, joten kybermaailman organisaatioon kohdistuvat tapahtumat vaikuttavat koko organisaation toimintaan.

"Organisaatio on eettisen hakkeroinnin kohde, tilaaja ja edunsaaja."

Eettisellä hakkeroinnin tiedoilla voidaan parantaa systeemin kyberturvallisuuden kokonaiskuvaa. Erityisen hyviä tuloksia voidaan saavuttaa, jos yleinen tietoisuus kybermaailman toimintaperiaatteista kasvaa. Sen avulla voidaan paremmin hallita riskejä, joita kybermaailman toimijat systeemille asettavat. Lisäksi sillä on selkeä vaikutus organisaation kyberturvavalmiuteen välittömästi muutosten implementoinnin eli haavoittuvuuksien korjausten jälkeen.

"Se on vain tarkistus."

Toisaalta on varottava liiallista luottamista hakkeroinnin tuloksiin, sillä eettinen hakkerointi saattaa testata vain pientä osaa koko kyberturvallisuuden laajasta ja kompleksisesta systeemiin vaikuttavasta toiminta-alueesta. Haastateltujen mukaan syitä eettisen hakkeroinnin käyttämättömyyteen ovat esimerkiksi siitä aiheutuvat kustannukset, uhkien ymmärryksen puute eli tiedon puute, organisaation epäkypsyys testauksen toteuttamiselle ja johtamisongelmat.

Herätys ja asennemuutos

Eettinen hakkerointi voi asiantuntijoiden mukaan toimia keinona saavuttaa innostusta ja uudenlaista ajattelutapaa turvallisuusasioihin. Monesti tärkein vaikutus onkin asennemuutos henkilöstön, johtajien ja koko organisaation keskuudessa. Tällöin huomataan kyberturvallisuuden tärkeys kaikessa toiminnassa.

"Hakkerointi ylipäätään käsitellään input-tekijänä, joka parhaimmillaan laittaa organisaatioissa dominot kaatumaan. Toisaalta huonoimmillaan tällä on vain jotakin pistemäistä vaikutusta."

Parhaimmilla eettinen hakkerointi toimii herätteenä systeemin kybertoiminnan uhkien ja mahdollisuuksien jatkuvaksi kehittämiseksi ja tunnistamiseksi. Eettinen hakkerointi voi olla myös keino herätellä organisaatioita muuttuneen toimintakentän vaatimuksiin. Toisaalta helposti saattaa käydä

niin, että hakkeroinnin avulla kerätyillä tuloksilla vain paikataan haavoittuvuuksia, eikä vaikuteta laajemmin organisaation sisäisiin menettelytapoihin. Tällöin sillä ei saavuteta haluttuja hyötyjä.

Missio, visio, selvitys, strategia ja toimeenpano

"Kyberturvallisuus on organisaatioiden päätoimialaan vaikuttava osa-alue."

GST kuvaa systeemit tulevaisuusriippuviksi. Tulevaisuuden tavoitteet määrittävät organisaation tavoiteltavan vakaan tilan. Tuohon tilaan pääsemiseksi on ennen eettisen hakkeroinnin tilaamista tai tuottamista selvitettävä seuraavat asiat. Millainen on organisaation tehtävä eli missio kybermaailmassa? Mikä nykytilanne on? Mihin tavoitteeseen, vakaaseen tilaan tai visioon organisaatio toiminnalla kybermaailmassa pyrkii? Miten ja millä menettelytapojen muutoksilla organisaatio saavuttaa visionsa? Onko organisaatio jalkauttanut tai toteuttanut kaikki menettelytapojen muutokset suunnitellusti? Eettisen hakkeroinnin menettelytapojen muutokset organisaatioissa kyberturvallisuuden parantamiseksi vaativat tulevan epävarmuuden vähentämistä. Tällöin suunnitelmallisuus, jatkuvammat ja vakaammat toimintatavat tuottavat tulosta.

"Yleisesti on sellainen harhaluulo, että muutaman päivän eettisen hakkeroinnin jälkeen kyberturvallisuus on kunnossa. Tämä kuitenkin vaatii jatkuvaa prosessia ja panostuksia, seurantaa sekä toiminnan kehittämistä organisaatioilta."

Eettinen hakkerointi ei yksinään ilman organisaation menettelytapojen muutosta ja kehitysehdotusten jalkauttamista – viemistä käytäntöön – vaikuta mihinkään. Tällöin sen tilaamisesta ei ole juurikaan hyötyä. Varsinaisen eettisen hakkeroinnin jälkeen suoritettavat organisaatioiden menettelytapojen muutokset, kuten tulosten läpikäynti, jatkojalostaminen ja raportissa mainittujen ehdotusten toteuttaminen vaikuttavat todelliseen kyberturvallisuuden tasoon parantavasti. Ilman näitä menettelytapoja – pelkän eettisen hakkeroinnin avulla – ei voi päästä kuvassa 7 esitettyihin kyberturvavalmiutta parantaviin vaikutuksiin. Myös kirjallisuus nostaa toimeenpanon tärkeyden esille: jos muutoksia ei tehdä, ei hyötyäkään saavuteta. (Beaver 2013 s. 24)

Perusteet riittäville resursseille

Kaikkeen organisaatioiden toimintaan vaaditaan resursseja eli osaava työvoimaa, rahaa, aineetonta pääomaa sekä fyysisiä rakennuksia, laitteita ja tarvikkeita. Resurssit ovatkin taloudellisia, inhimilli-

siä ja sosiaalisia voimavaroja (Tieteen termipankki 2016b). Eettisellä hakkeroinnilla voi asiantuntijoiden mukaan testauksen tuloksesta riippuen perustella resurssitarvetta. Resurssit saattavat vähentyä, kasvaa tai muuttaa hallitsijaansa. Mikäli testitulokset osoittavat suuren määrän haavoittuvuuksia ja korjattavia asioita kyberturvallisuudessa, voi organisaatio vastata korjaustarpeeseen esimerkiksi ulkoistamalla kaikki kyberturvallisuuden toteuttamiseen liittyvät palvelut oman henkilöstön kompetenssin puutteessa. Tällöin resurssit siirtyvät organisaation ulkopuolelle.

Toisessa skenaariossa kyberturvallisuuspalveluiden resursseja kasvatetaan systeemin sisällä. Kolmannessa vaihtoehdossa resursseja kyberturvallisuuden hoitamisesta vähennetään testituloksista tehtyjen väärien johtopäätösten takia.

> *"Todennäköisesti testausta on tehty riittävästi, jos riskienhallinnassa on määritelty, että tämä riskitaso hyväksytään."*

Resurssien tasoon vaikuttavat erityisesti riskienarviot, sillä riskien toteutumisella on monesti suora vaikutus taloudelliseen tulokseen. Riittävillä resursseilla voidaan parantaa systeemin kyberturvavalmiutta ja pienentää riskien eli arvon menetyksen toteutumisen todennäköisyyttä. (Kungwani 2014 s. 83) Toisaalta asiantuntijat korostavat, että liiallinen panostus eettiseen hakkerointiin saattaa viedä resursseja muilta tärkeiltä toiminnoilta ja vaikuttaa organisaation kilpailukykyyn ja kasvamisen mahdollisuuksiin heikentävästi. GST:n mukaisesti tulisikin löytää optimaalinen vakaa tila, jossa eettinen hakkerointi tukee parhaiten kasvamista ja kilpailukyvyn paranemista.

Häiriötiloista palautuminen

> *"Miten reagoidaan hyökkäyksiin heti, jotta pystytään vähentämään niiden vaikutuksia."*

Eettisen hakkeroinnin liikkeelle saamien menettelytapojen muutos on oiva tilaisuus systeemin kriisijohtamisen, maineenhallinnan ja yhteistyön parantamiseen niin systeemin sisäisillä vuorovaikutussuhteilla kuin myös ulkoisesti. Varautuminen tarkoittaa esimerkiksi kriittisiä kyberuhkia vastaan suoritettavien nopeiden toimenpiteiden pitämisen ajan tasalla. Tällaisia ovat nopeat reaktiot, vastatoimet ja muutokset esimerkiksi palvelunestohyökkäyksien aikana. Samalla voidaan kehittää nopeaa, täsmällistä ja selkeää kriisitiedottamista.

Kriittisten kohteiden tunnistaminen

Kyberkriittisten kohteiden tunnistaminen perustuu hakkeroinnin menetelmien mukaiseen tavoitteeseen: hakkeri hallitsee koko systeemiä. Tällöin hakkeri pyrkii löytämään GST:n mukaiset keskeiset elementit ja kohteet systeemiin hyökkäystä varten. Valkohattuhakkerit kirjaavat löydetyt keskeiset kohteet raporttiin, joka palautetaan asiakkaalle. Tällöin asiakas voi vahvistaa kyberkriittisten elementtien ja prosessien suojausta ja kehittää niiden toimintatapoja.

Laadun parantaminen

> *"Järjestelmien turvallisuutta parannetaan, johdon näkyvyyttä yrityksen kyberriskeihin parannetaan, henkilöstön tietoisuutta ja osaamistasoa parannetaan ja toivottavasti ohjelmistokehitysprosesseissa softan laatua ylipäätään parannetaan - ei siis ainoastaan tietoturvariskien kannalta."*

Asiantuntijoiden mukaan eettisellä hakkeroinnin jälkeisillä menettelytavoilla voidaan vaikuttaa myös toiminnan laatuun, teknisten valmiuksien tasoon ja jatkuvuudenhallintaan. Sillä on laatua parantavaa vaikutusta GST mukaisiin hierarkioihin eli prosesseihin ja rakenteisiin. Siten systeemin toiminnan tavoitteellisuus ja vakaus voidaan turvata paremmin tulevaisuudessa. Eettisen hakkeroinnin tiedoilla voidaan esimerkiksi luoda selkeämpiä suunnitelmia haavoittuvien osa-alueiden kehittämiseksi. Samalla voidaan luoda kehittämisohjelmia, joilla pistemäisten pikakorjausten sijaan tehtäisiin suunnitelmallista ennaltaehkäisevää kehitystyötä kyberturvavalmiuden parantamiseksi.

Organisaatiokulttuurin muutos

Menettelytapojen muutos voi johtaa kokonaisuudessaan parempaan organisaatiokulttuuriin, joka on aikaisempaa avoimempi, suunnitelmallisempi ja varautuneempi haasteellisiin tilanteisiin. Organisaatio on asiantuntijoiden mukaan tällöin tehokkaampi, innovatiivisempi ja vakaampi.

> *"Tilaamisen syyt: A. Tehdään enemmän rahaa ja säästetään kustannuksia tai B. joku käskee tekemään."*

Eettisen hakkeroinnin tilaamiseen asiantuntijat näkevät monia syitä, jotka voidaan tiivistää kahdeksi teemaksi: liiketoiminnan kannattavuuden parantaminen ja normien noudattaminen. Asiakkaiden luottamus organisaation toiminnan turvallisuuteen ja palvelun tarjonnan luotettavuuteen voi parantua. Toisaalta yrityksen johto voi haluta testata oman toimintaprosessin haavoittuvuudet ja tilata hakkeroinnin palveluna. Toimeksianto voikin tulla myös yrityksen korkeimmalta johdolta.

"Ristiriita organisaation sisällä on, että ylin johto joka tämän palvelun on tilannut, on sitoutunut sen toimeenpanoon ja haluaa kehittää tämän tyyppistä toimintaa. Ongelma tulee siitä, että miten saadaan henkilöstö kehittämään toimintatapoja ja kehittämään toimintaansa. Siinä kyllä sarkaa riittää."

Laajemmin tarkasteltuna syyt eettisen hakkeroinnin tilaamiselle voivat olla asiakkaiden toiveet, normit ja lainsäädäntö, liiketaloudellisen kannattavuuden parantaminen ja kustannussäästöt, tietoisuuden lisääminen kybertoimintaympäristön uhkista ja mahdollisuuksista sekä johdon keino muutoksien aikaansaamiseksi organisaatiossa.

Yhteistyön kehittäminen

Eettisen hakkeroinnin prosessi saattaa johtaa organisaatioissa menettelytapoihin, joissa kyberturvallisuuden testaamisesta tulee jatkuvaa. Suuremmat organisaatiot saattavat tällöin päätyä ratkaisuun, jossa systeemille perustetaan oma eettisen hakkeroinnin tiimi. Alalle hyvin tyypillistä on, että asiantuntijoita haetaan tiimiin ympäri maailmaa, sillä hakkeroinnin toteutus on kybermaailmassa aika- ja paikkariippumatonta. Palvelun voi tuottaa vaikkapa toiselta puolelta maapalloa.

"Eettinen hakkerointi on nykyään yhä enemmän verkostoitunutta ja globaalia. Tällöin organisaation sijainti on yhä epärelevantimpi asia testauksen näkökulmasta."

Asiantuntijat näkevät eettisen hakkeroinnin ja kyberturvallisuuden testauksen tulevaisuudessa laajempana ja merkittävämpänä osana kyberturvallisuuden testausta. Tällä hetkellä eettinen hakkerointi on vain pieni osa kaikesta kyberturvallisuuden testauskokonaisuudesta. Testauksen tuottamisen sijainti on tulevaisuudessa epärelevantimpaa ja sitä voi ostaa palveluna mistä vain, milloin vain. Asiantuntijoiden mukaan tulvaisuudessa kyberturvallisuuden testaaminen voi olla ehtona joidenkin tuotteiden alihankintaverkostojen osaksi pääsemiselle. Tällöin eettinen hakkerointi ja sen avulla saatu tarkistustulos voisivat olla eräs kriteeri verkostoon pääsemiselle.

"Eettinen hakkerointi voi ainoastaan todistaa, että jotakin on pielessä. Se ei voi koskaan todistaa asioiden olevan hyvin. Tässä moni tekee väärin."

Toisaalta eettistä hakkerointia ei asiantuntijoiden mukaan kannata käyttää systeemin vahvuuksien etsimiseen. Tämä johtuu eettisessä hakkeroinnissa käytettyjen mustahattuhakkerien menetelmien tarkoituksesta eli haavoittuvuuksien – ei vahvuuksien – tunnistamisesta ja etsimisestä. Tästä huolimatta eettinen hakkerointi voi varmasti avartaa organisaation toimijoiden ymmärrystä kybermaailma tarjoamista mahdollisuuksista.

Mahdollisuuksien kartoittaminen ja haavoittuvuuksien korjaaminen

"Eettisessä hakkeroinnissa raportoidaan prosesseissa olevista puutteista ja ne johtavat tietoturvapolitiikan tai -strategian kehittämiseen. Usein dokumentit päivitetään, mutta ihmisen arkipäiväiseen toimintaan vaikutus on utopiaa. Tämä johtuu siitä, että ihminen menee sieltä, mistä aita on matalin."

Ihminen on kyberturvallisuuden heikoin lenkki, mutta toisaalta myös organisaatioiden tärkein elementti. Ihmiset kartoittavat mahdollisuuksia ja kehittävät organisaation toimintaan. Näiden molempien havaintojen tunnistaminen on tärkeää, jotta ihmiset saadaan mahdollisimman itsenäisesti vaikuttamaan omaan toimintaansa kyberturvallisuusasioissa.

Oppiminen, kehittyminen ja innovatiiviset ratkaisut

"Eettisessä hakkeroinnissa on ympärillä ihmisiä, jotka ovat aidosti kiinnostuneita siitä, miten erilaiset asiat toimivat, jotta saataisiin toimimaan ne paremmin."

Kuten aiemmin tässä tutkimuksessa on esitetty, hakkeroinnin alkuperäisenä tavoitteena on ollut uudenlaisten ja innovatiivisten ratkaisujen löytäminen. Eettisen hakkeroinnin avulla voidaankin löytää uusia kybermaailman mahdollisuuksia ja kehittää uusia ratkaisuja myös vaikkapa johtamiseen, tiimityöhön ja vuorovaikutussuhteiden parantamiseen.

"Turvallisuudessa – ei pelkästään kyberturvallisuudessa – on kyse ympäristön havainnoinnista ja totuttujen asioiden uudella tavalla näkemisestä."

Turvallisuuden parantamisen lisäksi hakkeroinnin keinoja voi hyödyntää kaikessa toiminnassa ja kehittää organisaation uusia toimintatapoja luovia ratkaisumalleja. Jokainen organisaation työntekijä on tällöin itsenäinen hakkeri, joka pyrkii omilla toimillaan kehittämään rakenteita ja prosesseja paremmiksi. Paras tieto työnteon sujuvoittamisesta on yleensä työn tekijöillä itsellään. Parhaimmassa tapauksessa kaikki ideat yhdessä luovat täysin uudenlaisia ja joustavia tapoja toimia. Yleisen systeemiteoriankin mukaan uudet ratkaisut ja toimintatavat mahdollistavat systeemien kasvamisen.

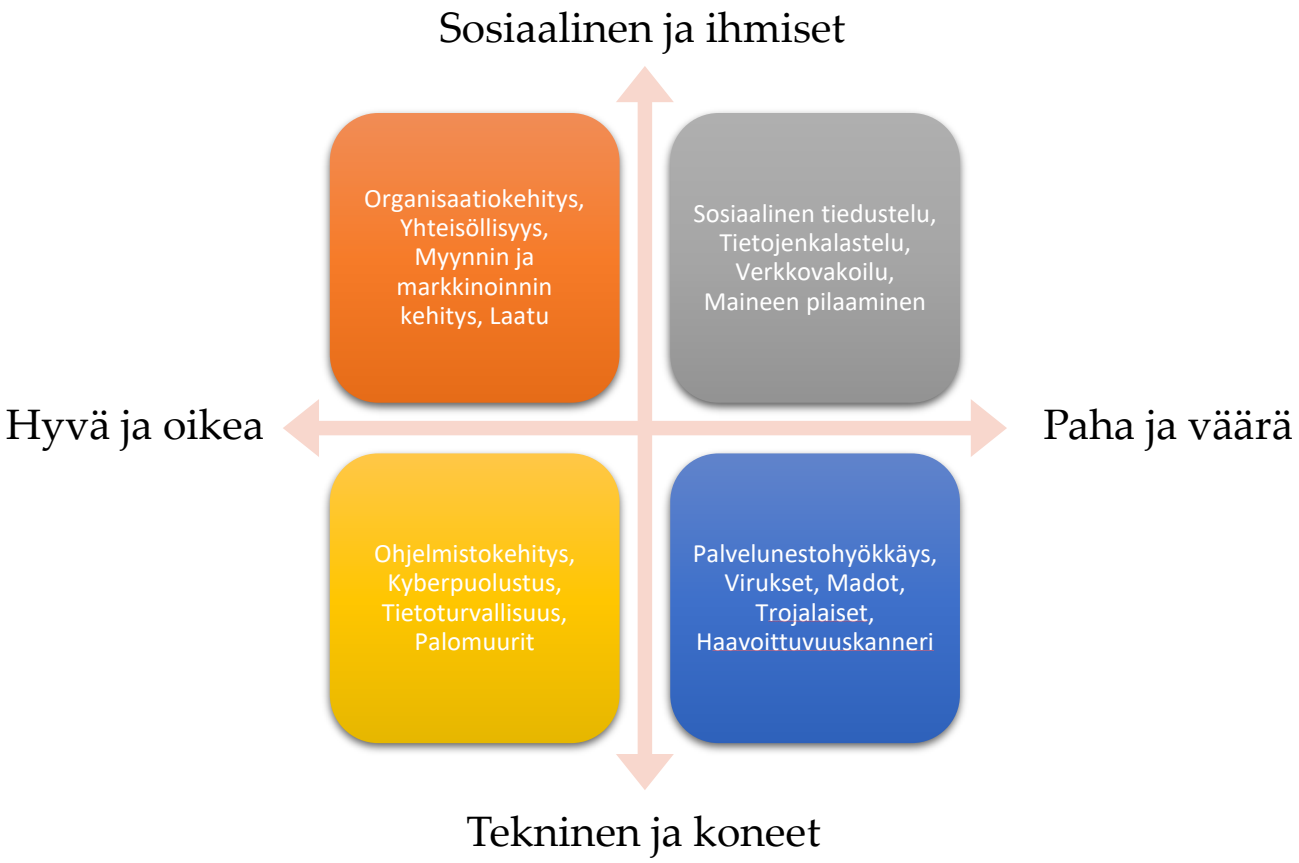
"Hakkeroinnin tulokset eivät ole salaisia, vaan ne käydään yhdessä läpi. Tämä lisää avointa kulttuuria. Tämä ei ole häpeän asian, vaan edistystä kulttuuriin. Avoimuus on yhteistyötä."

Organisaation toimintatapojen kehittäminen ja oppiminen liittyy myös sosiaalisen tiedustelun (engl. social engineering) toimintatapoihin. Ihminen on asiantuntijoiden ja kirjallisuuden mukaan aina

systeemien heikoin lenkki. Tämän vuoksi eettisen hakkeroinnin raporttien käsitteleminen työntekijöiden kanssa on hyvin tärkeää. Jokaisen tulisi pystyä kehittämään menettelytapojaan ja omia heikkouksiaan. Näillä menettelytavoilla organisaatioiden kyberturvallisuus paranee.

6.4. Hakkeroinnin vaikutukset organisaatioihin

Hakkeroinnilla voidaan vaikuttaa organisaation toimintaan monella tavalla hyvässä ja pahassa. Kuvassa 8 on esitetty koko tutkimusaineiston avulla rakennettu hakkeroinnin sovelluksien nelikenttä. Hakkerointi on innokasta järjestelmien ja systeemien tutkimista, jossa keksitään erilaisia ratkaisuja asioihin ja nautitaan niiden tekemisestä. Hakkerointia voi käyttää moraalisesti oikeiden menettelytapojen kehittämiseen ja ne voivat kohdistua sosiaalisiin ja teknisiin systeemien rakenteisiin ja prosesseihin. Sosiaalisia ovat esimerkiksi johtamiskulttuurin kehittäminen tai yhteisöllisyyden ja yhteistyön parantaminen. Teknisiä puolestaan olisivat esimerkiksi haavoittuvuuksien korjaaminen ja ohjelmistokehityksen laadun parantaminen.



Kuva 8. Tämän tutkimuksen mukaan hakkeroinnin vaikutukset organisaatiossa riippuvat tavoitteista ja käytetvistä menettelytavoista niiden saavuttamiseksi.

Hakkerointia voidaan käyttää myös pahoihin tarkoituksiin. Sosiaalisia muotoja tästä olisivat esimerkiksi teollisuusvakoilu, perusteettomien huhujen liikkeelle laskeminen tai sosiaalinen tiedustelu. Tekniset menetelmät voivat olla esimerkiksi palvelunestohyökkäyksiä tai troijalaisia. Yhteistä kaikille edellisille on se, että hakkeroinnin sovelluksia on rajattomasti. Hakkerointi on innovatiivinen keino tuottaa uusia asioita. Keskeistä on ymmärtää, että hakkeroinnin vaikutukset organisaatioon määrää käyttötarkoitus ja todelliset organisaation käyttämät menettelytavat.

7. Tutkimustulokset

Tässä luvussa kerrotaan tutkimuksen tulokset analyyttisesti ja kriittisesti pohtien sekä vastataan tutkimuskysymykseen. Tarkasteluun sisältyy teoriaosuuden sopivuuden arviointi aineistonhankintamenetelmillä kerättyyn kokemustietoon verrattuna. Tutkimustulokset perustuvat kirjallisuuslähteisiin, yleiseen systeemiteoriaan ja teemahaastatteluihin.

Digitaalitekniikan kehittyminen on mahdollistanut digitalisaation ja tuottavuuden parantamisen useissa organisaatioissa. Fyysisen maailman toiminnot ovat yhä riippuvaisempia kybermaailman eli digitaalisen maailman tapahtumista. Kybermaailman kautta hoidetaan kaikkea arkipäivän askareista valtavien fyysisten toimintojen ohjailemiseen. Toiminnoista on tullut aika- ja paikkariippumattomia. Kyberympäristössä toimii erilaisia ihmisen kehittelemiä kokonaisuuksia: sosiaalisia verkostoja ja hyvin teknisiä koneiden muodostamia järjestelmiä. Yhdessä nämä elementit muodostavat systeemejä.

Kybertoimintaympäristön entistä suurempaa kytkeytymistä organisaatioiden toimintoihin voidaan käyttää moraalisesti hyviin ja pahoihin tarkoituksiin. Etiikka moraalia tutkivana tieteenä voi määrittää hyvän ja pahan rajat eri näkökulmista. Hyvät keinot ovat uusia menetelmiä ratkaista erilaisia ongelmia innovatiivisesti, kehittää toimintatapoja ja hyödyttää näin yhteiskuntaa. Hakkerin alkuperäinen määritelmä on todennäköisesti tarkoittanut innokasta järjestelmien ja systeemien tutkijaa, joka keksii erilaisia ratkaisuja asioihin ja nauttii ratkaisujen tekemisestä. Hakkeri-sanan nykyinen konnotaatio on yleisesti moraalisesti paheksuttava. Pahat keinot ovat ilkeämielisiä, itsekkäitä ja heikentävät kybertoimijoiden kykyä kehittyä. Tällöin niitä voidaan kutsua uhkiksi systeemin kehittymiselle. Kohdatessaan organisaation pahojen hakkerien tuottamat pahat teot voivat tuottaa riskien täyttymistä eli arvonmenetyksiä. Pahimmassa tapauksessa organisaation toiminta loppuu riskien toteuduttua. Tämän vuoksi organisaatiot pyrkivät ennaltaehkäisemään kybermaailman uhkia ja välttämään riskejä kehittämällä kyberturvavalmiuttaan.

Eettinen hakkerointi on kokoelma menetelmiä, joiden avulla systeemin kyberturvallisuutta voidaan testata ja arvioida. Testauksessa käytetään pahamielisten hakkereiden käyttämiä menetelmiä hyviin tarkoituksiin. Testaajia kutsutaan tällöin valkohatuiksi. Hakkerointi jakautuu viiteen vaiheeseen, joita ovat tiedustelu, skannaus, haltuunotto, hallussapito ja jälkien peittäminen. Tiedusteluvaiheessa

kerätään tietoa kohdesysteemistä. Skannausvaiheessa tietoa jatkojalostetaan ja hankitaan tarpeen mukaan lisää. Haltuunottovaihe sisältää varsinaisen systeemiin hyökkäämisen. Hallussapitovaiheessa pyritään saavuttamaan hakkeroinnin tavoitteet. Jälkien peittämisvaiheessa pyritään poistamaan todisteet hakkeroinnin olemassaolosta. Tämä hakkeroinnin viimeinen vaihe korvataan eettisessä hakkeroinnissa monesti tärkeimmällä raportointivaiheella, jonka tarkoituksena on tuottaa tietoa organisaation hyödynnettäväksi ja jatkojalostettavaksi. Raporttiin kirjataan havainnot kyberturvallisuutta heikentävistä tekijöistä eli haavoittuvuuksista, eettisen hakkeroinnin prosessista ja suorista kehitysehdotuksista systeemin kyberturvavalmiuden parantamiseksi. Eettinen hakkerointi ei yksinään paranna juurikaan organisaation kyberturvavalmiutta, vaan ainoastaan testaa ja raportoi tuloksistaan kohdeorganisaatiolle. Varsinaiset kyberturvallisuutta parantavat menettelytavat voidaan saavuttaa eettisen hakkeroinnin tuloksen synnyttämällä tiedolla ja ymmärryksellä kyberturvallisuuden tilasta. Eettinen hakkerointi ei paranna kyberturvavalmiutta ilman organisaatioiden määrätietoisia menettelytapojen muutoksia.

Organisaatiot ovat avoimia systeemejä. Organisaatioiden toimintaa voidaan selittää yleisen systeemiteorian avulla. Sen mukaan fyysinen maailma ja kybermaailma muodostavat toimintaympäristön, jossa avoimet systeemit vuorovaikuttavat toistensa kanssa. Organisaation vuorovaikuttavat myös sisäisesti ja ovat rakenteeltaan holistisia. Kaikilla avoimilla systeemeillä on yhteisiä ominaisuuksia, joita ovat vakautuvuus, tulevaisuusriippuvuus, hierarkia, kokonaisvaltaisuus, jatkuva keskittyminen, kasvaminen, haje, edistyvä segregaatio, kilpaileminen ja itsenäistyminen. Organisaatioiden tavoitteena on mahdollisimman vakaa tila, joka mahdollistaa kasvamisen ja kilpailemisen. Organisaatiot koostuva hierarkialtaan prosesseista ja rakenteista. Prosessit hoitavat erilaisia systeemin tilaa ylläpitäviä tehtäviä. Rakenteet muodostavat toiminnan pohjan ja rakenteiden lisääntyminen merkitsee kasvua. Prosessit saattavat esimerkiksi keskittää toimintoja tiettyjen systeemin osien eli elementtien hoidettavaksi. Prosessit saattavat myös muuttaa rakenteita jakamalla ja itsenäistämällä osia organisaatioissa.

Pienetkin muutokset vaikuttavat koko organisaation toimintaan kokonaisvaltaisesti. Eettisellä hakkeroinnilla voidaan tunnistaa systeemin vakauden ja kybermaailmassa toimimisen kannalta erilaisia haavoittuvuuksia ja saada lisätietoa toiminnan kehittämiseksi. Teoria selittää hyvin eettisen hakkeroinnin tuloksena tehtävien menettelytapojen vaikutukset systeemin kyberturvallisuuden parantamiseksi. Se sopii hyvin tutkimuksen viitekehykseen ja on perusteltu valinta organisaatioiden eli

systeemien toimintaan keskittyvässä tutkimuksessa. Teoria sopii myös hyvin selittämään fyysisen maailman ja kybermaailma yhteyttä kokonaisuutena.

Eettisen hakkeroinnin mahdollistamia menettelytapoja organisaatioiden kyberturvallisuuden parantamiseksi on osana tutkimuksen edistymistä ja analyysia tunnistettu monia. Kybertoiminnan ongelmien kokonaiskuva paranee organisaation johdon ja henkilöstön keskuudessa. Kybermaailman huomioon ottaminen mission, vision, selvityksen, strategian ja toimeenpanon muodossa parantaa kybertoiminnan turvallisuutta. Tämä johtuu tulevan epävarmuuden vähenemisestä toiminnan ollessa vakaampaa ja suunnitelmallisempaa. Prosessien ja rakenteiden laatu paranee, kun esimerkiksi pistemäisten korjausten sijaan ennaltaehkäistään kyberuhkia suunnitelmallisesti, hallitusti ja kaikki osa-alueet huomioon ottaen. Organisaation johdon parempi ymmärrys kybermaailmasta antaa perusteita riittäville resursseille ja resurssien järkevälle käyttämiselle. Vähäinen ja liiallinen resurssien käyttäminen kyberturvallisuuden paranemiseksi voidaan paremmin ottaa huomioon. Samalla voidaan tarkastella eettisen hakkeroinnin toiminnan jatkuvuutta, omaa testaustiimiä tai kybertoimintojen ulkoistamisen hyötyjä.

Eettisen hakkeroinnin tuottamat tiedot mahdollistavat organisaation kyberkriittisten kohteiden tunnistamisen ja niiden menettelytapojen kehittämisen. Samalla voidaan parantaa häiriötiloista palautumisen menettelytapoja ja prosesseja. Näihin liittyvät esimerkiksi kriisiviestintä ja nopeat toimet vaikkapa palvelunestohyökkäyksen tai tunkeutumisen havaitsemisen jälkeen. Parhaimmillaan organisaation sisäinen yhteistyö eri osastojen välillä paranee kyberturvallisuuteen liittyvissä asioissa ja organisaatiokulttuurissa, kuten yhtenäisessä käyttäytymisessä sosiaalisen tiedustelun kohteeksi joutumisen aikana. Myös hakkeroinnin alkuperäinen määritelmä eli uusien ideoiden tuottaminen ja niiden soveltaminen voi parantaa organisaation kyberturvavalmiutta. Ihminen on organisaation kyberturvallisuuden heikoin lenkki ja suurin riski. Tästä syystä pienetkin parannukset ovat merkittäviä kokonaisvaltaisen kyberturvavalmiuden kohottamiseksi.

Kriittisesti tutkimusaineistoa tarkastellen voidaan todeta eettisen hakkeroinnin raportoinnin jälkeisten riittävien toimien herättävän organisaation henkilöstön ajattelemaan käyttäytymistään kyberympäristöissä. Henkilökohtainen palaute henkilöstölle auttaa ymmärtämään toimintatapojen muutoksen tärkeyttä osana laajempaa organisaation kyberturvavalmiutta. Oppimista, kehittymistä ja innovaatioita syntyy, kun kaikki tiedostavat ympäröivän kybertodellisuuden mahdollisuudet ja

siihen liittyvät riskit. Välinpitämättömyys ja tietämättömyys ovat useimmin syitä organisaation henkilöstön huonoon kyberturvavalmiuteen. Asennemuutos johtotasolla ja henkilöstön keskuudessa vaaditaan, jotta eettisen hakkeroinnin raportit muuttuvat todellisiksi paremmiksi menettelytavoiksi kybermaailmassa toimittaessa. Eettisellä hakkeroinnilla ei siis voida saavuttaa mitään valmista tai pysyvää, mikäli menettelytapoja ei määrätietoisesti lähdetä organisaatioissa edistämään.

8. Johtopäätökset

Tässä luvussa arvioidaan teorian ja empiria yhteensopivuutta, tutkimuksen onnistumista ja tutkimuksen yhteiskunnallista nykypäivän sekä tulevaisuuden arvoa. Lopuksi pohditaan eettisen hakkeroinnin tutkimuksen mahdollisia jatkotutkimusmahdollisuuksia ja tulevaisuuden käyttökohteita.

8.1. Kybervalmis organisaatio on nykypäivää

Kybermaailma mahdollistaa aiemmin mahdottomilta tuntuneita asioita. Työtä voidaan tehdä useammin kotona, työpaikalla tai vaikkapa maapallon toisella puolella. Automaatti tai yksi ainoa henkilö voi hallita valtavia fyysisiä toimintoja kompleksisen kyberverkon kautta. Tietoa voidaan varastoida, etsiä ja jalostaa aiempaa helpommin ja nopeammin ajasta ja paikasta riippumatta. Ubiikin (engl. *ubiquitous*) yhteiskunnan kehittyminen ja joka paikan tietotekniikan yleistyminen kaikkialla fyysisessä ympäristössä verkottaa systeemit kyberavaruuden elementeiksi. Turvallisuus ja turvattomuus ovat olemassa kybermaailmassakin. Uusi tilanne vaatii uusia keinoja ja menetelmiä kyberturvallisuuden parantamiseksi ja vakaiden toimintamahdollisuuksien säilyttämiseksi.

Eettinen hakkerointi on vain pieni osa kyberturvallisuuden monisyisestä kentästä. Tästä huolimatta sen avulla voidaan saavuttaa systeemeistä koostuvassa organisaatiomaailmassa useita hyviä menettelytapoja, jotka eivät rajoitu vain kyberturvallisuuden parantamiseen. Eettisen hakkeroinnin hyödyntäminen vaatii kuitenkin enemmän kuin vain asioiden selvittämisen. Se vaatii käytäntöön sovellettavia menettelytapoja, joita organisaation henkilökunta, johtajat ja toimijat soveltavat arkipäiväiseen toimintaansa. Nämä toimijat ovat kaikki arkipäivän hakkereita – menettelytapojen kehittelijöitä, jotka ovat kyberturvallisuuden parantamisessa kaikki kaikessa. Näin menettelevä organisaatoin on aikaisempaa innovatiivisempi, oppii virheistään ja kehittää itsenäisesti ratkaisuja ongelmiinsa.

Organisaation kyberturvallisuutta voidaan parantaa kyberturvavalmiutta parantamalla. Käytännössä tämä tarkoittaa kompleksiseen kybertoimintaan valmistautumista. Kokonaiskuvaa voitaisiin parantaa esimerkiksi hankkimalla säännöllisin määräajoin toteutettava eettinen hakkerointi ja sen perustella voitaisiin luoda kyberturvallisuuden parantamisen toimeenpano-ohjelma. Toimeenpano-

ohjelman missio eli tehtävä olisi parantaa organisaation kyberturvavalmiutta ja ohjata sen jalkauttamisessa. Ohjelmasta löytyisi selvät vastuusuhteet ja toimenpiteet, joita tulisi tehdä parempaa valmiuteen pääsemiseksi. Ohjelmaa varten tarkasteltaisiin kybermaailmaa kokonaisuutena muillakin keinoilla kuin vain eettisen hakkeroinnin keinoilla. Tällöin saataisiin selkeästi kokonaisvaltaisempi käsitys kybermaailma mahdollisuuksista ja uhkista. Toimeenpano-ohjelmalle voitaisiin antaa omat resurssit, joiden pohjalta menettelytapojen aktiivista kehittämistä edistettäisiin. Ohjelma tähtäisi kokonaisvaltaisuuden lisäksi keskeisten kriittisten kohteiden parantamiseen. Toimenpiteet voisivat olla erilaisia valmiusharjoituksia, koulutuksia, tietojärjestelmien ja tietoverkkojen kehittämistä, laiteinvestointien suunnittelua, tilannekuvan parantamista, luottamuksen parantamista, yhteistyön kehittämistä ja siiloutumisen estämistä. Toimenpide-ohjelma olisikin kokonaisvaltainen, konkreettinen ja suoraan toimeenpantava konsepti.

Edellä esitetty esimerkki on vain yksi tapa parantaa kyberturvavalmiutta kokonaisvaltaisesti. Jokainen yksittäinen keino turvallisuuden parantamiseksi on tärkeä, mutta kokonaisvaltaisella ja analyyttisellä lähestymistavalla voidaan tavoitteet saavuttaa varmemmin. Näin toimiva systeemi on kybervalmis toimija. Sillä on kyky käsitellä kybermaailman mahdollisuuksia ja vaaroja analyyttisesti.

Nykyään kybermaailma läpäisee koko yhteiskunnan ja koskettaa tulevaisuudessa yhä useampia. Yhteiskunta muodostuu organisaatioista – systeemeistä. Organisaatioiden ollessa kyberturvavalmiita ovat myös niistä muodostuvat yhteiskunnat kyberturvavalmiita. Kybervalmiit organisaatiot ovat tästä syystä yhteiskunnalle tärkeitä. Ilman niiden kyberturvavalmiutta ei yhteiskuntakaan ole valmis. Tämän tutkimuksen yhteiskunnallinen arvo perustuu näiden menettelytapojen jäsentämiseen ja aiempaa helpompaan tunnistamiseen organisaatioissa. Näin organisaatiot voivat toimia tavoitteellisemmin ja saavuttaa tuloksia paremmin.

8.2. Yhteiskunnan kyberturvallisuus koostuu systeemien kybervalmiuksista

Tässä tutkimuksessa on tutkittu organisaatioiden menetelmiä eettisen hakkeroinnin aikana ja menettelytapoja sen jälkeen. Tutkimus on tuottanut uutta jäsenneltyä tietoa tutkimuskirjallisuuden ja teemahaastattelujen pohjalta. Tutkimuksella on pyritty näkemään jatkuvasti esillä olevan sovelluspinnan yläpuolelle systeemiteoreettisen näkökulman avulla. Aihetta on tarkastelu monipuolisesti esimerkkien ja kuvien avulla. Toisaalta tutkimusprosessin aikana on pyritty jatkuvasti saamaan vas-

tauksia tutkimuskysymykseen, eikä tilaa liialliselle aiheen sivuuttamiselle ole annettu. Kaikkien tutkimuslähteiden kohdalla on noudatettu lähdekritiikkiä ja tutkimuskirjallisuutta on tarkasteltu kriittisesti. Kriittinen näkökulma korostuu erityisesti varovaisuutena kausaalipäätelmien tekemisessä ja teemahaastatteluiden analyysien tekemisessä. Kyberturvallisuuden tutkimusalue on varsin uusi tutkimusalue, joten liian pitkälle vietyjen päätelmien tekeminen ei olisi järkevää niin tutkimuksellisesti kuin metodologisestikaan.

Teemahaastattelut yleisemmin olivat onnistuneita, vaikka kaikki asiantuntijat eivät olleet kaikista asioista yksimielisiä. Kokonaisuudessaan haastatteluita voidaan kuitenkin pitää hyvin onnistuneina ja otoskokoa riittävänä. Teemahaastattelun hyvänä puolena on ollut uuden tutkimusalan tiedon tuottamisen tarpeen täyttäminen. Teemahaastattelut ovat sopineet tähän tarkoitukseen erittäin hyvin.

Yleinen systeemiteoria on ollut olennainen osa tätä tutkimusta. Sen avulla on löydetty organisaatioiden kehittymiseen ja toimintaan liittyvät perusperiaatteet. Ilman yleistä systeemiteoriaa olisi tutkimus ollut pinnallinen ja huonommin jäsennelty epäyhtenäinen kokonaisuus. Teoria on auttanut tutkimusprosessissa, sillä sen avulla on voitu perustella eettisen hakkeroinnin menettelytapojen vaikutukset organisaatioihin. Teoriaa on tarkastelu kriittisesti ja sen lähiteoriat on otettu huomioon tutkimusprosessin aikana. Yleinen systeemiteoria valittiin monitieteisyyden, hyvän sovellettavuuden ja laajojen aiempien sovelluksien onnistumisen takia.

8.3. Eettisen hakkeroinnin menettelytapojen tulevaisuus

Kybermaailman tutkimus vaatii jatkuvuutta nopean teknologisen kehittymisen ja uusien sovelluksien ilmestymisen takia. Toisaalta kybermaailman tutkimuksessa vaaditaan samanlaista teoreettista pysyvyyttä kuin fyysisenkin maailman ilmiöiden selittämisessä. Uutta tutkimusta tarvitaan selittämään vielä avoimina olevia kysymyksiä.

Tulevaisuudessa eettistä hakkerointia sovelletaan mahdollisesti yhä laajemmin esimerkiksi kybertoimijoiden välisissä sopimuksissa, ja siitä saattaa tulla jopa normi tai standardi. Laitekannan hurja kasvaminen tulee lisäämään hakkeroinnin kosketuspintaa lähes kaikkialle ubiikin yhteiskunnan osiin. Organisaatioiden sijainti muuttuu toiminnan kannalta yhä merkityksettömämmäksi, kun kybermaailma on läsnä kellonajasta riippumatta.

Jatkotutkimuksen aiheena olisi kiinnostavaa tietää kyberturvallisuuteen liittyvistä muista keinoista tavoitella kyberturvavalmiuden parantamista. Toisaalta olisi mielenkiintoista selvittää eettisen hakkeroinnin teknisiä menetelmiä entistä tarkemmin. Kolmanneksi olisi mielenkiintoista saada lisää tietoa ihmisen roolista digitaalisen maailman kautta tapahtuvien kybertoimintojen osana.

Lähdeluettelo

Aristotle 1999, *Nicomachean Ethics,* Batoche Books, Kitchener.

Beaver, K. 2013, *Hacking for Dummies,* 4th edn, For Dummies.

Bell, D.E. & LaPadula, L.J. 1973, *Secure Computer Systems: Mathematical Foundations*, National Technical Information Service.

von Bertalanffy, L. 1968, *General System Theory,* Braziller.

Blackburn, S. 2016, *Metaethics*, Oxford University Press.

Caldwell, T. 2011, "Ethical hackers: putting on the white hat", *Network Security,* vol. 2011, no. 7, pp. 10-13.

Canonical Ltd. 11.6.2016, *What is GNU/Linux?*. Haettu osoitteesta: https://help.ubuntu.com/lts/installation-guide/armhf/ch01s03.html [13.12.2016].

Clarke, R.A. & Knake, R.K. 2011, *Cyber War,* HarperCollins.

Colburn, T. 2015, *Philosophy and Computer Science,* Taylor and Francis.

Cooper, S.B. & van Leeuwen, J. 2013, *Alan Turing: His Work and Impact,* Elsevier Science.

Crisp, R. 1998, *Ethics and Meta-Ethics*, Informa UK Limited.

Engebretson, P. 2013, *The Basics of Hacking and Penetration Testing,* 2nd edn, Syngress Media Incorporated.

Erickson, J. 2003, *Hacking: The Art of Exploitation,* No Starch Press.

Falcon, A. 11.1.2016, *Aristotle on Causality*. Haettu osoitteesta: http://plato.stanford.edu/archives/spr2006/entries/aristotle-causality/ [31.10.2016].

Fieser, J. 21.11.2016, *Ethics* [Homepage of The Internet Encyclopedia of Philosophy], [Online]. Haettu osoitteesta: http://www.iep.utm.edu/ethics/#H2 [21.11.2016].

Fisher, A. 2014, *Metaethics: An Introduction,* Routledge.

Google 2009, *Chromium OS and Open Source*, Google.

Gots, J. 2016, *Hacker for the Hell of It: The Adventures of Kevin Mitnick*, The Big Think, Inc.

Graves, K. 2010, *CEH Certified Ethical Hacker Study Guide: Certified Ethical Hacker Study Guide,* Wiley.

Gunhild, H.G. 2012, "Security by any other name: negative security, positive security, and a multi-actor security approach", *Review of International Studies,* vol. 38, no. 4, pp. 1-25.

Haarala, R., Lehtinen, M., Grönroos, E., Kolehmainen, T., Nissinen, I., Eronen, R., Kantokoski, S. & Suorsa, M. 2016, *MOT Kielitoimiston sanakirja,* Kotimaisten kielten tutkimuskeskus.

Hadnagy, C. 2010, *Social Engineering,* 1st edn, Wiley.

Harisalo, R. 2008, *Organisaatioteoriat,* Tampere University Press.

Harju, J. 2015, *Tietoverkot ja tietoturva*, Tampereen teknillinen yliopisto.

Harris, S. 16.12.2016, *How security audits, vulnerability assessments and penetration tests differ*. Haettu osoitteesta: http://searchsecurity.techtarget.com/answer/How-security-audits-vulnerability-assessments-and-penetration-tests-differ [16.12.2016].

Helsingin Sanomat 2014, *Näin hakkeri murtautui ja miten sen olisi voinut estää – 3 tositapausta*, Helsingin Sanomat.

Henry, K. 2012, *Penetration Testing: Protecting Networks and Systems,* IT Governance.

Ihanus, J. 2010, *Ekvifinaliteetti*. Haettu osoitteesta: http://www.avoin.helsinki.fi/oppimateriaalit/psykologia/avoinsanasto.htm [10.12.2016].

Ince, D. 2013, *A Dictionary of the Internet* [Homepage of Oxford University Press]. Haettu osoitteesta: http://www.oxfordreference.com/view/10.1093/acref/9780191744150.001.0001/acref-9780191744150-e-1692 [17.12.2016].

Ives, B. & Learmonth, G. 1984, "The Information System as A Competitive Weapon", *Communications of the ACM,* vol. 27, no. 12, pp. 1193-1201.

Kärkkäinen, P. 23.11.2016, *Etiikan peruskäsitteitä*. Haettu osoitteesta: http://www.helsinki.fi/teol/kurssit/syste/03_peruskasitteita.shtml [23.11.2016].

Kerola, P. 22.10.2016, *Perjantain suuren verkkohyökkäyksen hurja tausta: Hakkerit valjastivat kodinkoneita aseikseen*. Haettu osoitteesta: http://yle.fi/uutiset/3-9246350 [13.12.2016].

Khaitan, S.K. & McCalley, J.D. 2015, "Design Techniques and Applications of Cyberphysical Systems: A Survey", *IEEE Systems Journal,* vol. 9, no. 2, pp. 350-365.

Khan, E. 2010, "Different Forms of Software Testing Techniques for Finding Errors", *International Journal of Computer Science Issues,* vol. 7, no. 3, pp. 11-16.

Kimppa, K.K. 2016, "(A short) Introduction to IT ethics (and IT ethics areas)", *Tietotekniikka ja yhteiskunta.* University of Turku, 13.4.2016.

Korkman, P. & Yrjönsuuri, M. 1998, *Filosofian historian kehityslinjoja,* Gaudeamus.

Krutz, R.L. 2008, *CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking,* Wiley.

Kungwani, P. 2014, "Risk Management", *Journal of Business and Management,* vol. 16, no. 3, pp. 83-86.

Lavington, S., Burton, C., Campbell-Kelly, M., Johnson, R. & Lavington, S. 2012, *Alan Turing and his Contemporaries,* British Computer Society.

Lavonen, J. & Meisalo, V. 30.7.2013, *Tiedon jäsentäminen*. Haettu osoitteesta: http://www.edu.helsinki.fi/malu/kirjasto/tieto/jasennys/index.htm [31.20.2016].

Libicki, M.C., Senty, D. & Pollak, J. 2014, *Hackers Wanted: An Examination of the Cybersecurity Labor Market,* Rand.

Malkin, G.S. & Parker, T.L. 1993, *Internet Users´ Glossary*, User Glossary Working Group.

Manion, M. & Goodrum, A. 2000, "Terrorism or civil disobedience", *ACM SIGCAS Computers and Society,* vol. 30, no. 2, pp. 14-19.

March, S.T. & Smith, G.F. 1995, "Design and natural science research on information technology", *Decision Support Systems,* vol. 15, no. 4, pp. 251-266.

Martin, E. 2016, *Metaethics*, Oxford University Press.

Maslow, A.H. 1943, "A theory of human motivation", *Psychological Review,* vol. 50, no. 4, pp. 370-396.

Merriam-Webster 27.11.2016, *A Brief History of 'Hack'*. Haettu osoitteesta: http://www.merriam-webster.com/words-at-play/hack-taxi-cab-driver-or-lousy-writer [27.11.2016].

Merriam-Webster 9.12.2016, *System*. Haettu osoitteesta: https://www.merriam-webster.com/dictionary/system [9.12.2016].

Mill, J.S. 1863, *Utilitarianism,* Fraser's magazine.

Mitleton-Kelly, E. 2003, *Complex Systems and Evolutionary Perspectives on Organisations : The Application of Complexity Theory to Organisations,* Emerald Group Publishing Limited.

National Science Foundation 2016, *Cyber-Physical Systems (CPS)*, National Science Foundation.

National Security Agency 3.3.2016, *National Security Agency*. Haettu osoitteesta: https://www.nsa.gov/what-we-do/cyber/ [13.12.2016].

Netmarketshare 18.12.2016, *Desktop Operating System Market Share*. Haettu osoitteesta: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qptimeframe=Y [18.12.2016].

Netmarketshare 18.12.2016, *Mobile/Tablet Operating System Market Share*. Haettu osoitteesta: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1 [18.12.2016].

Neusner, J. & Chilton, B. 2008, *The Golden Rule: The Ethics of Reciprocity in World Religions,* Continuum.

Opetushallitus 8.7.2009, *Etiikan keskeiset käsitteet*. Haettu osoitteesta: http://www02.oph.fi/etalukio/uskonto/kurssi3/sivu_3_2_1.html [20.11.2016].

Oxford English Dictionary 2016, *Hack* [Homepage of Oxford University Press]. Haettu osoitteesta: http://www.oed.com/view/Entry/83025?result=1&rskey=2Vdruz&amp [27.11.2016].

Oxford University Press 2016, *Empiria*. Haettu osoitteesta: http://www.oed.com.helios.uta.fi/view/Entry/61340?redirectedFrom=empiric#eid [10.12.2016].

Pietarinen, J. 3.3.2015, *Logos-ensyklopedia* [Eurooppalaisen filosofian seura ry:n kotisivu]. Haettu osoitteesta: http://www.filosofia.fi/node/6985 [21.11.2016].

Postel, J. 1981, *Internet Control Message Protocol*. Haettu osoitteesta: https://tools.ietf.org/html/rfc792 [17.12.2016].

Postel, J. 1981, *Transmission Control Protocol*. Haettu osoitteesta: https://tools.ietf.org/html/rfc793 [17.12.2016].

Pulliainen, M. 2016, *Isot nettihyökkäykset entistä isompia*, Aamulehti, 31.10.2016.

Ramachandran, V. & Nandi, S. 19.12.2005, "Detecting ARP Spoofing: An Active Technique", *ICISS 2005*, eds. J. Sushil & M. Chandan, Springer.

Rochlis, J. & Eichin, M. 1989, "With microscope and tweezers: The worm from MIT's perspective." *Communications of the ACM*, vol. 32, pp. 689-698.

Rojas, R. 1997, "Konrad Zuse's legacy: the architecture of the Z1 and Z3", *IEEE Annals of the History of Computing*, vol. 19, no. 2, pp. 5-16.

Ross, W.D. (ed) 2014, *Aristotle - Physics*, holybooks.com, http://www.holybooks.com/completes-aristotle-pdf/ [30.10.2016].

Routio, P. 3.10.2006, *Tutkimuksen rajaaminen*. Haettu osoitteesta: http://www2.uiah.fi/virtu/materiaalit/tuotetiede/html_files/132_empiir.html [23.10.2016].

Saaranen-Kauppinen, A. & Puusniekka, A. 2006, *Aineiston rajaaminen*. Haettu osoitteesta: http://www.fsd.uta.fi/menetelmaopetus/kvali/L6_2_1.html [23.10.2016].

Sachs, J. & Aristotle 1995, *Aristotle's Physics: A Guided Study*, Rutgers University Press.

Samson, P.R. 1959, *An abriged dictionary of the TMRC language*. Haettu osoitteesta: http://www.gricer.com/tmrc/dictionary1959.html [17.12.2016].

Saukkonen, P. 10.1.2011, *Aiheen valinta ja sen rajaaminen*. Haettu osoitteesta: http://www.mv.helsinki.fi/home/psaukkon/tutkielma/Aiheen_valinta.html [23.10.2016].

Scott, R., Liddell, H.G. & Jones, H.S. 1940, *System*, Clarendon Press.

Seeley, D. 1989, Password Cracking: A Game of Wits, *Communications of the ACM*, vol. 32, pp. 700-703.

Shirey, R.W. 2000, *Internet Security Glossary*, Network Working Group.

Simpson, M.T. 2012, *Hands-On Ethical Hacking and Network Defense*, Course Technology / Cengage Learning.

Stallman, R. 27.9.1983, *Initial GNU Announcement*. Haettu osoitteesta: https://www.gnu.org/gnu/initial-announcement.html [13.12.2016].

Taskinen, S. 2015, *Kuntien kyberturvavalmius*, Tampereen yliopisto, Johtamiskorkeakoulu.

Taylor, P. 1999, *Hackers,* Routledge.

Tieteen termipankki 17.7.2016, *Filosofia: etiikka*. Haettu osoitteesta: http://www.tieteentermipankki.fi/wiki/Filosofia:etiikka [20.11.2016].

Tieteen termipankki 19.12.2016, *Taloustiede: resurssi*. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Taloustiede:resurssi [19.12.2016].

Tieteen termipankki 13.12.2014, *Terminologiaoppi: käsite*. Haettu osoitteesta: http://www.tieteentermipankki.fi/wiki/Terminologiaoppi:käsite [31.10.2016].

Tietotekniikan termitalkoot 12.10.2000, *Sulautettu tietotekniikka*. Haettu osoitteesta: http://www.tsk.fi/tsk/termitalkoot/fi/hakemistot-267.html?page=get_id&id=ID0095&vocabulary_code=TSKTT [31.10.2016].

Torvalds, L. 31.7.1992, *LINUX's History*. Haettu osoitteesta: http://www.cs.cmu.edu/~awb/linux.history.html [31.10.2016].

Tutorialspoint 16.10.2016, *Penetration Testing Vs. Ethical Hacking*. Haettu osoitteesta: http://www.tutorialspoint.com/penetration_testing/penetration_testing_vs_ethical_hacking.htm [16.10.2016].

Valtionvarainministeriö 2009, *Valtionhallinnon tietoturvasanasto,* Valtionvarainministeriö.

Virta, S. 2011, "Turvallisuuden tutkimus", *Tiede ja ase,* vol. 69, pp. 112-126.

W3Techs 18.12.2016, *Usage Statistics and Market Share of Operating Systems for Websites, December 2016*. Haettu osoitteesta: https://w3techs.com/technologies/overview/operating_system/all [18.12.2016].

W3Techs 18.12.2016, *Usage Statistics and Market Share of Unix for Websites, December 2016*. Haettu osoitteesta: https://w3techs.com/technologies/details/os-unix/all/all [18.12.2016].

Wattles, J. 1996, *The Golden Rule,* Oxford University Press.

Wilhelm, T. 2013, *Professional Penetration Testing,* 2nd edn, Syngress Media Incorporated.

Zhou, Yajin & Jiang, Xuxian 2012, "Dissecting Android Malware: Characterization and Evolution", *IEEE Symposium on Security and Privacy* IEEE, 2012, pp. 95.

Liitteet

Liite 1. Kvalitatiivinen teemahaastattelurunko asiantuntijoille

Hei! Olen Santeri Taskinen Tampereen yliopistosta ja tutkin eettisen hakkeroinnin menettelytapoja organisaatioissa. Olisiko teillä aikaa vastata kysymyksiin liittyen organisaatioiden menettelytapoihin eettisessä hakkeroinnissa?

1. **Mitä eettinen hakkerointi mielestänne tarkoittaa?**

   Organisaatio voidaan käsittää rakenteeksi, jonka joukko ihmisiä muodostaa olemassaolon ja jonkin tarkoituksen perusteella. Tietotekninen kehittyminen on mahdollistanut erilaisiin verkostoihin pohjautuvien organisaatioiden kasvun globaalisti. Nykyisessä tietoyhteiskunnassa organisaatioiden menestys riippuu niiden kyvystä hallita muutosta ja toimia avoimesti - verkottuneesti. Toisaalta organisaatioista on tullut informaatioteknologian avulla aika- ja paikkariippumattomia rakenteita, joiden keskeisetkin toiminnot nojaavat verkkoihin.

2. **Mitä yhteistä organisaatioilla on eettisen hakkeroinnin kanssa tällä hetkellä?**

3. Tässä tutkimuksessa kyberturvallisuus tarkoittaa eri toimijoiden ja toimintojen kyberkokonaisuudesta aiheutuvaa turvallisuuden tilaa eli kattaa alleen kaikki tietoturvallisuuden osa-alueet ja niiden lisäksi kaiken fyysiseen maailmaan liittyvän ohjaamisen tietoverkkoja tai -tekniikkaa hyväksi käyttäen. **Vaikuttaako eettinen hakkerointi oikeasti organisaatioihin ja niiden toimintaan, kuten erilaisiin menettelytapoihin? Mihin menettelytapoihin? Entä kyberturvallisuuden todelliseen tasoon?**

   Aikaisemmin tekemässäni tutkimuksessa kuntaorganisaatioiden kyberturvavalmiudesta selvisi, että kunnan kaltaisen organisaation kyberturvavalmiuden keskeisiä tekijöitä ovat riittävät resurssit, tilannekuva ja johtaminen, auditoinnin, valvonnan ja luottamuksen kokonaisuus, henkilöstön koulutus ja osaaminen, avoimuus, maine ja imago, yhteistyö, lainsäädäntö ja standardit sekä turvallisuuden ulkoistaminen. (Näytetään liitettä 2.)

4. **Mihin kyberturvallisuuteen vaikuttaviin menettelytapoihin eettisellä hakkeroinnilla ei voida vaikuttaa? Miksi? Mihin voidaan? Miksi?**

5. **Voivatko kaikki organisaatiot hyödyntää eettistä hakkerointia toiminnassaan? Millaiset organisaatiot voivat? Onko eroja organisaatiotyyppien välillä?**

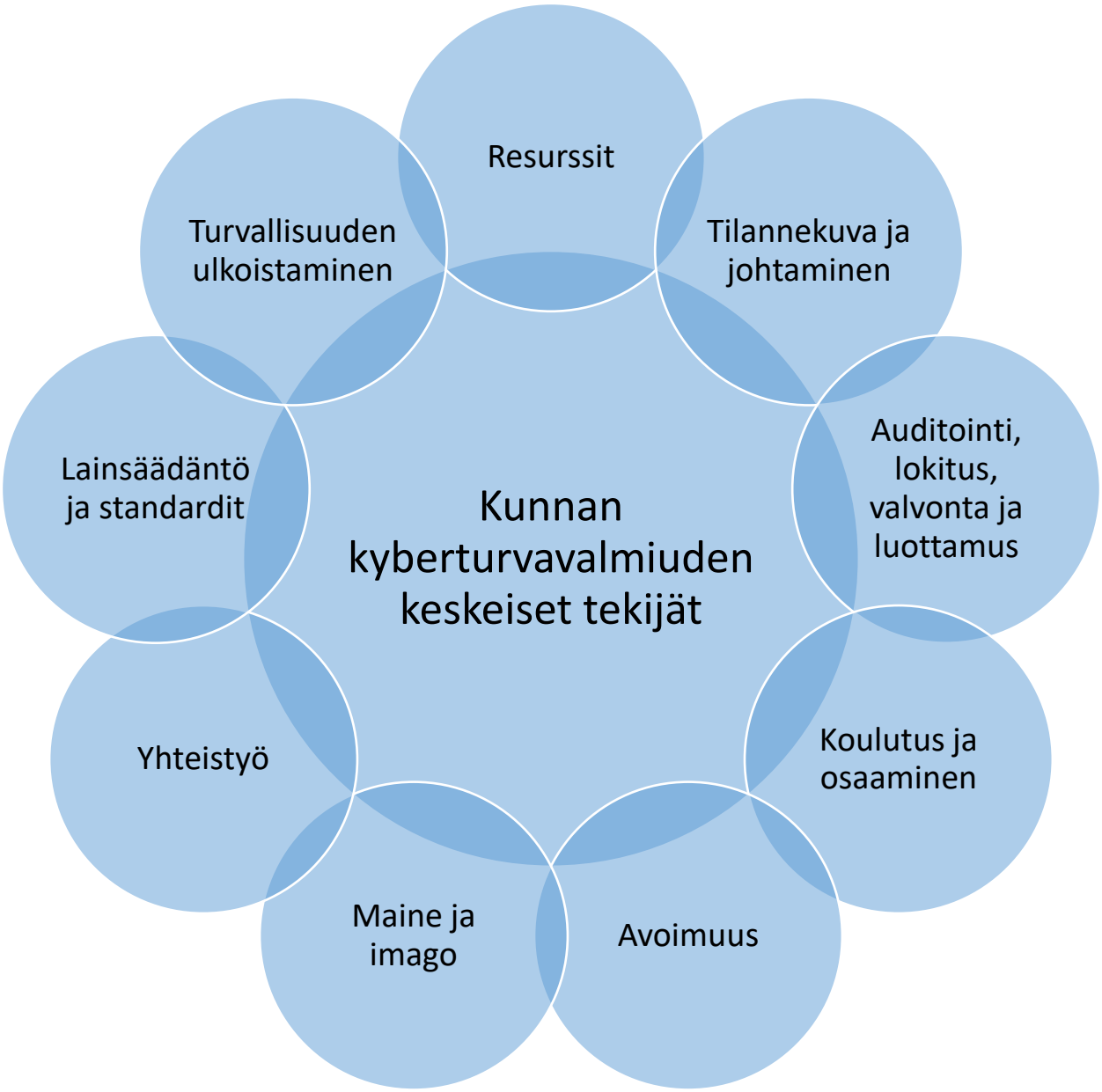
6. **Käytetäänkö eettistä hakkerointia tarpeeksi? Miksi/ Miksi ei? Miten se ilmenee käytännössä?**

7. **Lopuksi: Miten eettisen hakkeroinnin menetelmillä vaikutetaan organisaatioiden kyberturvallisuuteen?**

8. Aiheena oli eettisen hakkeroinnin menettelytavat organisaatioissa. **Onko jotakin olennaista jäänyt kysymättä?**

Kiitos paljon ajastanne!

Liite 2. Haastattelussa käytetty teemaympyrä



(Taskinen 2015)

TAMPEREEN YLIOPISTO