IKOLA, KATJA:

Maallikko ja asiantuntija tietoturvallisuudessa

Semioottinen analyysi Turvallisuus-lehden artikkeleista

TAMPEREEN YLIOPISTO
Sosiologian ja sosiaalipsykologian laitos

Pro gradu –tutkielma, 77 s., 2 liites.
Sosiologia
Huhtikuu 2006

TAMPEREEN YLIOPISTO
Sosiologian ja sosiaalipsykologian laitos

IKOLA, KATJA: Maallikko ja asiantuntija tietoturvallisuudessa. Semioottinen analyysi Turvallisuus-lehden artikkeleista
Pro gradu –tutkielma, 77 s., 2 liites.
Sosiologia
Huhtikuu 2006

Tutkimukseni tarkoitus on selvittää millaisena kulttuurisena ilmiönä tietoturvallisuus näyttäytyy. Tarkastelen tätä ilmiötä sen toimijoiden kautta. Tietoturvallisuus on hyvin asiantuntijavaltaista, joten pohdin asiantuntijuutta melko laajasti. Merkittävässä roolissa tietoturvallisuudessa ovat myös maallikot, joten tarkastelen myös maallikoiden asemaa. Tutkin myös asiantuntijan ja maallikon välistä suhdetta. Havainnoin näitä toimijoita ja koko ilmiötä myös osana riskiyhteiskuntaa. Tutkielma tarjoaa sosiologisen näkökulman yhdestä teknologisesta ilmiöstä kaikille tietoturvallisuudesta kiinnostuneille.

Käytän työssäni aineistona Turvallisuus-lehden artikkeleita. Lehti on suunnattu turvallisuusalan asiantuntijoille ja tietoturvallisuus kuuluu sen vakioaiheisiin. Lähestyn aineistoa semioottisesta näkökulmasta. Käytän A. J. Greimasin aktanttimallia, jotta voin nostaa esiin aineistossa esiintyvät toimijat ja niiden välisiä suhteita. Aktanttimallin avulla aineistosta hahmottuu narratiiveja, jotka puolestaan ilmentävät aineistossa kuvattua maailmaa. Väljänä viitekehyksenä analyysissani on toimijaverkkoteoria.

Aineistosta nousee esiin viisi kertomusta. Ensimmäisessä organisaatio tavoittelee parempaa tietoturvallisuuden tasoa erilaisilla yhteistyötavoilla. Toisessa tarinassa hyötyohjelma pyrkii torjumaan erilaiset tietoturvahyökkäykset. Kolmannessa puolestaan haittaohjelma haluaa levitä. Neljännessä kertomuksessa hyvä ihminen kehittää tietoturvallisuutta ja viimeisessä tarinassa paha ihminen tekee rikoksia.

Tarkastelen kertomuksissa esiintyviä toimijoita vielä tarkemmin ryhmittäin. Organisaatio näyttäytyy omassa itsenäisessä maailmassaan, jossa muilla toimijoilla ei ole vaikutusvaltaa. Tekniset toimijat eli hyöty- ja haittaohjelma osoittavat, että myös ei-inhimilliset toimijat voivat olla vuorovaikutuksessa ihmisten kanssa. Näitä toimijoita myös inhimillistetään. Asiantuntijat ovat merkittävässä asemassa tietoturvallisuudessa ja varsinkin tässä aineistossa, sillä heillä on valta määrittää ongelmat ja toimintatavat sekä muiden toimijoiden asema. Itse asiassa aineisto koostuu asiantuntijoiden välisistä dialogeista. Tietoturvallisuutta vastaan toimivat asiantuntijat kuten krakkerit saavat aineistossa yllättävän vähän huomiota. Silti tarve ymmärtää pahaa toista ja rajata se kauas itsestä nousee esiin. Maallikko mainitaan tietoturvallisuuden heikoimpana lenkkinä ja suurimpana riskinä. Maallikon nähdään silti olevan täysin riippuvainen muiden toimijoiden tekemisistä.

Tietoturvallisuusongelmat hankaloituvat koko ajan ja asiantuntijoiden työ vaikeutuu. Asiantuntijoiden olisi hyvä pohtia omaa toimintakulttuuriaan ja sen kehitysmahdollisuuksia. Varsinkin suhdetta maallikoihin olisi syytä kehittää, jotta tietoturvallisuudessa ei kohdattaisi ylitsepääsemättömiä ongelmia.

1 Tietoturvallisuus yhteiskunnassa

Tietoyhteiskunnalle ominaisena ilmiönä mainitaan informaatioteknologian vallankumous. Paljonhan siitä onkin puhuttu, kuinka tietokoneiden ja Internetin yleistyminen helpottaa elämäämme, kun monet palvelut siirtyvät verkkoon eikä fyysinen sijainti tai kellon aika vaikuta palvelun tai informaation saantiin. Alkuinnostuksessa kukaan ei osannut ajatella tai ainakaan ei tuonut julki, kuinka paljon maailman laajuista tietoverkkoa käytettäisiin myös kyseenalaiseen ja rikolliseen toimintaan.

Viime vuosina tietoturvallisuus on noussut usein julkisen keskustelun aiheeksi. Monenlaiset haittaohjelmat, kuten virukset ja madot ovat vaivanneet monia tietokoneen käyttäjiä, ja uutena ongelmana on phishing eli tietojen kalastelu huijausviesteillä. Viime aikoina paljon keskustelua on herättänyt pankkien nimissä lähetetyt sähköpostiviestit, joilla on pyritty saamaan asiakasnumeroita ja salasanoja, jotta tilit voisi tyhjätä. Pelkona onkin, että tämä on vasta alkua uusille huijaustavoille.

Työni käsittelee siis tietoturvallisuutta. Kokoavana tutkimusongelmana on, miten tietoturvallisuus rakentuu kulttuurisena ilmiönä? Lisäksi pohdin minkälaista asiantuntijuutta tietoturvallisuus edellyttää ja miten sitä ylläpidetään. Tietoturvallisuus on hyvin asiantuntijavaltaista, joten asiantuntijoilla on valta määrittää tietoturvallisuuden ongelmakohdat. Tarkastelen myös maallikon asemaa, joka yleensä ilmenee tietokoneen peruskäyttäjän muodossa. Asiantuntijan ja maallikon välinen konsensus tuntuu olevan melko heikko tietoturvallisuudessa, joten pureudun myös tähän ongelmaan. Lähestyn tietoturvallisuutta sen toimijoiden kautta alan sisäisessä keskustelussa. Jotta analyysini ei jäisi irralliseksi ympäristöstään, pohdin myös sitä, miten nämä toimijat nähdään yhteiskunnan jäseninä. Tietoturvallisuuden luonteen vuoksi mielestäni mielekkäintä on tutkistella toimijoita riskiyhteiskunnan näkökulmasta.

Usein tietoturvallisuus mielletään teknisenä ilmiönä, joten yhteiskuntatieteilijän kiinnostus aihetta kohtaan voi hämmentää. Tietoturvallisuus on uusi ja nopeasti muuttuva ilmiö, joten sen käsittely on kaikkea muuta kuin selvää. Keskustelu niin medioissa kuin kahvipöydissä on kiivasta, koska aihe koskettaa lähes meitä kaikkia. Valtiovaltakin on puuttunut asiaan monin tavoin, kuten perustamalla VAHTI:n

(Valtionhallinnon tietoturvallisuuden johtoryhmä), lisäksi Viestintävirastossa toimii tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittynyt ryhmä CERT-FI. Teknologia muokkaa ihmisten elämää ja ihmiset vaikuttavat teknologian kehitykseen. Teknologian ja yhteiskunnan suhde sitä vastoin on paljon kompleksisempi ja monitasoisempi kuin ihmisen ja teknologian suhde. Teknologia ei siis ole pelkkää tekniikkaa, vaan se on oikeastaan yhteiskunnan tuote. Esimerkiksi Bruno Latour kehottaa tutkimaan teknologiaa ja yhteiskuntaa integroituna kokonaisuutena eikä erillisinä osina (Latour 1991, 111). Tietoturvallisuudesta, kuten muistakin teknologioista on siis tullut sosiaalista todellisuutta, joka tekee siitä myös sosiologisesti kiinnostavaa. Tarkoitukseni on tuoda tietoturvallisuuskeskusteluun uusi laajempi näkökulma. Monimutkaistuva ilmiö vaatii yhteiskuntatieteellistä tutkimista, jotta siitä saataisiin kattava kokonaiskuva. Tarkastelen tietoturvallisuutta juuri kokonaisuutena, jotta näkisin, onko tietoturvallisuuden sisäisessä kulttuurissa esteitä sille, että asiantuntija ja maallikko ymmärtäisivät toisiaan.

Käytän aineistona Turvallisuus-lehden tietoturvallisuutta koskevia artikkeleita. Lehti on suunnattu turvallisuusalan ammattilaisille. Koen tämän aineiston relevantiksi, koska tietoturvallisuuskeskustelu on hyvin asiantuntijavaltaista. Toisin sanoen Turvallisuus-lehti reflektoi asiantuntijoiden näkemyksiä, jotka taas luovat pohjan yleiselle tietoturvallisuuskeskustelulle mediassa.

Aloitan työni teoriataustan esittelyllä, jossa luon kevyen katsauksen teknologian tutkimukseen, tuon esiin tietoturvallisuuden määritelmän ja hahmotan riskiyhteiskunnan käsitettä sekä pohdin asiantuntijuutta. Nämä luovat viitekehyksen, jonka puitteissa työni etenee koko matkan. Seuraavaksi käsittelen metodia, joka on semioottinen aktanttimalli. Analyysini rakentuu tämän mallin varaan, ja sen avulla pystyn hahmottamaan toimijat aineistosta. Tämän jälkeen kuvailen analyysini vaiheet, minkä jälkeen on luontevaa esitellä analyysin tuloksia. Esittelen viisi kertomusta, jotka kuvaavat tietoturvallisuuden sisäisiä maailmoja ja niiden toimijoita. Syvennän vielä toimijoiden tutkimista tarkastelemalla niiden välisiä suhteita sekä toimimista osana riskiyhteiskuntaa. Lopuksi pohdin esiinnousseita havaintoja ja kysymyksiä.

1.1 Teknologian tutkimus

Teknologia kiinnostaa tutkimuskohteena eri alojen tieteentekijöitä. Miksi ei kiinnostaisi, onhan teknologialla esimerkiksi teknisesti, taloudellisesti, sosiaalisesti ja poliittisesti relevantteja ulottuvuuksia. Yhteiskuntatieteissäkin teknologiaa on tutkittu, esimerkiksi teknologiahyödykkeiden muotoutumista kuluttamisen näkökulmasta (Pantzar 1996). Koska tietoturvallisuus on yhteiskuntatieteissä tutkimatonta maaperää, näin mahdollisuuden tarkastella teknologiaa tietoturvallisuuden kautta. Teknologian tutkimusta syytetään usein liiallisesta determinismistä, myös yhteiskuntatieteellisissä tutkimuksissa on syyllistytty tähän. Itse pyrin välttämään tätä omassa työssäni, ja koetan tarkastella tietoturvallisuuden ja yhteiskunnan suhdetta kaksisuuntaisena ilmiönä.

1.1.1 Teknologinen determinismi

Toisinaan teknologian ja yhteiskunnan vuorovaikutus nähdään yksisuuntaisena, jolloin tekniikan kehitystä ei voida hallita. Tällöin puhutaan *teknologisesta determinismistä*. Sen mukaan teknologian kehitystä suuntaa sen sisäinen logiikka, johon ihminen ei pysty vaikuttamaan. Jos tekniikka aiheuttaa ongelmia, niitä voidaan hallita vain uusien teknisten ratkaisujen kautta. Tekniikka on siis itseään täydentävä järjestelmä, joka kulkee omaa tietään. (Niiniluoto 2000, 29.) Tietoturvallisuus rakentuu pitkälle tekniikan varaan, sillä virukset, madot ja muut haittaohjelmat ovat uhkia, joita vastaan taistellaan palomuurien ja muiden hyötyohjelmien avulla. Tekniseen ongelmaan siis vastataan teknisellä ratkaisulla.

Radikaaleimman näkemyksen mukaan kehitystä ohjaa *teknologinen imperatiivi*, jonka mukaan kaikki tekniset mahdollisuudet toteutetaan, vaikka ne aiheuttaisivat vain tuhoa. Toinen vähemmän pessimistinen näkökulma puolustaa tekniikan valtaa. Tämä *teknokraattinen* näkemys korostaa tekniikan alan asiantuntijoiden kykyä tunnistaa tekniikan suunta. Siten he voivat opastaa muita tekniikan kehittymisen vastaanottamiseen. Tämänkään näkemyksen mukaan ihmiset eivät voi vaikuttaa tekniikkaan, mutta voivat sopeutua siihen asiantuntijoiden avulla. *Vapaan markkinatalouden* ideaa ei varsinaisesti voi pitää teknologisena determinisminä, mutta käytännössä se muistuttaa sitä. Kysyntä ja tarjonta ohjaavat teknologian muotoutumista, ja muut yritykset suunnata teknologiaa vain haittaavat sitä. Tämän näkemyksen sisällä

on eroavaisuuksia. Osa näkee kuluttajat täysin mainosten johdateltaviksi, jolloin teknologian kehitys perustuu täysin liiketaloudelliselle menestykselle. Optimistisempi näkemys esittää, että valistuneimmat kuluttajat pystyvät valinnoillaan vaikuttamaan teknologian kehittymiseen. (Niiniluoto 2000, 29-30.)

Vaihtoehtona teknologiselle determinismille on esitetty *indeterminismi*, jonka mukaan teknologian kehittyminen on kontekstisidonnaista. Ajatuksen takana on niin sanottu sosiaalinen konstruktivismi, jonka mukaan sosioteknologia verkottaa saumattomasti yhteiskunnan ja teknologian. Tekniset ratkaisut eivät siten kehity ennalta määrättyyn suuntaan, vaan useimmiten yllättävästi ja arvaamattomasti. (Niiniluoto 2000, 30.)

Sekä determinismi että indeterminismi kertovat jotain tekniikan luonteesta, mutta vain osan siitä. *Teknologiseksi voluntarismiksi* kutsutaan näkökulmaa, jonka mukaan ihmisen tahto vaikuttaa ainakin osittain tekniikan muovautumiseen. Tässä muistutetaan, että tekniikka on ihmisten sosiaalisesti aikaansaamaa, joten siihen voidaan myös vaikuttaa yhteistoiminnalla. Ehtona on, että tiedämme mitä haluamme ja tunnemme tarpeeksi hyvin teknologisten järjestelmien toimintalogiikan. Tekniikan hallinta vaatii siis ymmärrystä tekniikasta sekä kriittistä ajattelua, jonka avulla voi huomata teknologisten imperatiivien taakse kätketyt arvo-oletukset. Voimavarana ovat inhimilliset arvot, joilla pyritään vaikuttamaan teknisten tuotteiden koko elinkaaren ajan. (Niiniluoto 2000, 30-31.) Tämä olisi ideaalitilanne myös tietoturvallisuudessa. Käyttäjät ja teknologian kehittäjät voisivat avoimessa vuorovaikutuksessa luoda sellaista teknologiaa, joka palvelisi kaikkien intressejä. Esteenä on kuitenkin muun muassa teknologian nopea muuttuminen, sillä harvalla on mahdollisuus omaksua vaadittua teknistä ymmärrystä. Tämä ei ole ainoa este teknologisen voluntarismin esiinmarssille tietoturvallisuudessa, mutta käsittelen näitä ongelmia myöhemmin analyysissani.

1.1.2 Toimijaverkkoteoria

Teknologian tutkijat ovat huomanneet, että teknologia ei ole vain tekniikkaa, vaan siihen liittyy monenlaisia sosiaalisia, taloudellisia ja poliittisia ulottuvuuksia. Varsinkin yhteiskuntatieteellisessä teknologian tutkimuksessa tulisi huomioida se, että teknologia on osa yhteiskuntaa. Bruno Latour onkin todennut, että yhteiskuntaa ja teknologiaa ei

saisi käsitellä toisistaan erillisinä, vaan monimuotoisena kokonaisuutena (Latour 1991, 129). Monet nykyiset ongelmat johtuvat juuri siitä, ettei teknologian moniulotteisuutta ymmärretä. Onneksi rajoja ylittävää yhteistyötä löytyy. Michel Callon, Bruno Latour ja John Law ovat luoneet *toimijaverkon* käsitteen ja *toimijaverkkoteorian* (actor-network theory, ANT), jota voi pitää tieteidenvälisenä tutkimussuuntauksena. (Leskinen 2000, 176.)

Toimijaverkko on heterogeeninen ja sen inhimillisille sekä ei-inhimillisille toimijoille kuuluu yhtäläinen merkitys tulkinnassa. (Miettinen 1998, 28-29.) Toimijaverkkoteoriassa painotetaan juuri sitä, että ihmiset ovat vuorovaikutuksessa myös materiaalisen maailman kanssa, ei vain toisten ihmisten (Leskinen 2000, 184). Latour käyttää greimasilaista aktantti-käsitettä kuvaamaan yllämainittuja toimijoita. Toimijaverkkoteoriassa kehotetaan tarkkailemaan toimijoita silloin, kun he pyrkivät muuttamaan yhteiskuntaa ja tuottamaan tieteellistä tietoa sekä teknologisia järjestelmiä. Tarkoitus on välttää ennakointia, ketkä tai mitkä ovat merkittäviä toimijoita sekä mikä on sosiaalista ja mikä teknistä. Toimijaverkkoteoriassa yksityiskohdat ovat tärkeitä verkon kuvauksessa eikä siinä anneta rajoitteita siitä, minkälaiselle verkon osallistujalle voi antaa aktantin roolin. (Miettinen 1998, 28-30.)

Toimijamaailma on yksinkertaistettu ja heterogeeninen joukko ainesosia (Leskinen 2000, 183). Välillä toimijaverkkojen väliset erot voivat olla hienoisia, mutta yksityiskohdissa erot tulevat viimeistään ilmi (Latour 1991, 130). Toimijaverkon avulla pyritään kuvaamaan jännitteistä tilannetta, jossa tietty toimijamaailma saa kestävän ja dynaamisen rakenteen toinen toisensa määrittelemällä. Ei ole vaikeaa käsittää, että toimijamaailmat ovat heterogeenisia, mutta näiden maailmojen muuttumisen logiikkaa on huomattavasti haastavampi ymmärtää. Toimijaverkoston käsitteen avulla pyritään vastaamaan tähän ongelmaan eli miten luonnehtia kompleksista rakennetta, joka muuttuu koko ajan. (Leskinen 2000, 181-182.) Sosiologisessa mielessä toimijaverkostoteoria on relationaalista ja prosessiorientoitunutta. Kyseessä on teoria toimijuudesta, tietoteoriaa ja teoriaa koneista. (Leskinen 2000, 183-184.)

Toimijaverkkoteoriassa yhdistyy kaksi tärkeää tavoitetta teknologian tutkimuksen kannalta. Objekti on nähtävä aktiivisena kokonaisuutena osana konstruktiota, ja esineiden merkitystä ihmisen toimintaan on oleellista tutkia. Teknologia vahvistaa

yhteiskuntaa ja se on tarpeellinen yhteiskunnan rakenteistumisen ymmärtämiseksi. (Miettinen 1998, 28-29.) Ei-inhimilliset toimijat pitävät omalta osaltaan yhteiskuntaa koossa (Latour 1991, 103), esimerkiksi sähköposti yhdistää ihmisiä tarjoamalla helpon yhteydenpitotavan. Toimiverkkoteoriassa tähdätään perinteisen dualismin ylittämiseen. Subjekti ja objekti, luonto ja yhteiskunta luodaan samassa tieteen ja teknologian tekemisen prosessissa. (Miettinen 1998, 28-29.) Ymmärrys teknologian ja yhteiskunnan vaikutuksista toisiinsa on oleellista myös tarkasteltaessa tietoturvallisuutta. Ihmiset ovat vuorovaikutuksessa erilaisten teknisten ratkaisujen kanssa, niin tietokoneohjelmien kuin järjestelmien kanssa. Koska tarkoitukseni on tarkastella tietoturvallisuutta kokonaisena ilmiönä, oleellista on huomioida kaikki toimijat, olipa ne sitten inhimillisiä tai ei-inhimillisiä.

Toimijaverkkoteorian rooli työssäni on toimia löyhänä viitekehyksenä. Tiedostan teorian puutteet tutkimukseen sovellettaessa varsinkin toimijoiden rajaamisen sekä toisiinsa kytkeytymisen suhteen. Tärkein ohjenuora teoriasta on ymmärrys siitä, että toimijat voivat olla sekä inhimillisiä että ei-inhimillisiä. Teknologia on oleellinen osa tietoturvallisuuden toimijaverkkoa, joten sitä ei voi sivuuttaa vain sen takia, että se ei ole inhimillinen toimija. Toiseksi toimijaverkkoteoria tukee A. J. Greimasin semioottista aktanttimallia, jota käytän työssäni.

1.2 Tietoturvallisuus

Käyn seuraavaksi läpi tietoturvallisuuden eri osa-alueita. Vaikka alla olevissa toimenpidealueissa tietoturvallisuus määritellään laajasti koskemaan erilaisia laitteita ja ympäristöjä, useimmiten julkisissa keskusteluissa tietoturvallisuus rajautuu lähinnä tietokoneisiin ja -järjestelmiin, kuten myös aineistossani. Tuon esiin tietoturvallisuuden määritelmän ja tavoitteet. Lisäksi esittelen erilaisia tulkintoja krakkereista eli yhdenlaisista tietoturvallisuuden vihollisista.

1.2.1 Tietoturvallisuuden sisältö

Tietoturvallisuuskäsitteelle löytyy varsin vähän määritelmiä. Valtiohallinnon tietoturvallisuuskäsitteistön mukaan tietoturvallisuus on:

> ”Tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille”
>
> (Valtionhallinto 2003, 51).

Vaikka tietoturvallisuudesta on puhuttu runsaasti viime vuosina, sen käsitettä ei juurikaan ole avattu. Käsitteen määrittely jää usein tekniselle tasolle ja hyvin pinnalliseksi. Ruohosen mukaan tietoturvan tavoitteena on varmistaa, että tietokoneet ja niiden ohjelmat tekevät vain sen, mitä niiden on tarkoitus tehdä. Toisin sanoen pyrkimyksenä on suojata tietojärjestelmät mahdollisimman monelta riskiltä sekä varmistaa, että tiedot ovat oikeutettujen käyttäjien käytettävissä aina tarvittaessa. (Ruohonen 2002, 2.) Tässä määrittelyssä näkyy tietoturvallisuuden tietokonekeskeisyys. Määritelmässä ei lainkaan huomioida tietoa, joka on tietojärjestelmien ulkopuolella, kuten ihmisten tietämystä tai paperilla olevaa tietoa.

Tietoturvallisuuden tavoitteet voi jakaa viiteen osaan, jotka ovat luottamuksellisuus, autenttisuus/oikeellisuus, kiistämättömyys, eheys ja käytettävyys. *Luottamuksellisuus* tarkoittaa, että tietoja voi käyttää vain siihen oikeutetut käyttäjät. Luottamuksellisuus pätee vain silloin, kun tietojen ja tietojenkäsittelyn oikeudet säästyvät loukkauksilta ja vaarantumiselta. *Autenttisuuden* tavoitteena on taata, että kaikki tietojärjestelmän osat, niin käyttäjät kuin tapahtumat, kyetään tunnistamaan luotettavasti. *Kiistämättömyys* tähtää siihen, että kaikki tietojärjestelmän tapahtumat voidaan myöhemmin todistaa luotettavasti. Esimerkiksi alkuperän kiistämättömyydellä voidaan osoittaa henkilö, joka on lähettänyt tietyn viestin, ja luovutuksen kiistämättömyydellä viestin vastaanottanut henkilö. *Eheydellä* tavoitellaan tietojärjestelmien tietojen muuttumattomuutta ellei oikeutettu käyttäjä pyri niitä muuttamaan. *Käytettävyys* pyrkii siihen, että tietojärjestelmän tiedot ovat aina käyttäjien käytettävissä haluttuna aikana ja vaaditulla tavalla. Käyttäjän näkökulmasta tämä on järjestelmän tärkein ominaisuus, mutta tietojärjestelmän ylläpitäjälle haasteellisin. (Ruohonen 2002, 2-3; Valtiohallinto 2003, 20,22, 25)

Tietoturvallisuus jaetaan kahdeksaan toimenpidealueeseen. *Hallinnollisen tietoturvallisuuden* tavoitteena on luoda tietoturvasuunnitelma ja varmistaa, että kaikki tietoturvan osa-alueet ovat riittävällä tasolla. Usein hallinnollisella tietoturvallisuudella viitataan tietojärjestelmien tietoturvan eri osa-alueiden johtamiseen, mutta se kattaa myös muun muassa organisaatiojärjestelyitä, tehtävien ja vastuiden määrittelyä sekä henkilöstön ohjeistusta, koulutusta ja valvontaa. (Ruohonen 2002, 4-5; Valtiohallinto 2003, 11.) *Henkilöstöturvallisuus* tarkoittaa henkilöstöön liittyvien tietoturvariskien hallintaa. Henkilöstön tahattomia ja tahallisia vahinkoja ei voida kokonaan poistaa, mutta niitä voidaan vähentää henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan hallinnalla. (Ruohonen 2002, 4-5; Valtiohallinto 2003, 13.) *Fyysisellä turvallisuudella* viitataan henkilöiden, laitteiden, postilähetysten ja toimitilojen suojaamiseen vahinkoja vastaan. Esimerkiksi laitteet on sijoitettava ulkopuolisten ulottumattomiin. (Ruohonen 2002, 4-5; Valtiohallinto 2003, 10.) *Tietoliikenneturvallisuus* kattaa tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen turvallisuuden. Keinoja tietoliikenneturvallisuuden saavuttamiseen ovat muun muassa laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen. (Ruohonen 2002, 4-5; Valtiohallinto 2003, 48.) *Laitteistoturvallisuudella* on päällekkäisyyttä fyysisen turvallisuuden kanssa, sillä tavoitteena on laitteiston sekä tilojen fyysinen turvallisuus muun muassa käytettävyyden, toimivuuden, pääsynvalvonnan ja tarvikkeiden saatavuuden osalta (Ruohonen 2002, 4-5; Valtiohallinto 2003, 23). *Ohjelmistoturvallisuuden* tavoitteena on käyttöjärjestelmien ja ohjelmistojen suojaaminen luvattomilta käyttäjiltä sekä ohjelmistojen ylläpitäminen ja päivittäminen (Ruohonen 2002, 4-5; Valtiohallinto 2003, 28). *Tietoaineistoturvallisuudella* tarkoitetaan, että erilaisten tietoaineistojen käytettävyyttä, eheyttä ja luotettavuutta voidaan parantaa muun muassa varmuuskopioinnilla, virustorjuntaohjelmilla ja tietoaineistoa luokittelemalla (Ruohonen 2002, 4-5; Valtiohallinto 2003, 1). *Käyttöturvallisuuden* tavoitteena on tietotekniikan turvallinen käyttäminen. Tämän saavuttamiseksi ylläpito-, kehittämis- ja huoltotoimintojen täytyy olla ajan tasalla. (Ruohonen 2002, 4-5; Valtiohallinto 2003, 22.)

Tietoturvallisuuden yhteydessä puhutaan usein *tietoturvasuunnitelmasta*, joka sisältää muun muassa tietoturvan tavoitteet ja halutun tason. Tietoturvasuunnitelmaa luodessa

tietojärjestelmästä tehdystä *riskianalyysistä* on apua. Tämä käsittää tietojärjestelmään kohdistuvat riskit ja niiden laajuudet. Riskianalyysissä huomioidaan sisäiset ja ulkoiset uhat, tahattomat vahingot ja ennalta arvaamattomat tilanteet. Sisäiset uhat tulevat yrityksen sisältä, esimerkiksi käyttäjä pääsee käsiksi tiedostoihin, joihin hänellä ei ole oikeutta. Krakkerit, virukset ynnä muut sellaiset muodostavat ulkoiset uhat. Tahattomilla vahingoilla tarkoitetaan esimerkiksi tilannetta, että käyttäjä poistaa vahingossa väärän tiedoston. Ennalta arvaamattomia tilanteita ovat muun muassa varkaudet, tulipalot ja luonnonmullistukset. (Ruohonen 2002, 6-7.)

Tietoturvallisuuskeskustelun yhtenä osana on hyvin usein peruskäyttäjille annetut muutamat ohjeet. Ensinnäkin tietokone pitää lukita aina, kun sen ääreltä poistuu. Toiseksi aina pitää käyttää salasanoja, joita ulkopuolinen ei pysty arvaamaan. Näitä salasanoja ei kannata kirjoittaa muistiin, ei ainakaan tietokoneen läheisyyteen. (Ruohonen 2002, 107, 151-153.) Käytännössä näihin ohjeisiin sisältyy ongelmia. Ensinnäkin tietokoneen lukitseminen joka kerta, kun pöydän äärestä nousee, on melko työlästä. Se on samalla melkoinen epäluottamuslause työtovereita kohtaan, varsinkin jos ulkopuoliset eivät pääse tiloihin. Toiseksi nykyisin on kymmeniä salasanoja eri järjestelmiin ja ohjelmiin, joita pitää muuttaa säännöllisin väliajoin. Niiden muistaminen ulkoa on lähes mahdotonta, joten ihmiset kirjoittavat ne muistiin johonkin loogiseen ja ulottuvilla olevaan paikkaan. Useimmiten se on hiirimaton alla.

1.2.2 Krakkerit

Kun julkiseen keskusteluun nousee joku tietoturvauhka, kenties virus tai tietomurto, syylliseksi mainitaan useimmiten *hakkeri*. Tästä käsitteestä on kaksi hyvin erilaista tulkintaa. Yleisemmän mukaan hakkeri on asiantuntija, joka käyttää osaamistaan haitalliseen ja laittomaan toimintaan, kuten tietomurtoihin. Alkuperäinen selitys on, että hakkeri on tietokoneen ja sen toiminnan asiantuntija eli niin sanottu nörtti. Sen sijaan taitojaan rikoksiin käyttävää asiantuntijaa kutsutaan *krakkeriksi*. Jotta nämä kaksi erilaista näkemystä ei menisi sekaisin, erotteluna käytetään myös termejä *valkohatut* ja *mustahatut*. Valkohatut käyttävät osaamistaan hyviin tarkoituksiin, he pyrkivät pysäyttämään haittaohjelmat ja auttavat yrityksiä testaamaan tietoturvaansa. Mustahatut ovat rikollisia ja he pyrkivät murtautumaan tietojärjestelmiin sekä levittämään

haittaohjelmia. Näistä rikollisista käytetään myös käsitettä krakkeri. (Ruohonen 2002, 320) Myös *harmaahatut* on mainittu, he tekevät tietomurtoja, mutta eivät käytä tai levitä löytämiään tietoja. Heille riittää murron onnistumisen tuoma maine. (Ruohonen 2002, 320.)

Krakkerit voidaan erotella myös taitojensa mukaan. Useimmat krakkereista on niin sanottuja *Script kiddieitä*, jonka voisi suomentaa aloittelevaksi murtautujaksi. Nämä käyttävät muiden tekemiä ohjelmia ja pyrkivät tunkeutumaan jo löytyneistä tietoturva-aukoista. Script kiddiet onnistuvat yleensä tunkeutumaan vain huonosti suojattuihin tietokoneisiin, sillä heidän asiantuntijuutensa on heikkoa. Krakkeri, joka on todellinen asiantuntija ja tietoturva-asiantuntijoita askeleen edellä, tunnetaan nimellä *Elite*. Tästä voidaan käyttää myös käsitettä *31337* tai *7A69*. (Ruohonen 2002, 320.)

Peruskäyttäjästä hakkereiden toiminta voi tuntua päättömältä. Silti hakkeroinnin motiivina voi olla monia eri syitä. *Uteliaisuus* tietokoneisiin ja niiden toimintaa kohtaan on usein esitetty syyksi. Murtautuminen erilaisiin tietojärjestelmiin voi tuntua kiehtovalta *haasteelta*. Usein tähän liittyy turhautuminen kouluun, työhön tai muuhun elämään, joten hakkerointi voi tuoda mielenkiintoa elämään. Kiinnijäämisen pelko tuo *jännitystä* toimintaan. Jotkut hakkerit pyrkivät aiheuttamaan tahallista tuhoa eli tekevät *ilkivaltaa*. Hakkerit onnistuvat välillä suututtamaan toisensa esimerkiksi murtautumalla väärää hakkeria vastaan, ja seurauksena on *kosto*. Välillä kostoista tulee kierre, jolloin puhutaan *hakkerisodasta*. Hakkeroinnin taustalla voi olla myös *taloudelliset syyt*. Valkohatut auttavat yrityksiä suojaamaan tietojärjestelmänsä hyökkäyksiltä ja säästymään ansion menetyksiltä sekä pyrkivät ansaitsemaan palkkansa. Mustahatut tunkeutuvat tietojärjestelmiin rikollisten palkkaamana tai hankkivat itselleen laittomasti tietoja. Kun hakkerit toimivat *valtiollisista syistä*, heitä voi kutsua *cybersotilaiksi*. Tällöin hakkerointi on yksi sodankäynnin väline; hakkeri pyrkii edistämään oman valtionsa menestystä sodassa. Informaatiosodankäynnissä valtioiden perinteisellä vallalla ei ole juurikaan merkitystä, sillä pienikin valtio saattaa aiheuttaa huomattavan uhan suurvaltiolle. Jos hakkerointia käytetään aktivismin keinona, voidaan puhua *haktivismista*. Toiminta voi muuttua terrorismiksi, sillä internetin kautta on mahdollista levittää pakokauhua, kunhan vain löytyy tarvittava tekninen osaaminen. Hakkerit eivät aina pidä omaa toimintaansa rikollisena. Joidenkin mukaan yleistä hyötyä tuottavan tiedon tulisi olla kaikkien saatavilla. Esimerkiksi lääketieteelliset saavutukset olisivat

tällöin julkista tietoa yksityiskohtiaan myöden. Näin ajattelevat hakkerit saavat toiminnalleen hyväksynnän omassa yhteisössään, joten toiminnalla nähdään olevan moraalinen oikeutus. (Ruohonen 2002, 321-323.)

Pekka Himanen on yhdessä Linus Torvaldsin ja Manuel Castellsin kanssa kirjoittanut teoksen hakkerietiikasta. Tässä yhteydessä he tarkoittavat hakkerilla henkilöä, joka on innoissaan ohjelmoinnista. Tietokonerikollisiin ja muihin tietokoneella vahinkoa aiheuttaviin henkilöihin taas viitataan termillä krakkeri. (Himanen 2001, 7-8.) Teoksessa verrataan hakkerietiikkaa Weberin protestanttiseen etiikkaan. Kirjoittajien mukaan yhä vallitseva protestanttinen työetiikka tulisi korvata hakkerien työetiikalla. Hakkereille ohjelmointi ei ole vain tapa tienata elanto, vaan se on innostavaa, jopa intohimo. Työtä ei tehdä velvollisuuden tunnosta vaan koska se oikeasti kiinnostaa. Hakkerietiikassa kunnioitetaan yksilön vapautta. (Himanen 2001, 19-47.)

Hakkerietiikassa kannatetaan myös avointa lähdekoodia, jolloin tehty koodi olisi kaikkien käytössä ja kehitettävissä. Avointa lähdekoodia verrataan tiedeyhteisössä kaikkien käytössä oleviin tutkimuksiin ja tutkijoiden yhteistyöhön. Kirjoittajat myös korostavat, että hakkerit ovat sosiaalisia, vastoin yleistä käsitystä. Sosiaalisuus voi olla perinteisestä vuorovaikutuksesta poikkeavaa, enimmäkseen verkossa tapahtuvaa. (Himanen 2001, 66-79.)

Hakkereiden keskuudessa on silti erimielisyyksiä kuinka paljon vapautta ja valvontaa Internetissä tulisi olla. Useimmat hakkerit kannattavat täyttä sananvapautta ja haluavat ylläpitää yksityisyydensuojan mahdollisimman kattavana. Jotkut hakkereista kieltäytyvät jopa käyttämästä pankkikorttia, koska eivät halua, että omia henkilökohtaisia tietoja jää mihinkään tietokantaan. (Himanen 2001, 83-98.)

Vaikka kirjoittajien näkemys Weberin protestanttisen etiikan ja hakkerietiikan yhtenevyyksistä herättää epäuskoa, löytyy siitä myös pohdittavaa. Himanen ja kumppanit haluavat selkeästi puhdistaa parjattujen hakkereiden maineen tekemällä heistä edelläkävijöitä työetiikassa. Ongelmana on vain rajanveto, jonka kirjoittajatkin tunnustavat rivien välissä. Vapaa lähdekoodi on suotavaa, mutta miten varmistaa ettei joku ahne ota kunniaa toisen tekemästä työstä? Sananvapaus ja yksityisyydensuoja kuuluvat demokraattiseen maailmaan, mutta jos kuka tahansa voi sanoa nimettömänä

mitä tahansa, kuka vastaa kunnialoukkauksista ja rikollisten verkottumisesta? Intohimoinen suhtautuminen työhön on kunnioitettavaa, mutta kun siitä tulee pakkomielle, murtautuminen tietokantoihin on vain haaste. Himasen pyrkimyksenä voi nähdä hakkereiden toiminnan ylevöittämisen. Kirjan tärkein anti on kuitenkin muistutus siitä, että useat hakkerit tekevät tärkeää työtä tavalla, josta muutkin voivat ottaa oppia.

1.3 Riskiyhteiskunta

Riskien lisääntyminen näkyy jokapäiväisessä elämässä ja vaikuttaa yhteiskunnan eri tasoilla. Puhe riskiyhteiskunnasta tuntuu tästä näkökulmasta varsin loogiselta. Tietoturvallisuuden voi nähdä osana riskiyhteiskuntaa, sillä kummatkin ovat riskien ja uhkien kyllästämiä sekä asiantuntijatiedon varassa. Tarkastelen tässä luvussa riskiyhteiskunnan määritelmää, pohdin asiantuntijuutta sekä riskien ja uhkien luonnetta.

1.3.1 Riskiyhteiskunnan määritelmä

Riskiyhteiskunnan käsite liitetään usein ympäristöuhkiin, sillä teollisen tuotannon laajenemisen koetaan rasittavan juuri ympäristöä. Myös Ulrich Beck puhuu riskiyhteiskunnasta ympäristöuhkien yhteydessä. Tämän käsitteen voi nykyään hyvin ulottaa koskemaan muitakin elämän alueita, sillä teknistyneen yhteiskunnan riskit ovat muuttuneet oleellisesti teollistumisen alkuajoista (Beck 1990, 17). Yhteiskuntamme ongelmana ei enää ole pula hyödykkeistä, vaan riskien tunkeutuminen yhteiskunnan rakenteisiin ja toimintaan. (Sulkunen 1999, 305-306.) Beckin mukaan riskiyhteiskunnassa jaetaan hyödykkeiden sijasta riskejä, joita hän kutsuu *haitakkeiksi*. Perinteinen jakokonflikti muuttuu jakovastuuta koskevaksi, missä ongelmana on se, miten etujen tuottamisesta aiheutuvat riskit jaetaan, ehkäistään ja oikeutetaan. (Beck, Giddens & Lash 1995, 18.) Myös tietoturvallisuudessa ongelmana on, miten uusia tietoturvariskejä voisi parhaiten ehkäistä ja kenen siihen pitäisi osallistua. Toiseksi ihmisiä uhkaavat vaarat eivät enää ole luontoperäisiä, vaan ihmisen oman toiminnan tuloksia. Beck viittaa tähän ilmiöön käsitteellä *riskiyhteiskunnan refleksiivisyys*. Kolmanneksi riskejä määriteltäessä huomio kohdistuu vain toiminnan seurauksiin, mutta ei sen moraaliseen arvoon. (Sulkunen 1999, 307-308.) Tietoturvallisuudessakin

teknologian mahdollistamat hyödyt että haitat ovat ihmisen käsialaa. Alan sisäiselle keskustelulle on tyypillistä keskittyä eri teknisten ratkaisujen toimintaan eikä tietoturvallisuutta pohdita monimuotoisena ilmiönä.

Riskiyhteiskunnan tyypillinen ominaisuus on *epävarmuus*. Nykyiset riskit eivät kohdistu ajallisesti, paikallisesti eikä sosiaalisesti, sillä riskit koskevat kaikkia sosiaaliluokkia ja valtioita yhtä lailla (Beck 1990, 17-18, 113, 125). Tietoturvallisuudessa tietokonevirukset pystyvät hyökkäämään yhtä nopeasti naapurihuoneeseen kuin toiselle puolelle maapalloa. Riskit ovat sosiaalisessa todellisuudessa laskettuja todennäköisyyksiä, ei itsenäisesti olemassa olevia faktoja. Nämä sosiaaliset rakennelmat hyödyntävät teknistä esitystapaa ja teknisiä normeja. Hyväksyttävää riskiä voi siis pitää hyväksyttynä riskinä. Siksi tänään sietämättömältä tuntuva asia voi huomenna olla arkipäivää. Toisaalta se, mikä vielä tänään tuntuu normaalilta, voi seuraavana päivänä tuntua ahdistavalta ja pelottavalta. (Beck 1990, 134.)

Myös syyllisten tunnistaminen ja vastuun jakaminen, perinteinen kausaalisuus lakkaavat toimimasta. Tekniikan avulla ei pystytä poistamaan vaaroja kokonaan, sillä voidaan ainoastaan vähentää todennäköisyyksiä. Se ei riitä, sillä jopa kaikkein epätodennäköisin voi toteutua. Mitä enemmän aikaa kuluu ja mitä suuremmat tekniset järjestelmät lisääntyvät, sitä todennäköisempää on tuon vaaran toteutuminen. (Beck 1990, 17-18, 113, 125.) Ongelmana riskeissä on se, että ne kertovat mitä ei saa tehdä, mutta eivät sitä, mitä pitäisi tehdä. Riskit siis vaativat päätöksiä, mutta samalla ne purkavat niitä. (Beck ym. 1995, 22.)

François Ewardin mukaan turvallisuuden tuottaminen on sosiologinen ilmiö, joka muodostuu teollisen yhteiskunnan tuottamista vaaroista ja niihin liittyvistä institutionaalisista toiminnoista. Riskien laskeminen ja vakuutuslaitokset ovat yhteiskunnallinen vastaus turvattomuudelle. (Beck 1990, 160-161.) Turvallisuus ei ole silti turvallisuutta, vaan normeista ja tulkinnoista johdettu määritelmä. Sitä voi ja pitääkin muuttaa, kun nykyinen turvallisuus tuottaa ja normalisoi turvattomuutta. Tekninen turvallisuusmonopoli on mahdollista kyseenalaistaa. Ensinnäkin teknisen rationaalisuuden epävarmuus on nähtävissä. Toiseksi turvallisuutta ei voida koskaan taata teknisesti. Tekninen turvallisuus ei voi eliminoida pahinta mahdollista tapahtumaa.

Tämä ei ole mahdollista, koska riskilaskelmat perustuvat todennäköisyyksiin. (Beck 1990, 244-245.) Tietoturvallisuutta on pitkään pidetty puhtaasti teknisenä ilmiönä. Järjestelmät ovat laajenneet ja ongelmat monimutkaistuneet, joten myöskään tietoturvallisuudessa ei voida pelkällä tekniikalla poistaa kaikkia riskejä. Koska tietoturvallisuuteen liittyy muutakin kuin tekniikkaa, kuten käyttäjät, ei sitä voida tarkastella pelkästään teknisen rationaalisuuden näkökulmasta.

Vaikka yksilöt ovat entistä tietoisempia omasta turvallisuudestaan, valtiovalta pyrkii altistamaan heidät tuntemattomille suurvaaroille. Päätösten myötä vaarat ovat tulleet yhteiskunnallisesti vastattaviksi ja sosiaalisesti räjähdysalttiiksi. Nämä vaarat koskevat kaikkia ja ovat siten ristiriidassa perinteisten valtiollisten hyvinvointi- ja turvallisuuslupausten kanssa. Tästä Beck käyttää käsitettä *organisoitu vastuuttomuus*. Onnettomuuksien ehkäisyn oikeusperustan muodostaa yksilökohtaisesti tulkittu aiheuttajaperiaate, mutta se myös suojaa sitä aiheuttajaa, joka sen pitäisi asettaa vastuuseen. (Beck 1990, 18-19.) Ulrich Beckin mukaan modernin yhteiskunnan kehitysvaihe, jossa sosiaaliset, poliittiset, taloudelliset ja yksilölliset riskit muuttuvat teollisen yhteiskunnan seuranta- ja turvainstituutioiden tavoittamattomiin, merkitsee riskiyhteiskuntaa. Itse asiassa teollisen yhteiskunnan instituutiot luovat ja legitimoivat itse uhkia, joita eivät kuitenkaan kykene hallitsemaan. Tällöin osasta teollisen yhteiskunnan ominaisuuksista muotoutuu ongelmallisia niin yhteiskunnallisesti kuin poliittisesti. (Beck ym. 1995, 16.) Julkinen keskustelu tietoturvallisuudesta heräsi, kun siitä tuli arkipäiväinen ongelma. Tietoturvayhtiöt eivät yksin pysty hallitsemaan tietoturvauhkia, joten vastuun kantoon vaaditaan niin yhteiskuntaa kuin tavallista käyttäjää.

Oleellista on muistaa, että riskiarviot ovat kulttuurisidonnaisia. Tietyn asian määritteleminen riskiksi perustuu asiantuntija-arvioihin. Myös ratkaisujen löytäminen riskien toteutumisen estämiseksi riippuu asiantuntijatiedosta. Riskien välttämisen tekee ongelmalliseksi se, ettei niitä pysty selkeästi havaitsemaan eivätkä ne kohdistu tiettyyn ihmisryhmään. (Sulkunen 1999, 306-307.) Ihmisiä ei voi pakottaa sietämään vaaroja teknisen minimoinnin ja vaarojen liioittelun avulla. Lisäksi asiantuntijat horjuttavat toistensa asemia ja syrjäyttävät toisiaan. Epävarmuudesta tulee arkipäivää, mutta kuka tätä kestää jatkuvasti, on elämäkerrallinen ja poliittinen kysymys. (Beck 1990, 133; Beck ym. 1995, 24-26.) Asiantuntijatiedoilla on myös taloudellinen puoli. (Sulkunen

1999, 307.) Kun tietoturvayhtiön edustaja kehottaa kaikkia tietokoneen käyttäjiä hankkimaan uusia tietoturvaohjelmia ja päivityksiä uuden viruksen uhatessa, kuinka paljon kehotukseen liittyy taloudellisen hyödyn tavoittelua? Riskikysymyksiin sisältyy aina kulttuurinen hyväksyntä, siksi kaikki ja ei kukaan täyttävät asiantuntijuuden vaatimukset (Beck ym. 1995, 21-22).

1.3.2 Asiantuntijuus

Riskit ilmentävät uhkien rationalisointia. Vaarojen ennakoimiseksi ja tuhojen välttämiseksi luodaan yhä järkiperäisempiä ratkaisuja. Tätä kautta sosiaalinen koheesio on lujittunut. Yhteiskunnalliselle riskidynamiikalle on tyypillistä, että uhkien hallintatavoilla luodaan täydellisen vaaranhallinnan ja hallitsemattomuuden väliin jääviä tilanteita. Nämä ovat jo jokapäiväisiä ilmiöitä, mutta tarvitsevat yhä enemmän asiantuntijamäärittelyä banaalin elämän yläpuolella. (Ahponen 1997, 31.) Riskiyhteiskunnassa turvallisuus/epävarmuus -syndrooma yleistyy koko ajan, ja asiantuntijuudelle sekä asiantuntijatiedolle tulee koko ajan enemmän tarvetta. Kun aiemmin arjesta on selvitty rutiinien varassa, nykyään asiantuntijuus näyttäytyy arjen toiminnoissa enenevässä määrin. (Ahponen 1997, 27-29.) Tietokoneen käyttäminen ei ole yhtä huoletonta kuin jokunen vuosi sitten. Käyttäjän on oltava ajan tasalla uusimpien virusten, matojen ja muiden tietoturvauhkien suhteen, ja parhaiten se onnistuu kuuntelemalla asiantuntijoiden varoituksia mediassa.

Riskiteknologiat eli *asiantuntijuusteknologiat* parantavat turvallisuutta, koska niiden avulla uhat voidaan rajata tietyn ajallisen ja sosiaalisen etäisyyden päähän itsestä. Tiede ja asiantuntijat ovat kyenneet hallitsemaan riskejä määrittelemällä, luokittelemalla, ennakoimalla ja ehkäisemällä niitä. (Peltomäki ym. 2002, 98.) Yhteiskunnallisten ongelmien kompleksisuus ja abstraktisuus luovat pohjan asiantuntijoiden tarpeelle, mutta asiantuntijuutta täytyy olla riittävästi, jotta riskien hallinnasta voi luotettavasti kommentoida. (Ahponen 1997, 27-29.) Monimutkaiset ongelmat pakottavat asiantuntijat neuvottelemaan niiden luonteesta ja mahdollisuuksista sekä tavoista käsitteellistää, ennakoida, hallita ja ratkaista niitä. (Peltomäki ym. 2002, 98.) Riskitietoisuuteen sisältyy ymmärrys siitä, miten epävarmat ongelmat siirretään

julkiseen käsittelyyn ja siten tuodaan yleisen mielipiteen ulottuville. (Ahponen 1997, 27-29.)

Asiantuntijatietoon kuuluu *poliittisuus*. Tämän poliittisuuden valta ei ole samanlaista kuin poliittisen auktoriteettivallan käyttö, vaan se on paljon välittyneempää. Tieteen tekijöillä ei ole käytössään vallan välineitä, mutta poliittinen valta kaipaa asiantuntijavallan verkostoa tueksi punnitessaan käytettävissä olevia toimintakeinoja. (Ahponen 1997, 27-29.) Asiantuntijoilla on suuri periaatteellinen vastuu tuloksistaan. Vaikka poliittiset elimet soveltavat asiantuntijoiden tietoa omien intressiensä mukaan, on asiantuntijoiden ymmärrettävä jakamansa tiedon seuraukset.

Kristeva on nostanut *abjektin* käsitteen riskin rinnalle. Abjekti on ongelma, joka on olemassa vain tilannekohtaisen neuvottelun ja määrittelyn kautta. Sitä ei siis voi tarkasti kohdentaa eikä sen sijaintia hahmottaa. Abjekti on jotain epämääräistä, joka uhkaa tuolla jossain. Siksi oleellista onkin pyrkiä ymmärtämään sitä toimijaa, joka sen määrittää. Abjekti saa asiantuntijat kohtaamaan tietämättömyyden ja se kyseenalaistaa järjestyksen sekä turvallisuuden. Abjektin esiin nostaminen asettaa asiantuntijat uuden haasteen eteen. Kun ennen asiantuntijat pystyivät tulkitsemaan kohdetta tietämyksen ja tieteen nimissä, nyt heidän on tunnustettava paikallisuuden ja vuorovaikutuksellisuuden merkitys. Ilmiöitä on tarkasteltava oikeassa kontekstissa ja siitä on neuvoteltava muiden toimijoiden ja määrittelijöiden kanssa. (Peltomäki ym. 2002, 99-100.)

Asiantuntijuus on kaventunut ja syventynyt erikoistumisen kautta. Tämä on aiheuttanut sen, että kommunikointi asiantuntijoiden välillä on vaikeutunut. Maallikot ovat alkaneet epäillä asiantuntijoiden toimia muutosten ja riskien keskellä. Epäilyttävää on sekä asiantuntijoiden taidot että tahto. Onhan asiantuntijoille sattunut erehdyksiä, ja intressejä on muitakin kuin maallikkojen turvallisuuden takaaminen. Myöhäismodernia kulttuuria leimaa muutokset ja riskit. Tiede ja teknologia luovat uusia hyödyllisiä mahdollisuuksia ihmisten käyttöön, mutta samalla muodostuu myös uusia riskejä ja vaaroja. (Jokinen ym. 2001, 146-147.)

Esa Konttinen on määritellyt asiantuntijuudelle eli *professionaaliselle työlle* erilaisia tunnusmerkkejä. Ensinnäkin työn kohteena on kompleksinen tilanne, jota leimaa ainutkertaiset ja monimutkaiset tekijät. Lisäksi työ vaatii laajaa itsenäisyyttä

suunnittelusta lähtien. Osaamista on ylläpidettävä jatkuvalla koulutuksella. Työ ja ammatti ovat usein ammatinharjoittajalle tärkeä samastumisen kohde ja niillä on vaikutus hänen habitukseensa. Professionaaliselle työlle on myös tyypillistä, että erikoistuminen syventyy ja kaventuu, minkä myötä ammattiin samastuminen vahvistuu. (Konttinen 1997, 50-51.)

Professionaaliseen työhön kuuluu, että asiantuntija saa valtuudet työhönsä. Saadut valtuudet eivät ole silti ikuinen itsestään selvyys, vaan niistä joutuu kamppailemaan useammalla yhteiskunnallisella tasolla. Kamppailua on käytävä niin välittömän työympäristön, yhteiskunnan päätöksentekojärjestelmien kuin näiden välitasoilla. (Konttinen 1997, 53-54.) Riskiyhteiskunnan ongelmien monimutkaistuessa asiantuntijoilta vaaditaan laajempaa ymmärrystä kapea-alaisen suuntautumisen sijaan. Uudet ongelmat vaativat kokonaisvaltaisempaa tarkastelua ja kattavampaa yhteistyötä erilaisten asiantuntijoiden välillä. Kun tietoisuus riskiyhteiskunnasta kasvaa, kasvaa myös vaatimus asiantuntijuuden uudenlaisesta politisoimisesta. Vaikka erityisalojen rajat alkavat sulaa, se ei tarkoita, ettei erityisosaamista enää tarvittaisi. Yhteistyöhön sisältyy eri alojen asiantuntijuutta, ja tarkoituksena on yhdistää erilaiset osaamiset. (Konttinen 1997, 56.)

Individualisaatiolla on vaikutuksensa professionaaliseen työhön. Ammattiryhmään liittyvät symbolit eivät enää merkitse niin paljon, vaan yksilölliset ominaisuudet nousevat huomion kohteeksi. Tutkintotodistus ei enää riitä takaamaan osaamista nopeasti muuttuvassa työelämässä, vaan pätevyys ja maine on osoitettava toistuvasti erilaisilla näytöillä. (Konttinen 1997, 58.)

2 Semioottinen sosiologia

Aineiston tutkiminen vaatii valintoja menetelmän suhteen. Koska itse haluan tarkastella ilmiötä nimeltä tietoturvallisuus sen toimijoiden kautta, semioottinen aktanttimalli sopii välineeksi. Aktanttimallin avulla voin nostaa esiin toimijoiden välisiä suhteita sekä toiminnan arvoja ja merkityksiä. Toiminnan kuvaukset eli narratiiviset rakenteet ovat

merkittäviä, sillä ihmiset hahmottavat asioita tarinoiden logiikan tapaan (Sulkunen 1997, 39).

Sosiaalista todellisuutta ei voi lähestyä objektiivisena totuutena, vaan se on aina jonkun määrittelemä. Tutkimuksessa käytettävä aineisto on yksi näkemys sosiaalisesta todellisuudesta ja tutkija tuo analyysissa siihen oman tulkintansa. *Semioottista sosiologiaa* ei voi pitää analyysimenetelmänä, sillä se on metateoria todellisuuden ymmärrettävyydestä ja sen tuottamisen sosiaalisuudesta. Semioottiseen sosiologiaan sisältyy ymmärrys siitä, että sen luoma käsitys maailmasta on yksi muiden joukossa. Itse asiassa muiden käsitteellistämistapojen itsestään selvyydet ovat hedelmällistä tutkimusmaastoa. (Sulkunen 1997, 17.)

Tutkimusotteeni on semioottinen ja konstruktivistinen. *Sosiaalisen konstruktivismin* mukaan sosiaalista todellisuutta tuotetaan puhetavoissa. Tämä tarkoittaa sitä, että ilmiöstä tulee sosiaalista todellisuutta vasta määrittelyn kautta. (Sulkunen 1999, 146.) Osa konstruktivisteista on sitä mieltä, että tutkimuksessa on silti huomioitava myös sosiaalisista määrittelyistä riippumattomat olosuhteet. Tämä on oleellista siksi, ettei kuva maailmasta muodostu pelkästään median luoman käsityksen mukaiseksi. Tiedotusvälineillä onkin merkittävä rooli sosiaalisten ongelmien määrittelijänä ja yhteiskuntapolitiikan vaikuttajana yhteiskunnassa. (Sulkunen 1999, 151.) Pyrin pitämään tämän näkemyksen mielessäni koko analyysin ajan, jotta näkisin myös aineiston luoman maailman taakse.

2.1 Semiotiikan lähtökohdat

Merkkien toimintaa kutsutaan *semiosikseksi*. Se on oikeastaan kaiken toiminnan perusta; merkkejä tulkitaan ja niiden perusteella tehdään johtopäätöksiä. Esimerkiksi luolamies hankki ravintona eläinten jälkiä seuraamalla, mutta nykyään ruokakaupan nimikyltistä voi päätellä ruuan sijainnin. Semiosis on jatkuva prosessi, ilman semiosista ei olisi tietoisuutta maailmasta. Koska tapa tulkita ympäröivää maailmaa on niin automatisoitunutta, emme tiedosta tämän merkkiluonnetta. Jos tapahtumien kulku poikkeaa normaalista, joudumme pohtimaan odotuksiamme, käsityksiämme ja

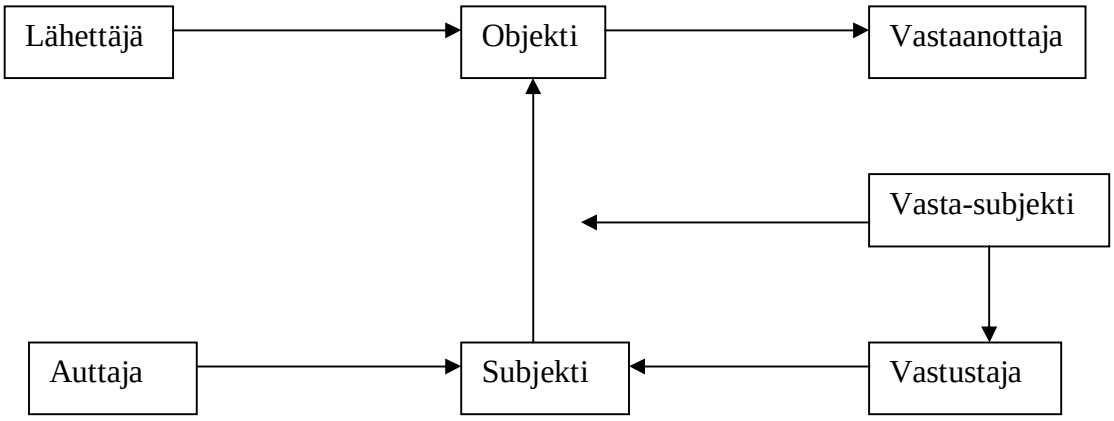
tulkintojamme. Semiosis kytkee aistihavainnot ja käsitteellisen ajattelun toisiinsa. Se yhdistää ruumiin, mielen ja kulttuurin. Semiosis muuttaa ihmisille yhteisen materiaalisen todellisuuden mentaaliseksi ja suhteelliseksi maailmaksi, joka on tietylle kulttuurille ominainen. Vaikka elämme kaikki samassa todellisuudessa, koemme sen silti hyvin eri tavalla. Semiosis on siis kaksisuuntainen prosessi, se välittää tietoa todellisuudesta, mutta samalla se muokkaa todellisuudesta käsityksiemme mukaisen maailman. Kuva havaitsijasta riippumattomasta todellisuudesta, minkä tiedot välittyvät aistihavaintojen kautta, ymmärretään opittujen ajatusmallien muovaamaksi konstruktioksi. (Veivo & Huttunen 1999, 14-16.)

Eero Tarastin mukaan semiotiikka on: ”merkkejä, merkkijärjestelmiä ja niiden tuottamista sekä käyttöä tarkasteleva tiede.” Tässä määritelmässä huomioidaan myös toiminta, niin vuorovaikutus merkkien kanssa kuin niiden välityksellä. Semiotiikka pyrkii määrittelemään tutkimuskohdettaan ulkopuolelta, mikä on hyvin vaikeaa. Semiotiikkakin on semiosista; tutkija tulkitsee merkkejä oman subjektiivisen näkemyksensä, itsereflektion kautta, sataprosenttisen objektiivisuuden saavuttaminen olisikin mahdotonta. (Veivo & Huttunen 1999, 18.)

2.2 Aktanttimalli

Semioottinen tekstuaalisia rakenteita käsittelevä teoria soveltuu mainiosti tekstien tulkintaan. A. J. Greimasin semiotiikan ideana on, että tekstin merkitystä ylläpitävät rakenteet voidaan jakaa osiin ja erilaisiin merkitysmekanismeihin. Tätä mallia voidaan soveltaa niin perinteisiin tarinoihin kuin uutisiin ja tieteellisiin teksteihinkin. Silti tavoitteena ei ole löytää yksiselitteistä tulkintaa, vaan havainnoida tarinassa ilmeneviä asemia ja toimijoiden välisiä suhteita (Veivo & Huttunen 1999, 74-75). Näitä kutsutaan *aktanttirooleiksi*, joiden avulla on mahdollista muodostaa vaihtoehtoisia tulkintamahdollisuuksia. Greimasin teoriaa kutsutaankin *aktanttimalliksi*. (Sulkunen 1999, 163-165.) Kyseessä on oikeastaan looginen tulkinnan apuväline (Sulkunen 1997, 35), jota on kutsuttu jopa ”narratiivisen kieliopin peruskaavaksi” (Korhonen & Oksanen 1997, 57).

Kuviossa 2.1 esitellään aktanttimallin idea. Sen ydin on subjektin ja objektin suhde, jonka varaan muut aktantit jäsentyvät. Jotta *subjekti* alkaisi tavoitella *objektia*, *lähettäjän* tehtävä on motivoida subjektia tuomalla esiin arvopäämäärän. *Vasta-subjekti* pyrkii estämään subjektia tavoitteen saavuttamisessa. Subjektin toimintaa edistää *auttaja*, kun taas vasta-subjektia avustaa *vastustaja*. *Vastaanottajan* rooli on arvioida toiminnan onnistumista sanktioiden avulla. (Korhonen & Oksanen 1997, 57) Lähettäjä ja vastaanottajan suhde nähdään kommunikaatioksi sanan väljässä merkityksessä. Lähettäjä saa toiminnan aikaan, vastaanottaja on taas se, jonka hyväksi toiminta koituu. (Veivo & Huttunen 1999, 74-75.) Greimas muistuttaa, että tarinan maailman arvojärjestelmää ei tarvitse tuntea läpikotaisin uskottavan kuvauksen aikaansaamiseksi (Greimas 1980, 211-212). Yksinkertaistettuna esimerkkinä lause ’Konsultti neuvoo Internetin käytössä’ kertoo, että konsultti auttaa eli kyseessä on auttaja-aktori.



Kuvio 2.1. Aktanttimalli (Korhonen & Oksanen 1997, 57)

Aktanttimalli pohjautuu aktanttien vastakkaisuudelle ja ristiriitaisille tavoitteille, jotka maustavat tarinan jännitteillä. Joskus nämä pyrkimykset ovat selviä tarinan alusta alkaen, mutta toisinaan ne selviävät vasta tarinan lopussa. *Aktantiaaliset asemat* eivät ole stabiileja, vaan ne muovautuvat tarinan haasteiden ja tapahtumien myötä. Toimijat myös siirtyvät usein aktantiaalisesta asemasta toiseen. (Korhonen & Oksanen 1997, 57-58.) Subjektin asemassa oleva toimija voi esimerkiksi näyttäytyä myös auttajan tai vastasubjektin roolissa. *Aktori* ja *aktantti* ovat siis eri asioita. Tekstin ilmaisun tasolla nähdään aktoreita eli tekstin kuvaamia konkreettisia toimijoita. Nämä taas edustavat aktantteja eli käsitteellisiä rooleja tekstin kuvaamassa kertomuksessa. Aktorien ja

aktanttien välillä ei välttämättä vallitse suoraa vastaavuussuhdetta. Samaa aktanttia voi edustaa sekä yksilöllinen että kollektiivinen aktori. Toimintaa muuttamalla siten, että päämäärä vaihtuu, muuttuu myös toimijan edustama aktantti. Aktantit voivat ilmetä tekstissä monella eri tavalla. Keskeistä on hahmottaa aktanttiroolit eli toiminnan käsitteellinen rakenne, johon tekstin aktoreiden keskinäiset suhteet perustuvat. (Veivo & Huttunen 1999, 74-75.)

Muutos on tarinan oleellinen ominaisuus. Aktantti aiheuttaa toiminnallaan muutoksia ympäristöönsä ja se vaikuttaa muihin aktantteihin. Koska jokaisella aktantilla on omat tavoitteensa, ne toteuttavat omaa *narratiivista ohjelmaansa*. Nämä voivat olla toisiaan täydentäviä tai täysin erillisiä toisistaan, yhdistyviä tai toisiaan vastaan suuntautuvia. Greimas kutsuu tarinan sisältämiä narratiivisten ohjelmien liittoumaa *narratiiviseksi kuluksi*. Vaikka jokaisella aktantilla on oma ohjelmansa, niillä on lisäksi rooli toisissa tarinan narratiivisissa ohjelmissa. Tämän takia toimijat näyttäytyvät useammassa eri asemassa narratiivisen kulun aikana. Tyypillisesti tapahtumat tarinoissa esitetään subjektin näkökulmasta, onhan kyseessä useimmiten päähenkilö. (Korhonen & Oksanen 1997, 57-59.) Jokainen tarina kuvaa siis omaa maailmaansa, sitä mikrouniversumia, jossa aktantit näyttäytyvät ja toimivat. Tällaisia mikrouniversumeja on huomattavasti helpompi tutkia kuin laajaa semanttista universumia kokonaisuutena. (Greimas 1980, 197-198).

Omassa analyysissani käytän neljää aktanttia, subjektia, objektia, auttajaa ja vasta-subjektia. Mielestäni lähettäjän ja vastaanottajan tarkastelu ei ole välttämätöntä aineistoni ja tutkimusongelmani yhteydessä. Ensinnäkin keskityn analyysissani toiminnan tavoitteisiin ja sen edistäjiin sekä estäjiin, joten tapahtumien käynnistäjän ja onnistumisen arvioijan tarkastelu ei tunnu relevantilta. Toiseksi lähettäjä ja vastaanottaja ovat siinäkin mielessä hedelmätön tutkimuskohde, että ne näyttäytyvät aineistossa tietoturvallisuusyhteisönä, sillä aineisto koostuu asiantuntijoiden puheenvuoroista asiantuntijoille. Vasta-subjektin auttajaa eli vastustajaa ei juurikaan aineistossa esiinny, joten sen käsittely ei mielestäni ole tärkeää.

Turvallisuus-lehden tietoturvallisuutta koskevia artikkeleita voi tarkastella aktanttimallin avulla, sillä se kertoo millaisen maailman ympäröimänä tietoturvallisuuden toimijat nähdään. Asiantuntijavaltaisella areenalla asiantuntijoiden

kannanotot otetaan helposti vastaan faktoina eikä ymmärretä huomioida kommentoijien omia intressejä. Aktanttimallin avulla voin hahmottaa myös toimijoiden välisiä suhteita ja pohtia niiden merkitystä. Vaikka artikkelit ovat vain poimintoja tietoturvallisuuskeskustelusta, ne kuvaavat silti tuon maailman arvoja ja oletuksia. Greimasin sanoin, asettamalla aktantti muiden joukkoon voidaan kollektiivinen arvojärjestelmä tuoda esiin käsitteellisenä (Greimas 1980, 196). Aktanttimalli antaa tutkijalle melko vapaat kädet analyysia tehdessä ja olenkin hyödyntänyt tätä vapautta. Soveltamani tavan avulla pystyn rakentamaan analyysista ymmärrettävän ja hallittavan kokonaisuuden, jonka sisälle lukijankin on helppo päästä.

2.3 Modaalisuus

Puhe ja teksti kuvaavat sosiaalista maailmaa erilaisista näkökulmista erilaisille yleisöille. Jos sosiologinen tulkinta pyrkii selvittämään keitä esittäjät ja yleisö ovat, millaisia heidän väliset suhteensa ovat ja minkälaisia ominaisuuksia heillä nähdään, voidaan puhua *enonsiaation ulottuvuudesta*. Jos tavoitteena on selvittää käsitys sosiaalisesta maailmasta, joka puheessa ja tekstissä kuvataan, kyseessä on *lausuman ulottuvuus*. (Sulkunen 1997, 43.) Erottelu on tarpeen siksi, että voidaan ymmärtää teksteissä tuotettuja arvoja (Sulkunen & Törrönen 1997a, 82). Toiseksi tekstiä voi tarkastella monipuolisemmin ulottuvuuksien erilaisten näkökulmien ansiosta (Sulkunen & Törrönen, 1997b, 100). Tässä työssä hyödynnän lausuman ulottuvuutta tutkiessani millaisena tietoturvallisuuden sisäinen maailma näyttäytyy ja enonsiaation ulottuvuutta tarkastellessani tietoturvallisuuden erityistä kulttuuria asiantuntijoilta asiantuntijoille.

Merkitysten dynaamista rakentumista voidaan analysoida *modaliteetin* käsitteen avulla. Modaliteettia pystyy lähestymään sekä enonsiaation että lausuman ulottuvuuden kautta. Enonsiaation näkökulmasta tarkasteltuna huomio kiinnittyy puhujan ja yleisön välisiin suhteisiin, ja lausuman ulottuvuus keskittyy siihen, millaisena maailma kuvataan. (Sulkunen & Törrönen 1997a, 81-82). Modaliteetti kuvaa aktantin suhtautumista toimintaan tai tilanteeseen sekä aktanttien välisten suhteiden motivoitumista. Modaliteetin teoriaa on pidetty tärkeänä, koska se luo mahdollisuuden analysoida tekstien arvomaailmaa ja tapaa, jolla aktantit siihen suhtautuvat. Modaliteettien avulla

voidaan myös analysoida aktanttien kehittymistä tarinan edetessä. Tällöin huomio kiinnittyy siihen, mitä modaalisia ominaisuuksia tarinan toimijoilla on ja miten ne kehittyvät toimijoiden välisessä vuorovaikutuksessa. (Veivo & Huttunen 1999, 74-75.)

Tarinat saavat tapahtumiinsa arvoja ja merkityksiä haluamisen, kykenemisen, osaamisen ja täytymisen sekä niiden johdannaisten kautta. Nämä ovat myös olennaisia tekstin tulkittavuuden kannalta. Nämä ovat *pragmaattisen modaalisuuden* lajeja ja niiden muovaamat kuvat todellisuudesta jättävät usein kertomatta kuka tuon arvioinnin takana on. (Sulkunen 1997, 41.) Subjektius luodaan pragmaattisten modaalisuuden lajien varaan tarinoissa. Nämä lajit aikaansaavat tarinan subjekteille ja objekteille ominaisuuksia ja valmiuksia toisiinsa sekä tarinan kuvaamaan maailmaan nähden. (Korhonen & Oksanen 1997, 63-64.) Esimerkiksi virke ”Yritykset haluavat turvata liikesalaisuutensa, joita vakoojat havittelevat” kertoo, että subjekti ”yritykset” tavoittelevat objektia eli ”turvata liikesalaisuutensa”, mutta ”vakoojat” vaikuttavat onnistumiseen. Joku arvioi, että yritykset haluavat pitää liikesalaisuutensa salassa. Arvioija jää huomaamattomaksi, koska virkkeessä on vain pragmaattisia modaalisuuden lajeja, kuten haluaminen. Pragmaattinen modaalisuus siis tuo esiin, miten arvot ja merkitykset linkittyvät toisiinsa. (Sulkunen 1997, 42.)

Subjekti motivoituu tehtäväänsä siten, että se kokee objektin arvokkaaksi, toisin sanoen objektiin kohdistuu *tahto* tai *halu*. Näin objektin tavoittelu tulee ymmärrettäväksi. Haluamisen ja tahdon erottaminen on oleellista. Jälkimmäinen kohdistuu itse toimintaan ja edellinen viittaa johonkin kohteeseen. Tahtominen on kyseessä silloin, kun pyritään muuttamaan asiantiloja, ja haluamisen kohdalla toiminta on arvo-objekti sinänsä. (Sulkunen & Törrönen 1997a, 90.) Haluaminen ja velvollisuus taas luokitellaan *virtuaalisiksi modaalisuuden* lajeiksi. Nämä ovat subjektin ja objektin olemista kuvaavia ominaisuuksia ja ne luovat merkityksen subjektin toiminnalle. *Aktuaalisiksi modaalisuuden* lajeiksi luetaan kykeneminen ja osaaminen. Nämä auttavat vastasubjektin toiminnan kautta ymmärtämään subjektin toimintaa. (Sulkunen & Törrönen 1997a, 83.)

Modaalisuutta voidaan jäsentää myös sen mukaan, mistä lähteestä toiminnan motivointi tapahtuu. Esimerkiksi voi pohtia, mikä taho velvoittaa subjektin toimimaan tietyllä tavalla eli mistä täytymisen motivaatio tulee ja miten se ilmenee tekstissä (Veivo &

Huttunen 1999, 74-75). *Endotaktinen modaalisuus* viittaa subjektiin itseensä, kun taas *eksotaktisen modaalisuuden* lähde on subjektin ulkopuolella. (Korhonen & Oksanen 1997, 65.) Kykeneminen ja velvoite lähtee useimmiten eksotaktisesta yllykkeestä eli motivaation lähde on subjektin ulkopuolisia ominaisuuksia. Sen sijaan osaaminen ja tahtominen ovat endotaktisen modaalisuuden tyyppejä eli subjektista itsestään lähtöisin. (Sulkunen & Törrönen 1997a, 83.) Näitä edellä mainittuja ominaisuuksia voi selventää vielä siten, että osaaminen on subjektin pysyvä ominaisuus, jota voi kutsua myös kompetenssiksi. Kykenemiseen vaikuttaa paremminkin ulkopuoliset tai sisäiset tilanteeseen liittyvät tekijät. (Sulkunen & Törrönen 1997a, 88-89.)

Pragmaattisen modaalisuuden lajien avulla voi osoittaa ne valmiudet, joita tarinan maailmassa tarvitaan. Lisäksi on mahdollista tuoda esiin, kuinka subjektit vaikeuksien ja haasteiden kautta tavoittavat päämääränsä. Pragmaattisen modaalisuuden lajit auttavat lukijaa näkemään tarinan yhteisön eri arvot, niin hyväksytyt kuin hylätytkin. (Korhonen & Oksanen 1997, 65.)

3 Tulkinta

Valitsin aineistokseni Turvallisuus-lehden tietoturvallisuutta käsittelevät artikkelit. Lehti ilmestyy kuusi kertaa vuodessa ja vuonna 2004 sen keskilevikki oli 5 444 kappaletta (Kotilainen 2005, 5). Lehtiartikkelit aineistona ovat mielekkäitä, koska niiden tutkimiseen löytyy soveltuvia välineitä. Turvallisuus-lehdessä käsitellään tietoturvallisuusasioita joka numerossa, joten se tarjoaa kattavan kuvan tietoturvallisuudesta sekä takaa riittävän laajan aineiston tutkimukseen.

Aluksi keräsin aineistoa vuosien 2000 – 2004 ilmestyneistä Turvallisuus-lehdistä. Valitsin vain ne artikkelit, jotka lehdessä on laitettu tietoturvallisuusotsikon alle. Lehdissä on muitakin tietoturvallisuuteen liittyviä artikkeleita, mutta haluan säilyttää aineistolle luontaisen määrittelyn tietoturvallisuuden sisällöstä. Aluksi kävin läpi artikkelit vanhimmasta tuoreimpaan luodakseni kokonaiskäsityksen siitä, mitä tietoturvallisuudesta on kirjoitettu kyseisten viiden vuoden aikana. Lukiessani

hämmästelin, kuinka rajusti tietoturvallisuus ja siitä käytävä keskustelu olikaan muuttunut noiden vuosien kuluessa. Jotta tämän pystyisi paremmin sisäistämään, haluan luoda nopean yleiskatsauksen aineistoon ja siinä esiin tuotuihin teemoihin. Lisäksi katsaus auttaa paremmin ymmärtämään, miksi alan ongelmien ratkaisu on niin haasteellista ja miksi ajan tasalla pysyminen tuntuu niin vaikealta.

Vuonna 2000 tietoturvallisuuskeskustelu on hyvin tekniikkapainotteista. Aiheena on muun muassa serverikaapit, erilaiset tietoliikenneverkot ja tehonsyöttölaitteet eli UPS:t. Myös laitteiden fyysinen turvallisuus tuodaan esiin, esimerkiksi miten tietokoneen varastamisen voi estää. Artikkeleissa kerrotaan myös miten virukset leviävät ja hakkereiden keinoista tunkeutua tietokoneisiin. Verkkopankkien turvallisuuden takaajiksi esitellään lähinnä tekniset ratkaisut, kuten oikeanlainen selain ja palomuuri. Tietoturvallisuuden suunnittelua käydään läpi hyvin yleisellä tasolla.

2001 tekniikka esiintyy edelleen monessa artikkelissa keskeisessä roolissa, mutta keskustelu on jo selkeästi monipuolistunut. Uutena asiana esiin nostetaan valtiovallan rooli. Tietoturvan uhkia pohditaan kansallisella tasolla, ja poliisin valmiuksia tietoturvallisuuden osalta herättää kysymyksiä. Erilaisia sääntöjä esitetään tietoturvallisuuden takaamiseksi, mutta nekin liittyvät lähinnä tekniikkaan ja järjestelmien käytön rajoituksiin. Myös tietoturvakoulutustarjontaa käsitellään, ja inhimilliset virheet mainitaan ohimennen.

Vuoden 2002 artikkelit ovat tekniikkakeskeisiä, sillä aiheena ovat muun muassa tunkeutumisen havainnointijärjestelmä, VPN-tekniikat ja langattomat videoyhteydet. Yhdessä artikkelissa, jossa käsitellään kertakirjautumista, korostetaan myös käytettävyyden merkitystä tietoturvallisuuden ylläpitämisessä. Aineistoa tarkastellessa tämä vuosi vaikuttaa jonkinlaiselta suvantovuodelta, sillä artikkeleita on vähiten ja ne eivät sisällä juuri mitään uutta edellisvuosiin verrattuna.

Vuodesta 2003 on sanottu, että se on ollut koko historian pahin tietokonevirusten määrän suhteen. Aineistossa se näkyy muun muassa siinä, että tietoturvallisuutta käsitteleviä artikkeleita on lähes tuplasti enemmän kuin aiemmin. Teemaa myös käsitellään paljon monipuolisemmin, eikä tekniikka ole enää ykkösaihe. Toki sitäkin käsitellään, esimerkiksi langattomia tietoverkkoja ja sähköpostin tietoturvaa lähestytään

lähinnä tekniikan näkökulmasta. Tekniikasta puhutaan kyllä useassa artikkelissa, mutta eri ratkaisujen esittelystä on siirrytty pohtimaan sitä, miksi palomuuria ja virustorjuntaohjelmia tarvitaan ja miten niitä käytetään sekä kerrotaan miten suojaamaton tietokone joutuu rikollisten armoille ja miten virukset leviävät. Tietoturva-alan eri tahojen välistä yhteistyötä myös kaivataan, jotta taistelua nettirikollisuutta vastaan ei hävittäisi. Esimerkiksi tietoturva- ja turvayritysten välinen yhteistyö nähdään tärkeänä, samoin operaattoreiden, ohjelmistovalmistajien ja valiovallan välinen yhteistyö. Jonkinlaisena merkkinä ongelmien laajenemisesta voi pitää sitä, että tämän vuoden artikkeleissa tietoturvallisuuskeskustelu ulotetaan koskemaan yhteiskuntaa. Yhdessä artikkelissa varoitellaan verkko- ja informaatiosodan uhkaavan valtioita ja yhteiskuntia, varsinkin jos hakkerit ryhtyvät palkkasotureiksi. Toisessa artikkelissa peräänkuulutetaan valtiovallan vastuuta ja yhteiskunnan roolia tietoturvallisuuden valistustyössä.

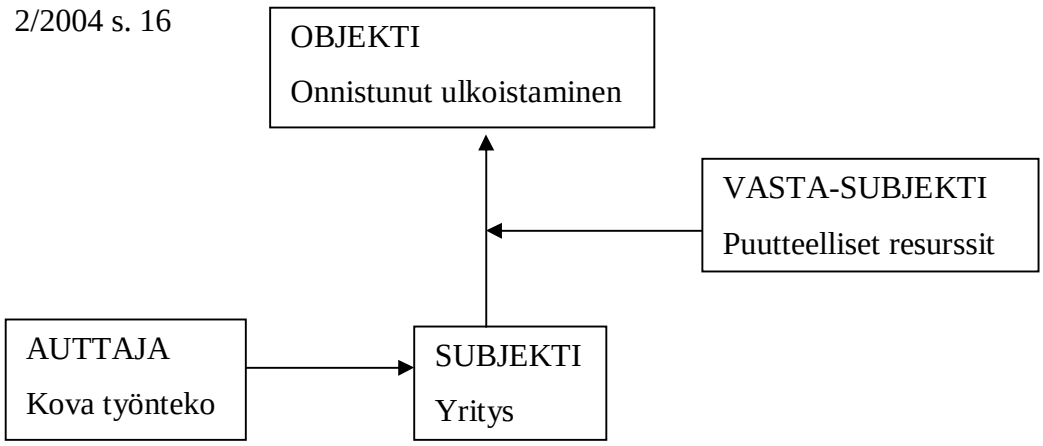
Vuoden 2004 artikkeleille tyypillistä on se, että tietoturvallisuutta tarkastellaan monipuolisesti eri näkökulmia käyttäen. Esimerkiksi tietoturvajohtamista käsittelevässä kirjoituksessa tuodaan esiin tietoriskianalyysin tekeminen, tekniikka sekä asiantuntijuuden hyödyntäminen, ja roskapostilta suojautumiseen ehdotetaan tueksi tekniikkaa, lainsäädäntöä ja käyttäjän tietotaitoa. Tietoturvastrategian ja –politiikan merkitystä yrityksen turvallisuudelle korostetaan, kuten myös riittävän ajan resurssointia tietoturvavastaavan avuksi. Tietoturvallisuuden kustannukset nousevat puheenaiheeksi pari kertaa ja ulkoistamista ehdotetaan yhdeksi vaihtoehdoksi kustannusten karsimiseksi. Erilaisia tietoturvauhkia tarkastellaan ja niille pohditaan suojautumiskeinoja, esimerkiksi yritysvakoilu, tietomurrot, phishing ja social engineering ovat haittaohjelmien ohella ongelmana. Uutena tietoturvallisuuden haasteena nähdään käyttäjä, jonka inhimillisyys nähdään lähinnä heikkoutena. Yrityksiä patistetaan kouluttamaan käyttäjiä ja käyttäjiä herätellään varovaisuuteen, koska käyttäjä on tietoturvallisuuden heikoin lenkki.

3.1 Analyysin vaiheet

Luettuani tietoturvallisuusaiheiset artikkelit läpi totesin, että lähempään tarkasteluun kannattaa ottaa vuosien 2003 – 2004 artikkelit. Näitä vuosia aikaisemmat tekstit

keskittyvät pelkästään teknisiin laitteisiin, joten en nähnyt niitä relevanteiksi tutkimukseni kannalta. Koska vuosien 2003 – 2004 artikkeleissa on selkeästi laajempi näkökulma, sillä muun muassa ihmiset ovat mukana, tuntui luontevalta valita analyysiini nuo kahden vuoden artikkelit. Lisäksi näiden kahden vuosikerran artikkeleista saa mielestäni jo kattavan käsityksen käydystä tietoturvallisuuskeskustelusta ja ne ovat riittäviä validin tutkimuksen toteuttamiseksi. Varsinaisessa analyysissa käytössäni oli siis 12 lehteä ja 29 artikkelia. Artikkelien tarkempi esittely löytyy liitteestä 1.

Aluksi tein jokaisesta artikkelista oman aktanttimallin paperille kuvion 3.1 mukaisesti. Poimin tekstistä ensin subjektin ja objektin, jonka jälkeen auttaja ja vasta-subjekti oli helpompi tunnistaa. Kaavion vasempaan yläkulmaan merkitsin, milloin ja millä sivulla artikkeli oli julkaistu. Aluksi pohdin myös vastaanottajia, lähettäjiä ja vastustajia, mutta mitä pidemmälle analyysissani pääsin, sitä epäolennaisemmiksi nämä muuttuivat. Ensinnäkin vastustaja esiintyi vain muutamassa artikkelissa ja silloinkaan sillä ei ollut vaikutusta toisiin toimijoihin. Toiseksi aineistoni koostuu asiantuntijoiden sisäisestä keskustelusta, jossa lähettäjä ja vastaanottaja ovat näiden asiantuntijoiden muodostama yhteisö tietoturvallisuuden näyttämöllä. Lähettäjän ja vastaanottajan lähempi tarkastelu olisi siten ollut melko hyödytöntä.



Kuvio 3.1.Esimerkki analyysin aktanttimallista

Seuraavaksi keräsin kaikki löytämäni subjektit erilliselle paperille ja jaottelin ne ryhmiin. Subjektien mukaan jaottelu tuntui luontevalta, koska onhan subjekti artikkeleiden ”päähenkilö” ja muut toimijat määrittyvät tämän mukaan. Annoin jokaiselle subjektikategorialle kuvaavan nimen ja kokosin oman taulukon jokaiselle subjektiryhmälle, mistä on esimerkki taulukossa 3.1. Taulukon otsikko on siis subjektiryhmän nimi. Jokainen artikkeli sai oman rivinsä, ja omiin sarakkeisiin tuli jokaisen artikkelin subjekti, objekti, auttaja ja vasta-subjekti. Tässä vaiheessa pyrin jo hieman tarkentamaan muitakin aktantteja, esimerkiksi ’kova työnteko’ konkretisoitui yritykseksi itseksi.

ORGANISAATIO

SUBJEKTI	OBJEKTI	AUTTAJA	VASTA-SUBJEKTI
Yritys 2/2004 s.16	Onnistunut ulkoistaminen	Kova työnteko (yritys itse)	Puutteelliset resurssit (yritys itse)
Yritys 5/2004 s.17	Tietomurron korjaaminen	Tietoturvapolitiikka (yritys itse)	Asenne (yritys itse)

Taulukko 3.1. Esimerkki subjektin mukaan tehdystä taulukosta

Seuraavaksi tein objekteista, auttajista ja vasta-subjekteista omia ryhmiään ja nimesin ryhmät sopivilla nimillä. Näin sain koottua löydökseni hallittavampaan muotoon. Pieneksi ongelmaksi muodostui se, miten aktantit kannattaisi kirjoittaa auki. Aloitin aktanttien esittelystä järjestyksessä, ensin subjektit, sitten objektit ja niin edelleen. Huomasin kuitenkin, että näin tekstistä tulee lähinnä pitkä sekä epäselvä tuoteluettelo, ja analyysin narratiivisuus kärsii kovasti. Kirjoitin silti kaikki aktantit auki tällä tavalla, koska sitä kautta pystyin hahmottamaan analyysini tulokset kokonaisuudessaan paremmin. Tarkasteltuani löytämiäni aktantteja aikani, oivalsin, että niistä löytyi yhdenmukaisuuksia. Useissa artikkeleissa, joissa aktorit edustivat samaa subjekti- ja objektiryhmää, myös auttaja ja vasta-subjekti olivat samasta kategoriasta. Näiden löydösten jälkeen tuntui luontevalta esitellä löytämäni aktantit juuri näissä jäljempänä esiteltävissä tarinoissa. Toisin sanoen kerron viisi kertomusta, joissa ilmenevät kaikki esiinnousseet aktantit niille tyypillisessä narratiivisessa kulussa.

Jotta analyysi ei jäisi irralliseksi kontekstistaan, tarkastelen kertomuksissa esiintyviä toimijoita vielä yhteiskunnan jäseninä. Kun ensin tarkastelin näitä toimijoita tietyssä asemassa osana kertomusta ja suhteessa objektiin, tämä toinen vaihe keskittyy itse toimijaan ja siihen, miten tämä nähdään osana yhteiskuntaa ja miten suhteet muihin toimijoihin esitetään. Koen tarpeelliseksi rajata yhteiskunnan käsitettä, joten käsittelen toimijoita tietoturvallisuuteen sopivasti riskiyhteiskunnan kautta.

4 Viisi kertomusta

Tässä luvussa esittelen aineistolleni viisi tyypillistä tarinaa. Yhteistä näille tarinoille on luonnollisesti tietoturvallisuus. Toisissa tarinoissa toimitaan tietoturvallisuuden puolesta, toisissa taas sitä vastaan. Huomasin kootessani yleisimpien subjekti-objekti – parien ympärille aineistossa esiintyviä vasta-subjekteja ja auttajia, että kaikista muodostamistani aktanttiryhmistä on aktori mukana jossain tarinassa. Tämä havainto lisäsi uskoa siihen, että nämä esimerkkitarinat tuovat kattavasti, mutta hallitusti esiin kaikki aineistosta analysoidut löydökset.

Greimas on luonut tarinoille ideaalimuodon, jota kutsutaan *narratiiviseksi kaavioksi*. Se koostuu kolmesta vaiheesta, joita hyödynnän seuraavaksi esiteltävissä viidessä kertomuksessa. *Kvalifioivassa eli valmistava tarinassa* subjekti saa velvoitteen, motivaation, kyvyn ja kompetenssin tavoitteen saavuttamiseksi. (Korhonen & Oksanen 1997, 59.) Tässä työssä valmistava tarina muodostuu subjektin esittelystä, jossa kerron miten subjekti nähdään, esimerkiksi mitkä ovat sen ominaisuudet ja konteksti aineistossa. Lisäksi tuon esiin subjektin päämäärän. Nämä kaksi, subjekti ja objekti, muodostavat parin, jonka ympärille muut aktantit rakentuvat. Tavoitteessa kiinnitän huomiota modaliteetteihin. Tarkastelun alla on, nähdäänkö toiminnan mahdollisuudet omasta itsestä vai ulkopuolisista seikoista riippuvaisiksi sekä miten olemista ja tekemistä kuvataan. *Päätarinassa* subjekti joutuu haasteiden eteen vasta-subjektin vastustaessa päämäärään pyrkimistä (Korhonen & Oksanen 1997, 59). Itse etenen päätarinaan auttajan kuvailulla. Auttaja edistää nimensä mukaisesti subjektia tavoitteen

saavuttamisessa. Tässäkin pohdin sitä, onko auttaja subjektille ulkoinen vai sen toiminnasta riippuvainen. Lisäksi tuon esiin vasta-subjektin, joka pyrkii estämään subjektia päämäärän tavoittelussa. Tälle on auttajan kanssa yhteistä se, että molemmat ovat sidoksissa subjektiin. Myös vasta-subjektin kohdalla tarkastelen, onko se subjektin ulkopuolinen vai siitä itsestään lähtöisin. *Sanktioivassa eli vahvistavassa tarinassa* evaluoidaan aktanttien toiminta (Korhonen & Oksanen 1997, 59). Sanktioiva tarina näyttäytyy kertomusten lopussa tarinan opetuksessa, kun tuon esiin arvioinnin aktanttien toiminnasta.

4.1 Organisaatio tavoittelee yhteistyötä

Aineistossa yleisin subjekti on organisaatio. Tässä yhteydessä organisaatiolla viitataan muutamaa poikkeusta lukuun ottamatta yritykseen. Yritys nähdään siis sosiaalisena kokonaisuutena ja toimijana.

> ”Jos yritys haluaa laajentaa lähiverkkoaan, se onnistuu liittämällä siihen muutamia langattomia tukiasemia.”
>
> Turvallisuus 4/03 s. 16

> ”Jos yritys tekee yhteistyötä Suomen puolustusvoimien kanssa, puolustusvoimat määrittelee turvallisuusluokan.”
>
> Turvallisuus 5/04 s. 14

Yrityksistä puhutaan niille luontaisessa asiayhteydessä eli suhteessa liiketoimintaan. Teksteissä puhutaan strategiasta, johtamisesta ja kustannustehokkuudesta, jotka liittyvät tarkemmin sanottuna yrityksen *johtamiseen*. Toisin sanoen painotetaan yritysjohdon toimintaa, jotta tietoturvallisuus saataisiin osaksi liiketoimintaprosesseja. Lisäksi yritykset nähdään jonkinlaisina edelläkävijöinä uuden tekniikan hyödyntämisessä, sillä yritysten tietoturvatarpeisiin esitetään paljon uutta tekniikkaa ja vastaavasti uutta tekniikkaa tuodaan esiin yritysten tarpeiden näkökulmasta.

> ”Jos bisneksen tietoriskejä ei hallita, hävitään palvelujen tarjonnassa, tuotekehityksessä ja tarjouskilpailussa.”
>
> Turvallisuus 6/04 s. 26

Kun tarkastelee sitä, miten yrityksen tekemistä kuvataan, voi huomata, että yritys tuodaan esiin elävänä, lähes inhimillisenä olentona. Aineistossa yritys asentaa, myy, sanoo, tietää, tarvitsee, pohtii ja toivoo. Myyminen viittaa tietoiseen toimintaan, samoin tietäminen. Puhuminen, sanominen liitetään vain ihmiseen eikä tässä yhteydessä ole todellakaan kyse papukaijan puheesta, matkimisesta. Tarvitseminen ja toivominen ovat myös inhimilliselle olennolle tyypillisiä ominaisuuksia, jotka vaativat ajattelua ja emotionaalisuutta.

> ”Jotkut yritykset ulkoistaminen saa hymyilemään. Toiset latelevat voima-sanoja, kun lähes kaikki on mennyt pieleen.”
>
> Turvallisuus 2/04 s. 16

4.1.1 Objekti: Yhteistyöllä parempi tietoturva

Organisaation tavoitteena on yhteistyön kautta parantaa omaa tietoturvallisuutta. Tälle yhteistyölle on ominaista se, että yrityksen ja tietoturvaorganisaation tai –ammattilaisen välillä on kumppanuussuhde, jossa osapuolet ovat tasa-arvoisia. Tämä yhteistyö on myös selkeästi liiketoimintaa; tavoitteena on taloudellinen hyöty, joko välillisesti tai välittömästi. Toisin sanoen yhteistyö on tahdon kohde, sillä tavoitteena on muuttaa asiantiloja eikä yhteistyö arvona sinänsä.

> ”Kun yritys pohtii ulkoistamista, tietoturvallisuuskustannusten toivotaan laskevan. Yritys toivoo myös saavansa tietoturvallisuuden hoitoon ammattimaista tietotaitoa. Samalla yritys toivoo, että omaan ydinliiketoimintaan voisi keskittyä tehokkaammin.”
>
> Turvallisuus 2/04 s. 16

Yrityksiä yhteistyöhön ajaa tietoturvallisuuden muuttuminen haasteellisemmaksi. Yhä suurempi osa yrityksen tiedoista ja liiketoiminnasta on verkossa sekä verkossa kiinni olevissa tietojärjestelmissä ja samalla tietoturvallisuuden uhat ovat laajentuneet. Muutosta ovat vauhdittaneet ulkoisina tekijöinä krakkerit ja muut nettirikolliset. Ulkopuolisia kannustimia tietoturvallisuuden ylläpitämiseen löytyy myös: lainsäädäntö, asiakkaat ja yhteistyökumppanit vaativat yrityksiltä tietoturvallista toimintaa.

> ”Turva-alan yritykset saavat asiakkailtaan yhä useammin vaatimuksia siitä, että järjestelmien tietoturvan pitää olla hoidettu. Niinpä nopeimmat yritykset ovat jo ehtineet solmia yhteistyösopimuksia tietoturva-alan yritysten kanssa.”
>
> Turvallisuus 2/03 s. 20

Yrityksen sisäiset kannustimet yhteistyölle ovat taloudellisia. Tietoturvallisuus muuttuu koko ajan ja yritysten on vaikea pysyä muutosten perässä. Kun ainakin osa IT-toiminnoista ulkoistetaan ulkopuoliselle asiantuntijalle, pystyy yritys itse panostamaan ydinosaamiseensa ja mahdollisesti säästämään kustannuksissa.

> ”Tietoturvan ulkoistaminen on erityisen houkutteleva vaihtoehto pienille ja keskisuurille yrityksille. Tietoturvan osaamiseen ja infrastruktuuriin ei silloin tarvitse kuluttaa yrityksen rajallisia resursseja.”
>
> Turvallisuus 2/04 s. 18

Ratkaisuksi kompleksoituneeseen tietoturvaongelmaan ehdotetaan siis yhteistyötä. Jotta yhteistyö tuottaisi halutun tuloksen, yrityksen on panostettava tähän kumppanuuteen. Ulkopuolisia ehtoja asettaa asiakas ja yhteistyökumppani oman liiketoimintansa puitteissa. Yrityksen oman toiminnan mahdollisuudet ovat tässä kova työnteko, tarvittava tietotaito ja riittävien resurssien varaaminen yhteistyöhön.

> ”Ulkoistamisessa voidaan kuitenkin onnistua. Se vaatii yrityksen johdolta vain maatiaisjärjen käyttöä ja työtä enemmän kuin äkkiseltään arvaisi.”
>
> Turvallisuus 2/04 s. 16

Kun tätä tarkastellaan pragmaattisen modaalisuuden kannalta, tarinan alussa yritystä motivoi eksotaktinen modaalisuus, sillä asiakkaat vaativat, että yrityksen *täytyy* huolehtia tietoturvallisuudestaan. Tarinan edetessä yritys ryhtyy yhteistyöhön toisen yrityksen kanssa, koska se *tahtoo* huolehtia omasta tietoturvallisuudestaan. Modaalisuus on siis muuttunut endotaktiseksi motivaation kummutessa yrityksestä itsestään. Myös onnistuminen riippuu yrityksestä itsestä: yhteistyö edellyttää kompetenssia, osaamista.

4.1.2 Auttaja ja vasta-subjekti: Organisaatio itse

Subjektin tavoitteen saavuttamista edistää auttaja. Auttaja on sidoksissa objektiin ja se voi tilanteen mukaan olla myös vasta-subjekti. Tässä tarinassa auttaja onkin subjekti itse eli yritys. Se, että yritys on itsensä auttaja, tarkoittaa luonnollisesti myös sitä, että auttaja on subjektin omasta toiminnasta riippuvainen. Yritys on itsensä auttaja silloin, kun se varaa tarpeeksi resursseja objektin eli yhteistyön onnistumiseksi. Kompetenssia

ja aikaa on oltava tarpeeksi, lisäksi suunnitteluun on panostettava ja viestinnän sekä koulutuksen on oltava riittävää. Yhteistyömalli on räätälöitävä yrityksen omien tarpeiden perusteella.

> ”Tietoturvallisuuden hyvä hallinta vaatii jatkuvaa seurantaa, pitkäjännitteistä suunnittelua, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Näiden päämäärien toteuttamiseksi on laadittu tietoturvaperiaatteet, joissa määritellään tietoturvallisuuden tavoitteet ja suuntaviivat tietoturvallisuustyölle. (…) Tietoturvallisuusperiaatteiden noudattamisesta solmitaan sopimukset myös yhtiömme tietoja käsittelevien, toisen yrityksen palveluksessa toimivien henkilöiden ja organisaatioiden sekä alihankkijoiden kanssa.”
>
> Turvallisuus 6/04 s. 24

Tässä tarinassa vasta-subjektikin on yritys itse. Vasta-subjekti pyrkii estämään subjektin tavoitteen saavuttamista joko tietoisesti tai tiedostamatta. Kuten auttajan kohdalla myös vasta-subjekti on luonnollisesti riippuvainen subjektin toiminnasta. Yritys on silloin itsensä vasta-subjekti, kun se toimii ajattelemattomasti ja suhtautuu yhteistyöhön ylimalkaisesti. Myös tietämättömyys ja puutteellinen viestintä hidastavat tavoitteeseen pääsemistä. Jos yritys jättää IT-toimintojen ulkoistamisessa kaiken vastuun ja valvonnan yhteistyökumppanille, tavoitteen saavuttaminen varmasti hidastuu. Ongelmia yhteistyöhön tulee myös siitä, että yhteistyössä ei ole huomioitu yritystä kokonaisuudessaan ja liiketoiminta on unohtunut taka-alalle.

> ”Jos suojausratkaisuista vastaavat asiantuntijat tekevät työnsä liiketoiminnasta irrallisena, heille jää epäselväksi, mitä liiketoiminnan tietoja itse asiassa käsitellään, ja kuinka luottamuksellisia ne ovat.”
>
> Turvallisuus 6/04 s. 26

4.1.3 Tarinan opetus

Käyn läpi vielä lyhyesti tarinan pääpiirteet, jotta juoni ei jäisi epäselväksi. Yritys siis tavoittelee yhteistyön kautta tietoturvallista yritysympäristöä, jotta liiketoiminta voisi jatkua ja kehittyä. Sysäys tähän yhteistyöhön tulee lähinnä ulkopuolelta, sillä asiakkaat ja yhteistyökumppanit haluavat asioida turvallisen yrityksen kanssa. Kun yhteistyöprosessi on käynnistynyt, yritys on oman onnensa nojassa. Jos yritys tekee onnistuneita valintoja ja päätöksiä, yhteistyö edistyy. Mutta jos yritys toimii liian vähäisen tietämyksen varassa ja ajattelemattomasti, se itse vaikeuttaa yhteistyötä.

Tässä tarinassa yritys nähdään hyvin vahvana ja itsenäisenä toimijana. Liike-elämässä tyypillisesti vaikuttavat tekijät kuten lainsäädäntö, asiakkaat, fyysinen ympäristö eivät juurikaan edistä tai estä yrityksen toimintaa. Oikeastaan koko yrityksen ulkopuolinen maailma osoittautuu vähäpätöiseksi, sillä yritys itse kuljettaa toiminnallaan tarinaa eteenpäin. Toisaalta myös yrityksen sisäinen kulttuuri on unohdettu; työntekijöistä ei juurikaan puhuta. Yritys on itsessään inhimillinen toimiva olento omassa bisnestietoisessa todellisuudessaan.

4.2 Hyötyohjelma torjuu hyökkäykset

Toisessa tarinassa päähenkilönä on hyötyohjelma. Aineistossa mainittuja hyötyohjelmia ovat virustorjuntaohjelma, palomuuri, roskapostisuodatin ja tyhjennysohjelma. Viimeiseksi mainitulla tarkoitetaan sellaista ohjelmaa, joka tyhjentää tietokoneen kiintolevyn ilman fyysistä tuhoamista. Hyötyohjelmat ovat siis tietokoneohjelmia, joiden avulla pyritään parantamaan tietoturvallisuutta. Kun hyötyohjelman mahdollisuuksista puhutaan, kohteena on lähinnä yksittäinen tietokone. Vaikka teksteissä mainitaan yritysten tietoturvaongelmia, enimmäkseen keskitytään yhden koneen turvaamiseen ja suojaamiseen.

> ”Kun yrityksen verkko on eristetty Internetistä palomuurilla, etätyöskentelijän täytyy pystyä osoittamaan palomuurille, että hänen pitää päästä käyttämään yrityksen verkkoa. Tätä varten on turvallisia VPN-ratkaisuja ja vastaavia tunnistusmenetelmiä.”
>
> Turvallisuus 1/03 s. 30

Tarinan hyötyohjelma on kehittyvä. Se kehittyy joko päivittämisen kautta tai se on älykäs ja oppimiskykyinen.

> ”Ehkä tärkein ominaisuus ja ero eri tuotteiden (virustorjuntaohjelmien KI) välillä on päivityksen tiheys. Ohjelma on päivitettävä ennen kuin se pystyy tunnistamaan joitakin tiettyjä viruksia.”
>
> Turvallisuus 1/03 s. 30

> ”Älykäs roskapostisuodin erottaa hyötyviestit vahingollisista. Se osaa pysäyttää jopa uuden, ennestään tunnistamattoman viruksen.”
>
> Turvallisuus 2/04 s. 22

Tarinan hyötyohjelma nähdään ihmistä älykkäämmäksi. Kun ihmisen omat tiedot ja taidot eivät enää riitä torjumaan tietoturvallisuuden uhkia, avuksi hälytetään hyötyohjelma. Ja ilmeisesti ihmisen kompetenssi ei nykyään riitä juuri lainkaan. Hyötyohjelma on kuin turvamies, joka on tehty ihmisen puolustajaksi. Se tunnistaa ja luokittelee tunkeilijoita sekä päättää kenet voi päästää sisälle ja kenet on pysäytettävä.

> ”Hyvä palomuuri ja sen apuna toimiva virustentorjuntaohjelma jatkuvasti päivitettyinä estävät yhdessä mahdollisimman suuren osan vihamielisistä hyökkäyksistä, mutta sallivat normaalin työskentelyn.”
>
> Turvallisuus 1/03 s. 30

Aineistossa esitellään erilaisia hyötyohjelmia ja niiden tarjoamia mahdollisuuksia. Esittelyistä puuttuu objektiivisuus, sillä jutut perustuvat enimmäkseen ohjelman valmistajan tai myyjän sanoihin. Mainitut ominaisuudet ovat pelkkää hyvää ja kaunista, huonot puolet ja puutteet unohdetaan tyystin. Tarina onkin enimmäkseen mainostamista.

> ”Sairaalan tietoturva oli pettänyt pahemman kerran. Arat potilastiedot menivät käytetyn PC:n mukana kierrätykseen. Ideasta kehitetty Blancco Data Cleaner on nyt maailman ainoa kiintolevyn tyhjennysohjelma, jolla on kansainvälinen Infosec-sertifikaatti.”
>
> Turvallisuus 3/03 s. 21

4.2.1 Objekti: Hyökkäysten torjuminen

Hyötyohjelman tavoitteena on ylläpitää tietoturvallisuutta. Kyse on passiivisesta tietoturvallisuudesta, sillä pyrkimyksenä on lähinnä torjua mahdolliset tunkeutumisyritykset ja välttyä roskapostilta. Voi siis sanoa, että hyötyohjelma on altavastaajana ja se pyrkii puolustamaan eikä niinkään aktiivisesti hyökkäämään. Hyötyohjelma on tehty estämään haittaohjelmien tunkeutuminen ja sitä se vain tekeekin. Sille ei loppujen lopuksi ole merkitystä tietoturvan taso kokonaisuutena. Kyseessä on siis haluamisesta, sillä hyötyohjelmalle virushyökkäysten torjuminen on arvo sinänsä eikä sillä pyritä muuttamaan asiatiloja.

> ”Virustorjuntaohjelman pitäisi tunnistaa kaikki tunnetut virukset. Piste. Siitä ei tingitä. Se tarkoittaa, että ohjelma tunnistaa hyvin monen tyyppisiä

> viruksia: sähköposti- ja verkkomatoja, makroviruksia sekä ihan perinteisiä tiedostoviruksia.”
>
> Turvallisuus 1/03 s. 30

Tietokonevirusten, matojen ja muiden haittaohjelmien määrän lisääntyessä ja monimutkaistuessa hyötyohjelmien on myös kehityttävä. Yksi tärkeimmistä asioista on hyötyohjelmien päivitys.

> ”Ehkä tärkein ominaisuus ja ero eri tuotteiden (virustorjuntaohjelmien KI) välillä on päivityksen tiheys. Ohjelma on päivitettävä ennen kuin se pystyy tunnistamaan joitakin tiettyjä viruksia.”
>
> Turvallisuus 1/03 s. 30

Virustorjuntaohjelmat ovat siis melko vahvasti ulkopuolisen toiminnan armoilla. Niiden olisi tunnistettava kaikki virukset, mihin taas vaikuttaa se, kuinka usein ohjelma päivitetään. Toisaalta tällaisia ohjelmia pidetään ensimmäisen polven ohjelmina, sillä toisen polven hyötyohjelmissa on tekoäly, jonka avulla ohjelma kykenee oppimaan.

> ”Nykyaikainen roskapostin torjunta pohjautuu pitkälle kehitettyyn tekoälyyn ja monivaiheiseen tunnusmerkkien tunnistamiseen ja arviointiin. Eri tunnusmerkeistä pystytään päättelemään, miten todennäköisesti kyseessä on roskaposti.
>
> Turvallisuus 2/04 s. 22

Nämä toisen polven hyötyohjelmat pystyvät siis vaikuttamaan omalla oppimiskyvyllään objektin saavuttamiseen. Toki näihinkin ohjelmiin vaikuttaa päivittäminen ja haittaohjelmat.

> ”WM Concept saastutti MS Word –ohjelman tekstikäsittelyn dokumenttitiedostoja. Silloin jouduttiin muuttamaan virustorjuntaohjelmistoja niin, että ne pystyivät käsittelemään myös Word-dokumentteja.”
>
> Turvallisuus 1/03 s. 30

Pragmaattisen modaalisuuden näkökulmasta ensimmäisen polven hyötyohjelmien *täytyy* tunnistaa kaikki virukset ja ne *kykenevät* tehokkaaseen toimintaan, jos niiden päivitys on ollut riittävää. Kun ensimmäisen polven hyötyohjelmilla esiintyy vain eksotaktisia modaalisuuden lajeja, toisen polven ohjelmilla ilmenee myös subjektiin itseensä viittaavaa modaalisuutta. Toisen polven hyötyohjelmat *osaavat* tunnistaa roskapostin eri tunnusmerkkien avulla.

4.2.2 Auttaja ja vasta-subjekti: Asiantuntija ja käyttäjä

Tässä tarinassa auttaja edustaa asiantuntijuutta, tarkemmin sanottuna se on hyötyohjelman kehittäjä. Hyötyohjelmien tekijät edistävät hyötyohjelman toimimista jo tekovaiheessa, sillä hyvin suunniteltu ja toteutettu ohjelma onnistuu haittaohjelmien torjunnassa mallikkaasti. Kun yritys ottaa käyttöön esimerkiksi palomuurin, sen toiminta on räätälöitävä yritykselle sopivaksi joko palveluntarjoajan, yrityksen tietoturva-asiantuntijan tai kolmannen asiantuntijatahon toimesta.

> ”Useimmiten tietosuoja pettää siksi, että palomuurin määrittely eli konfigurointi on huono.”
>
> Turvallisuus 1/03 s. 30

Jotta ohjelmia voisi päivittää, palveluntarjoajan täytyy tehdä jatkuvasti päivitettyjä versioita. Lisäksi päivityksen on oltava niin helppoa, että kaikki ohjelman käyttäjät osaavat sen tehdä. Paras ratkaisu on kuitenkin automaattinen päivitys. Auttaja on siis subjektin kannalta ulkopuolinen toimija eikä subjektin omasta toiminnasta riippuvainen.

Subjektin toimintaa vastustaa käyttäjä. Käyttäjältä puuttuu tarvittava tekninen osaaminen tietoturvallisuudesta, joten hän tyhmyyttään estää subjektia.

> ”Tietoturvallisuuden ehkä suurin ongelma on tänä päivänä, että käyttäjä on niin sanottu ei-tekninen henkilö. Hän ei osaa vastata esimerkiksi palomuurin kysymyksiin järkevästi. Palomuuri kysyy teknisillä termeillä, haluatko sallia vai estää jonkin tietyn pakettityypin, mutta käyttäjä ei ymmärrä, mitä se käytännössä tarkoittaa.”
>
> Turvallisuus 1/03 s. 30

Tietämyksen lisäksi käyttäjiltä puuttuu myös oikeanlainen ymmärrys. Käyttäjät eivät välttämättä käsitä minkä takia esimerkiksi yrityksellä on käytössään sähköpostin suodatin.

> ”Suodattaminen voidaan ymmärtää väärin, että joku ulkopuolinen henkilö lukee kaikki sähköpostit. Näinhän ei ole, vaan koko prosessista huolehtii tekoäly.”
>
> Turvallisuus 2/04 s. 22

Myös vasta-subjekti on subjektin ulkopuolisista tekijöistä riippuvainen. Hyötyohjelma ei pysty vaikuttamaan käyttäjään, se voi vain toivoa, että käyttäjä oppisi ymmärtämään ja tietämään enemmän tietoturvallisuudesta.

4.2.3 Tarinan opetus

Kertaan jälleen nopeasti tämän tarinan pääpiirteet ennen kuin siirryn seuraavaan. Hyötyohjelma pyrkii passiivisesti estämään virusten ja muiden haittaohjelmien pääsyn tietokoneeseen. Se torjuu erilaiset tunkeutumisyritykset, koska se on tehty sitä varten. Se onnistuu paremmin jos sen apuna on asiantuntijuutta. Esimerkiksi ohjelman kehittäjät ja palveluntarjoajat voivat kehittää hyötyohjelmaa toimimaan mahdollisimman hyvin. Hyötyohjelman tavoitteen saavuttamista vaikeuttaa käyttäjä eli ei-tekninen henkilö, joka on liian tietämätön tietoturvallisuusasioista.

Ensimmäisen polven hyötyohjelma on täysin riippuvainen ulkopuolisista toimijoista. Sillä ei ole omaa tahtoa ja auttaja on vaikutusmahdollisuuksiltaan paljon sitä voimakkaampi. Sen sijaan toisen polven hyötyohjelmilta löytyy jo osaamista. Nämä ohjelmat tuntuvat heräävän eloon, sillä riittää kun joku ne tekee, niin tekoälyn avulla ne kehittyvät ja viisastuvat hetki hetkeltä. Ihmisen heikkous korostuu vasta-subjektin kautta, sillä tämän tarinan ihminen ei ole paha rikollinen vaan tyhmä käyttäjä. Tarinan subjekti, hyötyohjelma onkin ihmistä paljon vahvempi ja merkittävämpi toimija tässä tarinassa. Toisaalta ihminen voi syyttää siitä itseään: luomalla oppivia ja tekoälyllä varustettuja hyötyohjelmia, hän heikentää omaa merkityksellistä asemaansa tarinan maailmassa.

4.3 Haittaohjelma leviää

Kolmannessa tarinassa pääosassa on haittaohjelma. Tällä tarkoitan viruksia, matoja ja muita sellaisia tietokoneohjelmia, jotka eivät kuulu tietojärjestelmään tai ovat tulleet siihen ylläpitäjän tietämättä. Melkein poikkeuksetta aineistossa haittaohjelma on virus. Virus nähdään vihollisena ja tuholaisena.

> ”Nopeasti pitää myös tietää viruksen vaarallisuusaste, eli millaista tuhoa virus voi saada aikaan. Tuhoaako se esimerkiksi koko kiintolevyn sisällön, käynnistääkö se joitakin prosesseja uudelleen, hidastaako se verkon toimintaa, varastaako se työasemilta luottamuksellisia tietoja, vai tekeekö vain jotakin pientä harmia.”
>
> Turvallisuus 4/03 s. 18

Kun puhutaan haittaohjelmasta, yleensä siihen liitetään jotain rikollista ja pahaa. Yllä olevassa aineistolainauksessa mainitaan vaarallisuus, tuho, varastaminen ja harmin aiheuttaminen. Aineistossa käytetään lisäksi muun muassa ilmauksia saastuttaa, iskee, vahingoittaa, lamaannuttaa, kaataa, huijaa, varastaa ja uhkaa, kun puhutaan haittaohjelmien toiminnasta. Haittaohjelman olemista pahuuden edustajana pidetään niin itsestään selvänä, että sen motiiveja ei nähdä tarpeelliseksi pohtia. Sehän haluaa vain aiheuttaa pahaa ja tuhoa.

> ”Internetistä löytyvän atomikellon avulla Sobif.F iskee 22.8.2003 Suomen aikaa kello 22.00 satoihin tuhansiin Internetin kautta toisiinsa synkronoituihin tietokoneisiin ja suorittaa tehtävän, jonka sisältöä ei tiedetä.”
>
> Turvallisuus 6/03 s. 12

Viruksen sanotaan olevan myös ärhäkkä, ovela ja häijympi kuin edeltäjänsä. Viruksia pidetään myös pirullisina, koska niiden koodi on niin monimutkaista ja kehittynyttä. Viruksilla kerrotaan olevan tuho-ominaisuuksia, jotka määrittävät sen tavan tehdä pahojaan. Jonkinlaisena pehmennyksenä kaiken tämän pahuuden keskellä voi pitää sitä, että aineistossa puhutaan myös virus*perheestä*.

> ”Ympäri maailmaa leviää tieto Sobig-virusperheen uusimmasta tulokkaasta, tietokonemato Sobig.F:stä.”
>
> Turvallisuus 6/03 s. 12

4.3.1 Objekti: Leviäminen

Haittaohjelman tavoitteena on levitä. Vaikka virukset ja madot toimivatkin monella eri tavalla, niiden perimmäinen tarkoitus on levitä mahdollisimman moneen tietokoneeseen, ainakin tässä tarinassa. Laajasta leviämisestä aiheutuu monenlaista haittaa eri puolille maailmaa, kun yksityisten ja julkisten organisaatioiden tietoverkot kaatuvat ja tietojärjestelmät menevät sekaisin. Haittaohjelmalle on loppujen lopuksi yhdentekevää, mitä sen toiminta aiheuttaa. Sen *haluaa* vain levitä. Haittaohjelmalle leviäminen on siis arvo itsessään, se ei tavoittele leviämisen avulla mitään.

> ”Mato oli levinnyt kannettavaan lentokentän loungesta tai hotellin verkosta. Tästä kannettavasta tietokoneesta Slammer levisi välittömästi it-operaattorin sisäverkkoon, jossa oli useita tietokoneita palomuurin sisällä ’turvassa’. It-operaattorin sisäverkossa Slammer toimi siten, että se levitti satunnaisiin paikkoihin datapaketteja. Osa näistä paketeista levisi vpn-tunnelin kautta ydinvoimalan sisäverkkoon ja aloitti leviämisensä kuin kulovalkea.”
>
> Turvallisuus 3/04 s. 12

Haittaohjelman toimintaan vaikuttavat tekijät ovat subjektin ulkopuolisia. Internetin ja sähköpostin käytön nopea yleistyminen on aiheuttanut haittaohjelmien lisääntymisen. Lisäksi tietoverkkojen ja –järjestelmien homogeenisyys helpottaa haittaohjelmien leviämistä.

> ”Tietoverkot firmojen sisällä ovat puhvelilaumoja. Ne ovat hyvin homogeenisia verkkoja. Joka työpöydällä on 32-bittinen Pentium-prosessori, joka ajaa Windowsin Wordia ja Exceliä, lukee sähköpostia Outlookilla Exchance-palvelimelta, ja surffaa Internet Explorerilla. Jos verkkomato saastuttaa yhden käyttäjän koneen, millään muullakaan koneella ei ole vastustuskykyä. Kaikki verkon koneet saastuvat.”
>
> Turvallisuus 3/04 s. 12

Eri ohjelmiin unohtuneet tietoturva-aukot luovat leviämistien haittaohjelmille. Nämä tietoturva-aukot korjataan mahdollisimman nopeasti, mutta joskus madot ja virukset ehtivät hyödyntää niitä ensin. Se, miten nopeasti tietoturva-asiantuntijat tunnistavat viruksen tai madon ja tiedottavat siitä julkisuuteen, vaikuttaa myös haittaohjelman leviämiseen.

> ”Hiljattain ohjelmista on löytynyt toinenkin aukko, jota virukset voivat hyödyntää. Netsky.V –virus käyttää xml-tekniikkaan liittyvää aukkoa, johon Microsoft on julkaissut korjauksen lokakuussa 2003.”
>
> Turvallisuus 3/04 s. 14

> ”Kun tietokoneviruksesta annetaan varoitus, tai pahojen virusten kohdalla hälytys, tietoturva-ammattilaisen kuten myös monen maallikon tehtävä on selvittää välittömästi viruksen luonne ja vaarallisuusaste.”
>
> Turvallisuus 4/03 s. 18

Haittaohjelma leviää, koska se *haluaa* levitä. Voi tuntua epäuskottavalta, että tietokoneohjelman toiminnan motivointi nousee siitä itsestä, mutta toisaalta ei mikään tai kukaan ulkopuolinenkaan pakota sitä toimimaan. Tietoturvallisuuden tasosta ja haittaohjelman tunnistamisesta riippuu *kykeneekö* haittaohjelma leviämään ja miten laajasti. Haittaohjelmalla on myös kompetenssia, sillä se *osaa* etsiä ja hyödyntää erilaisia tietoturva-aukkoja.

4.3.2 Auttaja ja vasta-subjekti: Käyttäjä ja tekniikka

Haittaohjelman tavoitteen saavuttamista edistää ihminen. Tämä viittaa sellaiseen tietokoneen käyttäjään, jonka tietämys tietoturva-asioista ei ole asiantuntijatasolla. Käyttäjä on silloin haittaohjelman auttaja, kun hän on varomaton ja huolimaton esimerkiksi sähköpostin liitetiedostojen kanssa.

> ”Kantona kaskessa ovat käyttäjät, joiden mielestä on hauska klikkailla kavereitten lähettämiä hupiohjelmia ja tiedostoliitteitä. (…) Kaverilta tulevaksi merkitty viesti saattaakin olla peräisin toiselta puolelta maailmaa ja sisältää ärhäkän viruksen.”
>
> Turvallisuus 5/03 s. 20

Erilaiset käyttäjät voivat tietämättään ja tahtomattaan toimia haittaohjelmien auttajina. Turhautunut teinipoika saattaa luoda viruksen tajuamatta mitä seurauksia se voi aiheuttaa. Mato pääsee suljettuun tietoverkkoon jos matoa kantava kone liitetään siihen esimerkiksi huoltotöiden takia. Haittaohjelmat käyttävät hyväkseen ihmisten tietämättömyyttä ja siten saavat nämä auttajikseen. Subjekti pystyy siis vaikuttamaan auttajaan huijaamalla, naamioitumalla ja tämän heikkouksia hyödyntämällä.

> ”Tekniset virussuojaukset alkavat olla varsin hyviä, mutta ihminen on ja pysyy tietoturvan heikkona lenkkinä. Siksi virusten kirjoittajat tulevat jatkossakin hyödyntämänä inhimillisiä heikkouksia.”
>
> Turvallisuus 3/04 s. 14

Haittaohjelman vasta-subjektina on tekniikka. Tässä tarinassa esiintyy lähinnä virustorjuntaohjelmat ja palomuuri estämässä subjektin toimintaa. Torjuntaohjelmat onnistuvat parhaiten, kun ne on päivitetty tarpeeksi usein ja niiden toimivuutta seurataan.

> ”Matoja vastaan suojaudutaan asentamalla palomuuri ja pitämällä huoli siitä, että koneessa on aina asennettuna uusimmat korjauspäivitykset.”
>
> Turvallisuus 3/04 s. 14

Vasta-subjekti on subjektin vaikutusmahdollisuuksien ulkopuolella. Haittaohjelma ei pysty vaikuttamaan tekniikan toimintaan, vaan tekniikka on riippuvainen ylläpidosta huolehtivista tahoista.

4.3.3 Tarinan opetus

Tässä kolmannessa tarinassa seurataan haittaohjelman toimintaa. Haittaohjelmat, jotka enimmäkseen ovat viruksia, pyrkivät leviämään mahdollisimman nopeasti ympäri maailmaa. Haittaohjelman leviämiseen ovat luoneet mahdollisuuden Internetin käytön yleistyminen ja tietoverkkojen homogeenisyys. Haittaohjelman objektiin pyrkimistä edistää tietämätön ja välinpitämätön ihminen, joka ei välttämättä itse tiedosta tätä rooliaan. Haittaohjelmia vastustaa tekniikka, mutta usein tuo edellä mainittu auttaja eli ihminen vaikeuttaa tekniikan toimivuutta.

Haittaohjelma on ovela olio ja ilmeisen elävä, pystyyhän se hyödyntämään inhimillisiä heikkouksia. Haittaohjelma tuntuu edustavan puhdasta pahuutta, sillä se leviämisellään tekee tuhoja ja aiheuttaa vahinkoa. Ihminen, tuo tietoturvan heikoin lenkki on avuton uhri haittaohjelman edessä. Tässä tarinassa haittaohjelmat tuntuvat olevan yhteiskunnan suurin vihollinen. Matkaamme kohti kauhuskenaariota, jota ei ole edes määritelty. Mutta mitä on tehtävissä, jos ihminen on kerran niin tyhmä eikä siitä muuksi muutu?

4.4 Hyvä ihminen kehittää tietoturvallisuuttaan

Neljännessä tarinassa subjektina on hyvä ihminen. Tästä toimijasta tekee hyvän se, että hän toimii tietoturvallisuuden puolesta. Tässä tarinassa hyvä ihminen on joko yrityksen työntekijä tai tietoturvavastaava. Kun subjekti on työntekijä, tarinassa on opettavainen ote. Aivan kuin subjektia pidettäisiin hieman yksinkertaisena, joka kaipaa ohjausta kädestä pitäen.

> ”Tottumuksesta käytämme arkista sähköpostia myös arkaluontoiseen viestintään. Kuvittelemme luottavaisin mielin, että sähköposti olisi yhtä turvallinen kuin vaikkapa kännykkäpuhelu tai tekstiviesti. Todellisuudessa sähköpostin tietoturva on erittäin huono. (…) Siksi arkaluontoiset viestit, kuten henkilökohtainen kirjeenvaihto tai esimerkiksi yrityksen taloustiedot, tulisi aina lähettää salattuna. Eihän kukaan lähettäisi vastaavia tietoja postikortille kirjoitettuna.”
>
> Turvallisuus 5/03 s. 18

Työntekijää valistetaan myös monella eri sääntö- ja ohjelistalla. Ohjeet koskevat muun muassa sähköpostiviestintää ja roskapostin hallintaa. Jotta jälkimmäiseen liittyvät ohjeet

menisivät varmasti perille, ensin listataan miten pitää toimia ja heti perään mitä ei pidä tehdä. Koko roskapostiongelman ytimenä nähdään subjektin kovapäisyys.

> ”Kokonaan roskaposti loppuu vasta sitten, kun kukaan ei enää tilaa mitään mainosten perusteella. Yksikään yritys ei halua käyttää markkinointia, joka ei toimi.”
>
> Turvallisuus 1/04 s. 16

Kun subjekti on yrityksen tietoturvavastaava, muuttuu kertomuksen sävy. Tietoturvavastaava nähdään sankarillisena johtajana, joka joutuu taistelemaan oikeuksistaan. Kun hän pystyy toteuttamaan tietoturvallisuuden laatujohtamisen kunnolla, yrityksen arvostus työntekijöiden ja asiakkaiden silmissä kohoaa pilviin. Tietoturvavastaavalla on sitkeyttä, luovuutta ja järkeä. Hän on keksijä, valmentaja, johtaja ja kulttuuritulkki. Suuri vääryys on se, että hän joutuu toimimaan ilman muodollista valtaa.

> ”Hänen on kuljettava työntekijöiden seassa. Keskusteltava heidän kanssaan. Kyseltävä heidän tietämystään, opastettava ja opetettava heitä – mieluiten heidän työpisteissään. Hänen on osattava puuttua asiantuntevasti käytännön epäkohtiin.”
>
> Turvallisuus 1/04 s. 12

4.4.1 Objekti: Tietoturvallisuuden kehittäminen

Tässä tarinassa tavoitteena on aktiivisesti parantaa tietoturvallisuutta. Tämä poikkeaa toisena esitetyn tarinan passiivisesta tietoturvallisuudesta siten, että tietoturvallisuutta kehitetään omin ehdoin ilman ulkopuolista pakotetta. Toisin sanoen ei odoteta virusten tai krakkereitten hyökkäystä, vaan pyritään kehittämään valmiiksi luotettava tietoturvallisuuskokonaisuus, jotta uhat eivät toteutuisi. Esimerkiksi sähköposti kannattaa tarvittaessa salata, jotta kukaan ulkopuolinen ei pääsisi sitä lukemaan.

> ”Hienojen tekniikoiden ja varmenteiden rinnalla on hyvä muistaa, että salauksen voi hoitaa yksinkertaisemminkin: kirjoitetaan viesti Word-dokumentiksi, joka tallennetaan riittävän pitkällä (…) salasanalla suojattuna. Sen jälkeen dokumentti välitetään tavalliseen tapaan sähköpostin tiedostoliitteenä.”
>
> Turvallisuus 5/03 s. 18

Lisäksi tietoturvallisuuden laatujohtaminen tuodaan esiin. Koko prosessi tilanteen kartoituksesta toteutukseen ja ylläpitoon täytyy olla kunnossa. Mainittu laatujohtaminen onnistuessaan nostetaan yhdeksi yrityksen menestystekijäksi.

> ”Tietoturvallisuuden laatujohtaminen on erittäin tärkeä menestystekijä. Jos yritys haluaa hyvää mainetta, tehokkuutta ja arvostusta, silloin tietoturvallisuutta pitää johtaa laadukkaasti.”
>
> Turvallisuus 1/04 s. 12

Tavoitteena on siis luoda yritykselle toimiva tietoturva, – tai ainakin imago sellaisesta - jotta asiakkaat ja työntekijät tuntevat olonsa turvalliseksi ja pysyisivät uskollisina yritykselle. Aktiivisella tietoturvallisuudella pyritään parantamaan ja suojelemaan liiketoimintaa eli kyseessä on tahto.

Aktiivisen tietoturvallisuuden tavoitteluun on monia syitä. Edellä jo mainittiin yksi oleellinen, yrityksen liiketoiminnan jatkuvuuden turvaaminen. Onnistuminen riippuu pitkälti resursseista.

> ”Hyväkin johtamisjärjestelmä epäonnistuu, jos toimintatapoja parantavat muutokset jäävät toteuttamatta. Siksi jokaisen tietoturvallisuuden laadusta vastaavan pitää itse keksiä, miten aikoo onnistua muutoksen läpiviemisessä. Antaako esimerkiksi ’terrierin’ nykiä niin kauan ylimmän johdon housunlahjetta, että hyväksyntä muutokseen lopulta saadaan. Vai kannattaako muutoksen toteuttaminen organisoida jollekin toiselle työryhmälle, ja toimia itse valmentajana. Vai kannattaako keksiä joku kolmas keino.”
>
> Turvallisuus 1/04 s. 12

Pitää myös ymmärtää, että kaikkia tietoturvariskejä ei voi eliminoida. Riskejä pystyy vähentämään, mutta ei täysin poistamaan. Siksi asiat pitää priorisoida.

> ”Siksi jokaisen yrityksen tulee laittaa arvonsa tärkeysjärjestykseen. Miten tärkeää yritykselle on esimerkiksi henkilöstön turvallisuus, laitteistojen fyysinen turvallisuus ja vaikkapa tietoaineistoturvallisuus? Kun tietoturvallisuuden laatujohtamisjärjestelmää rakennetaan, liikkeelle lähdetään aina arvojärjestyksestä.”
>
> Turvallisuus 1/04 s. 12

Esimerkiksi sähköpostit kannattaa salata, koska niiden salakuuntelu on melko helppoa. Salauksessa on omat ongelmansa, sillä lähettäjällä ja vastaanottajalla on oltava yhteinen salausavain tai salasana. Myös sisäänrakennettuja varmenteita on joissakin toimistojärjestelmissä, mutta niitä voi käyttää vain intranetissä. Myös politiikalla on oma kauha sopassa.

> ”Osittain hankaluus johtuu salaustekniikoiden luonteesta, mutta asialla on myös poliittinen ulottuvuus: aina kevääseen 2000 asti Yhdysvallat käytännössä esti tehokkaiden salausohjelmien maastaviennin. Näin haluttiin turvata maan oman sähköisen tiedustelun toimintamahdollisuudet.”
>
> Turvallisuus 5/03 s. 18

Tietoturvavastaavalta löytyy monipuolinen kompetenssi, jonka avulla hän pystyy luotsaamaan yrityksen tietoturvalliselle tielle. Toki yrityksen johdon myöntämillä resursseilla on oma vaikutuksensa, mutta tässä tarinassa ennen kaikkea tietoturvavastaavan sitkeys ja kekseliäisyys vaikuttavat siihen, kuinka paljon hänelle resursseja suodaan. Toisin sanoen tietoturvavastaava itsenäisesti vaikuttaa onnistumiseen oman *osaamisen* ja *tahtomisen* kautta. Työntekijän tietoturvallisuuden tasoon vaikuttaa se, miten hän *kykenee* käyttämään erilaisia salausmenetelmiä. Onko yrityksessä käytössä varmenteita tai muita salausmenetelmiä ja ovatko ne työntekijän ulottuvilla. Myös se, ymmärtääkö työntekijä lähetettävän viestin salaustarpeen, vaikuttaa asiaan.

4.4.2 Auttaja ja vasta-subjekti: Tekniikka ja asiantuntija

Auttajana tarinassa esiintyy tekniikka. Tekniikka koskee lähinnä sähköpostin suojaukseen ja roskapostin välttämiseen liittyviä ohjelmia ja salaustekniikoita.

> ”Jos postitulva alkaa viedä liikaa työaikaa, lataa netistä jokin roskapostin torjuntaohjelma tai päivitä sähköpostiohjelmasi sellaiseen, missä on sisäänrakennettu torjunta.”
>
> Turvallisuus 1/04 s. 16

Auttajan mahdollisuus edistää subjektia tavoitteeseen pääsemisessä riippuu subjektista ja sen kompetenssista. Esimerkiksi sähköpostin salaus vaatii teknistä ymmärrystä ja tietoutta, sillä kyseiset tekniikat ovat melko hankalia ja haasteellisia.

> ”Wordin sijaan voidaan käyttää monia Internetistä löytyviä salausohjelmia. Silloin on kuitenkin varmistettava, että vastaanottajalla on käytössään sama ohjelma. Erityisen turvallinen ohjelma on PGP eli Pretty Good Privacy, mutta sen käyttö ei sovellu aivan maallikolle.”
>
> Turvallisuus 5/03 s. 18

Tavoitteiden estäjänä toimii asiantuntija. Tässä tarinassa asiantuntija on krakkeri tai roskapostinlähettäjä. Jälkimmäisen asiantuntijuus perustuu siihen, että hän ymmärtää markkinoinnin logiikan, osaa kiertää lakia ja pystyy toimimaan jäämättä kiinni.

> ”Paha vain, että (roskapostin KI) lähettäjät ovat oppineet yhä ovelimmiksi ja keksivät yhä houkuttelevampia otsikoita saadakseen vastaanottajan avaamaan viestin.”
>
> Turvallisuus 1/04 s. 16

> ”Vuoden 2004 alussa Yhdysvalloissa astui vihdoin voimaan liittovaltion tasolla vaikuttava niin sanottu can spam –laki. Se ei estä roskapostia sinänsä, mutta kieltää lähettäjätietojen ja osoitteen väärentämisen sekä velvoittaa noudattamaan vastaanottajan pyyntöä päästä pois listalta (niin sanottu opt-out –periaate). (…) Alku ei ollut erityisen lupaava, sillä ainakin tammikuussa roskapostitus jatkui yhtä villinä kuin ennenkin. Lisäksi mainostajat voivat helposti siirtää lähetystoiminnan niihin lukuisiin maihin, joissa ei ole minkäänlaista lakia asiasta.”
>
> Turvallisuus 1/04 s. 16

Tarinan krakkeri pyrkii kyseenalaisin keinoin pääsemään käsiksi luottamukselliseen sähköpostiviestintään. Teon laittomuus voi olla krakkerin tiedossa, mutta ei aina. Krakkeri ei välttämättä ole tuntematon teini, joka sattumanvaraisesti pyrkii urkkimaan toisten sähköposteja verkon kautta. Kyseessä voi olla esimerkiksi utelias naapuri tai teollisuusvakooja. Sähköpostin tirkistely ei aina ole suunniteltua tiedon kaappaamista, vaan tilaisuus voi tehdä varkaan.

> ”Alaisella voi olla houkutus kurkistaa johtajan sähköpostiin – tai johtajalla alaisen, jos epäilee tämän suunnittelevan vaikkapa vaihtoa kilpailevaan firmaan. Ja varsinaiset rikollisethan eivät ole koskaan laeista piitanneetkaan.”
>
> Turvallisuus 5/03 s. 18

Subjekti pystyy vaikuttamaan vasta-subjektin toimintaan. Kun yrityksen työntekijä tai tietoturvavastaava käyttävät sähköpostia järkevästi ja vastuuntuntoisesti sekä tuhoavat arveluttavat viestit, roskapostinlähettäjien ja krakkereiden mahdollisuudet heikentää tietoturvallisuutta pienenevät.

4.4.3 Tarinan opetus

Tarinassa mainitaan kaksi erilaista pääosan esittäjää. Yrityksen työntekijä on kuin sinisilmäinen lapsi, joka kaipaa viisaampien johdatusta ja opastusta. Tietoturvavastaavalta löytyy kyllä tarvittava osaaminen, mutta yritysjohdolle tietoturvallisuuden tärkeys ei välttämättä aukea kovinkaan helposti. Kumpikin näistä

subjekteista pyrkii parantamaan tietoturvaa omalla tavallaan, jotta yritys menestyisi. Voidaan myös ajatella, että kummankin tavoitteena on turvata oma työpaikka. Aktiivisen tietoturvallisuuden tavoittelu liittyy siis täysin yritysturvallisuuteen, kotikoneita ei tässä yhteydessä juuri mainita. Tietoturvallisuuden parantamiseen vaikuttaa yrityksen myöntämät resurssit ja subjektin oma osaaminen. Auttajana tekniikka on tehokas ja muista toimijoista riippumaton väline suojaamaan sähköpostia. Asiantuntevat vasta-subjektit haluavat taloudellista tai informatiivista hyötyä, mutta heidän keinonsa ovat subjektin kannalta haitallisia.

Sähköpostin käyttäjä on turvassa, kun ei avaa epäilyttävää tai tuntemattomalta tulevaa sähköpostia eikä jätä konettaan hetkeksikään lukitsematta, kun poistuu sen luota. Epäilyttävän sähköpostin määritteleminen jääkin sitten käyttäjän vastuulle. Jos yrityksessä tuhotaan kaikki tuntemattomilta tulevat viestit, voi miettiä kuinka monta potentiaalista asiakasta, työntekijää ja yhteistyökumppania menetetään sekä paljonko tärkeää tietoa päätyy lukematta roskakoriin? Tarinan opetuksena kannattaa oikeastaan pitää peräänkuulutettua valppautta ja maalaisjärkeä, jota tietokoneen käyttäjiltä vaaditaan. Samalla on hyvä muistaa missä menee käytännön kannalta järkevyyden raja ja mistä alkaa hätävarjelun liioittelu.

4.5 Paha ihminen rikkoo lakia

Viidennessä tarinassa subjektina on paha ihminen. Tämä pahuus määrittyy saman logiikan mukaan kuin edellisen tarinan ihmisen hyvyys. Kun hyvä ihminen työskentelee tietoturvallisuuden puolesta, paha ihminen toimii sitä vastaan. Näitä pahoja ihmisiä mainitaan kahdenlaisia. Teinit ovat lähinnä kiusantekijöitä, jotka haluavat pitää hauskaa. Vakavamman uhan tietoturvallisuudelle aiheuttavat nettirikolliset, kuten vakoilijat, palkkasoturina toimivat krakkerit ja järjestäytyneet rikolliset. Teineistä puhutaan silloin, kun jonkun organisaation tietojärjestelmään on tunkeuduttu ja www-sivuille on jätetty esimerkiksi sinne kuulumattomia kuvia. Näitä teinejä kutsutaan myös script kiddieiksi, sillä he ovat amatöörejä, jotka käyttävät muiden tekemiä ohjelmia tietomurtoihin.

> ”He (teinit KI) jättävät esimerkiksi yrityksen www-sivuille musiikkiäänitteitä tai elokuvia edelleen levitettäviksi, tai siirtävät yritysten kotisivut syrjään ja laittavat omansa tilalle niin sanottuina nettigraffiteina. Joskus he tuhoavat

> yrityksen omia tiedostoja, jotta saavat riittävän määrän tyhjää levytilaa johonkin haluamaansa tarkoitukseen.”
>
> Turvallisuus 4/04 s. 15

Näiden teinien toimintaa ei pidetä kovinkaan vakavana rikollisuutena, vaan lähinnä haitallisena hauskanpitona ja kenties iästä johtuvana tietämättömyytenä.

Varsinaiset nettirikolliset aiheuttavat suurempaa haittaa. Nettirikollisista puhutaan alamaailman toimijoina eli heidän toimintansa nähdään täysin rikollisena. He eivät kaihda keinoja saavuttaakseen tavoitteensa.

> ”Alamaailma on nyt löytänyt Internetin mahdollisuudet. Se myös käyttää niitä siekailematta hyväkseen. Sen lisäksi harrastusluontoiset viruskirjoittajat ja bot-kooderit ovat huomanneet, että harrastuksella voi tienata rahaa, vieläpä isoja summia.”
>
> Turvallisuus 5/04 s. 20

Näihin toimijoihin liittyy mystifiointi; rikollisia ei kuvata mitenkään eikä heillä tunnu olevan lainkaan ominaisuuksia. Puheessa paistaa vain kylmyys.

4.5.1 Objekti: Rikoksilla mainetta ja mammonaa

Pahojen ihmisten tavoitteena on tehdä rikoksia. Useimmiten rikos on vain väline saavuttaa jokin muu tavoite, mutta välillä rikoksista puhutaan tavoitteena sinänsä. Kun teini tekee tietomurron, hänellä on tavoitteena maine ja kunnia omassa vertaisryhmässään. Häntä ei niinkään kiinnosta murtauduttavan organisaation liikesalaisuudet, oikeastaan koko organisaatio on yhdentekevä.

> ”Teineillä on netissä myös rankinglistoja. Mitä enemmän tietokonemurtoja he tekevät, sen paremmat rankingpisteet he saavat. Teinin maine voi olla kuin keisarilla.”
>
> Turvallisuus 4/04 s. 15

Teinit siis *tahtovat* rikollisen toiminnan kautta kasvattaa mainettaan.

Kun subjektina on vakooja, rikoksen tavoitteena on informaatio. Vakooja voi edustaa kilpailevaa organisaatiota tai valtiota, jolloin salaisia tietoja varastamalla halutaan parantaa omaa asemaa suhteessa kilpailijaan. Jos tavoitteena on enemmänkin propaganda, voi motiivina olla jokin aate tai uskonto. Pahimmillaan kiistat voi äityä sodaksi, joka leviää helposti myös verkkoon.

> ”Irakin sota – tai mikä tahansa laajempi konflikti – aiheuttaa sodan myös tietoverkoissa. Vähintäänkin näemme uusia viruksia ja matoja, verkkosivujen hakkerointia, niin sanottuja palvelunestohyökkäyksiä sekä vaikuttamista maailman mielipiteeseen. Tätä tekevät erilaiset ryhmät, osa huvikseen, osa aatteen vuoksi ja osa rahasta, ja mukana ovat myös valtiot.”
>
> Turvallisuus 2/03 s. 14

Useimmiten vakooja on kuitenkin organisaation omaa henkilöstöä, jolloin informaatiota varastetaan kostoksi tai ahneuden takia. Vakooja voi olla joko oma työntekijä tai organisaation tiloissa työskentelevä henkilö.

> ”Tyypillinen väärinkäytös on yrityksen tietojen varastaminen. Usein tekoon syyllistyy yrityksen oma työntekijä työnantajan maksamalla työajalla. Tällöin viedään esimerkiksi yrityksen asiakasrekisteri tai tuotekehitystietoja, joita hyödynnetään työntekijän itse perustamassa yrityksessä. (…) Jos rikollinen toiminta on organisoitua, odotettavissa voi olla mitä tahansa. Esimerkiksi erääseen liikeyritykseen ujutettiin henkilö siivoojaksi vuodeksi. Tänä aikana hän keräsi vaivihkaa tietoja syvemmältä ja syvemmältä.”
>
> Turvallisuus 3/03 s. 24

Vakoojankin kohdalla kyse on *tahtomisesta*. Rikos ei sinänsä ole tavoite, vaan sillä pyritään saavuttamaan jotain hyötyä.

Krakkerit eivät huvikseen kaappaa tietokoneita, vaan niistä voi esimerkiksi muodostaa laajan bot-verkon, jota voi käyttää palvelunestohyökkäyksiin. Tällä hyökkäyksellä uhkaamalla voi esimerkiksi kiristää (DDos-kiristys).

> ”Jossakin jalkapallomaassa on tulossa ratkaiseva ottelu, jonka tuloksesta lyödään vetoa jättimäisillä rahasummilla. Netissä toimiva vedonlyöntitoimisto saa uhkauksen palvelunestohyökkäyksestä. Jos kiristäjän vaatima summa suojelurahaa ei heti siirry rikollisten tilille, satatuhatta palvelintietokonetta ottaa pian yhteyttä vedonlyöntifirman järjestelmään ja tukkii sen täydellisesti. Vedot jäävät lyömättä, ja raha jää liikkumatta.”
>
> Turvallisuus 5/04 s. 20

Uusi krakkereitten keino on phishing. Tämä tarkoittaa sosiaalista hakkerointia, jossa krakkeri tekeytyy jonkun virallisen tahon edustajaksi ja pyytää salaisia tietoja.

> ”Se (phishing K.I.) on sosiaalista hakkerointia, eli ihmisten henkilökohtaisten tietojen kalastamista erilaisilla virallisen tuntuisilla ”päivityspyynnöillä” rikollisten edelleen käytettäviksi. Tietojen päivityspyyntö tulee erittäin arvostetulta taholta, ja tiedot päivitetään aidon näköisellä, virallisella elektronisella lomakkeella. (…) Sosiaalinen hyökkäys on rikollisille erittäin vahva ja toimiva menetelmä.”
>
> Turvallisuus 5/04 s. 20

Nämä krakkerit *tahtovat* lähinnä taloudellista hyötyä kiristämällä ja salaisia tietoja huijaamalla. Kun yhä useampi palvelu ja informaatio, niin julkinen kuin yksityinen, siirtyy verkkoon, myös nettirikollisten mahdollisuudet kasvavat. Kolikolla on aina kaksi puolta.

Pragmaattisen modaalisuuden näkökulmasta teinin kohdalla modaalisuus on eksotaktista, sillä vertaisryhmän sosiaalinen paine saa teinin murtautumaan jonkin organisaation tietojärjestelmään. Lisäksi muiden tekemistä murtautumisohjelmista riippuu, *kykeneekö* teini murtautumaan järjestelmään. Tarinan teini on siis vahvasti muista riippuvainen. Vakoojan ja krakkerin kohdalla on kyse enemmänkin endotaktisesta, subjektista itsestä riippuvasta modaalisuudesta. Näiltä löytyy tarvittava *osaaminen* rikokseen, ja taloudellinen hyöty saa aikaan rikokseen ryhtymisen. Jos taustalla on jokin aate tai uskonto, joka ajaa subjektin rikokseen, modaalisuuden voi ajatella olevan ulkopuolinen voima, joka vaikuttaa toimijaan sisäisen tulkintaprosessin kautta.

4.5.2 Auttaja ja vasta-subjekti: Käyttäjä ja uhri

Tavoitteen saavuttamista edistää ihminen. Tämä viittaa sellaiseen ihmiseen, joka ei ole ammattilainen tietokoneiden ja niiden käyttämisen suhteen. Esimerkiksi kotikoneen käyttäjä ja yrityksen työntekijä voivat olla auttajia. Tämän tarinan auttaja ei kuitenkaan tietoisesti auta subjektia rikoksessa, vaan tavoitteen edistäminen perustuu lähinnä tietämättömyyteen ja sinisilmäisyyteen.

> ”Vielä vakavampaa on pahaa-aavistamattoman kotikäyttäjän koneen valjastaminen verkossa tehtäviä hyökkäyksiä ja tietomurtoja varten. Kukaan ’järkevä’ rikollinen ei tee hyökkäyksiä suoraan omalta koneeltaan. Hän tunkeutuu suojaamattomaan koneeseen ja tekee hyökkäyksiä sen kautta. Pahantekijän kiinni saaminen on erittäin vaikeaa ja hyväuskoinen tietokoneen omistaja joutuu vähintäänkin kiusalliseen tilanteeseen.”
>
> Turvallisuus 2/03 s. 18

Ihminen on siis auttaja silloin, kun hän ei osaa suojata tietokonettaan tietoturvahyökkäyksiltä. Yrityksen työntekijä auttaa subjektia, kun hän paljastaa yrityksen liikesalaisuuksia ulkopuolisille. Useimmiten tämä ei kuitenkaan ymmärrä, että on tekemisissä vakoojan kanssa.

> ”Jos tekijä ajautuu agentiksi ymmärtämättömyyttään, jossakin vaiheessa hän ryhtyy ihmettelemään ”että mitä kumman outoa ympärilläni oikein tapahtuu”. Tekijän ajatukset ovat tiiviisti ”oudossa”, ja hänen olonsa on kurja. Teot painavat häntä yötä päivää, mutta silti hänen voi olla vaikea kertoa muille ”ystävästään” ja tämän esittämistä pyynnöistä.”
>
> Turvallisuus 4/04 s. 12

Auttaja on riippuvainen subjektin toiminnasta. Se, miten hyvin subjekti pystyy huijaamaan ja harhauttamaan auttajaa, vaikuttaa siihen, miten paljon subjekti auttajastaan hyötyy.

Subjektin tavoitteeseen pääsyä estää rikoksen kohde. Jotta yritys pystyisi estämään vakoilun, sen on panostettava yritysturvallisuuteen.

> ”Kun työntekijä ryhtyy vuotamaan yrityksensä salaista tietoa joko kilpailijalle tai toisen maan edustajalle, yritys on jo myöhässä. Vuotomahdollisuus olisi pitänyt tukkia etukäteen. Sen olisi voinut tehdä olemalla vähemmän sinisilmäinen ja kertomalla henkilöstölle vakoiluun liittyvistä riskeistä.”
>
> Turvallisuus 4/04 s. 12

> ”Yritykset toimivat oikeastaan kummallisesti. Ne investoivat suuria summia upouusiin suojausmenetelmiin, kun yli 95 prosenttia varsinkin teinien tekemistä tietomurroista estetään sillä, että korjausohjelmat asennetaan välittömästi.”
>
> Turvallisuus 4/04 s. 15

Vasta-subjektina toimii myös yhteiskunta. Sen tehtävistä vasta-subjektina ei juurikaan puhuta, ainakaan konkreettisella tasolla.

> ”Suojaamattomat tietokoneet yhteiskunnalle kuin ladattu ase.”
>
> Turvallisuus 2/03 s. 18

> ”Yhteiskunnan kannalta vaarallisempaa on kuitenkin mahdollisuus käyttää hyväksi suojaamatonta tietokonetta niin ettei omistaja edes tiedä siitä. (…) Yhteiskunnan taas tulisi ottaa aktiivisempi rooli tietoturvan edistäjänä – vähintäänkin valistajana.”
>
> Turvallisuus 2/03 s. 18

Vaikka vasta-subjektin oleminen vasta-subjektina muodostuu täysin subjektista ja sen tavoitteesta, vasta-subjekti ei ole mainittavasti subjektin vaikutusvallassa. Rikollinen voi vain toivoa, että sen tavoite jäisi huomaamatta uhrilta ja siten vastarinta jäisi pienemmäksi.

4.5.3 Tarinan opetus

Paha ihminen pyrkii rikkomaan lakia, jotta saisi mainetta tai mammonaa. Keinona on joko informaation varastaminen, DDoS-kiristäminen (palvelunestohyökkäys), sosiaalinen hakkerointi (phishing) tai murretun järjestelmän kaappaaminen omaan käyttöön. Tavallinen tietokoneen käyttäjä ja yrityksen työntekijä edistää tietämättään ja tahtomattaan subjektia rikollisissa toimissa. Pahaa ihmistä hidastaa rikoksen kohde; kun yritys tai yhteiskunta panostaa tietoturvallisuuteen, rikos ei enää kannata yhtä varmasti.

Vaikka paha ihminen ei tässä tarinassa juuri ominaisuuksia saa, jotain myönnytyksiä sillekin suodaan. Toiminnalle löytyy rationaalinen selitys, hyödyn tavoittelu, joten paha ihminen ei edusta puhtaasti pahuutta, vaan saa hieman inhimillistä ymmärrystä. Syyllisyyttä vieritetäänkin melko vahvasti tavallisen ihmisen harteille. Vaikka todetaan, että tietokoneen käyttäjältä vaaditaan liikaa, heti perään muistutetaan, että vastuu on kuitenkin koneen omistajalla. Yritysvakoilussa sormi osoittaa työntekijään, joka on lipsauttanut jotain salaista. Nähdäänkö subjekti, rikollinen liian ylivoimaisena vastuksena, kun kukaan ei nouse sitä vastaan ja vaadi tilille?

5 Asiantuntija, maallikko ja tekniikka riskiyhteiskunnassa

Kertomukset on nyt käyty läpi. Ne kaipaavat hieman lisätarkastelua, jotta analyysiin saisi lisää syvyyttä ja ymmärrettävyyttä. Nostan kertomuksista esiin toimijat ja niiden väliset suhteet, että voin tutkia niitä riskiyhteiskunnan valossa. Tämä mielestäni auttaa ymmärtämään, miksi kyseiset toimijat nähdään niin kuin analyysissani kuvailen. Lisäksi on helpompi havaita, mitkä ovat tietoturvallisuuskeskustelun pinnan alla majailevia todellisia ongelmia ja pohtia sitä, löytyisikö näihin ongelmakohtiin ratkaisua. Haluan silti korostaa, että kyse ei ole vuorovaikutustutkimuksesta, vaan luonnehdin, miten aineiston narratiiveissa kuvataan näitä toimijoita ja heidän välisiä suhteitaan.

Nämä edellä esitellyt tarinat ovat eräänlaisia kehityskertomuksia, mikä on tyypillistä tietotekniikkaa käsitteleville teksteille. Pantzar huomauttaa, että teknologiahistoriat ja –visiot pohjautuvat edistysmyyttiin, jossa uskotaan lineaariseen menestystarinaan. Nämä tarinat jättävät epäonnistumiset kertomatta ja häviäjät vaipuvat unohduksiin. Siksi teknologian kehitys näyttää yksinkertaiselta ja lineaariselta. (Pantzar 1996, 148-149.) Uusien teknologisten innovaatioiden saapuessa markkinoille puhutaan vain niiden tuomista eduista. Kun jossain vaiheessa myös haittapuolia alkaa ilmaantua, yleinen hämmästys on suuri. Tämänhän piti tuoda parannusta eikä uhkia elämään. Teknologinen edistysusko on juurtunut syvälle.

Vaikka valtiovalta ei saa roolia tarinoissa, se ei tarkoita, että valtiolla ei olisi merkitystä. Valtiovaltaa ja yhteiskuntaa peräänkuulutetaan lähinnä valistajaksi. Siksi näen tarpeelliseksi luoda nopean katsauksen valtion rooliin riskiyhteiskunnassa. Eerik Lagerspetz tarjoaa kolmea teesiä kuvaamaan aikaamme. Ensinnäkin modernisaation myötä varmuuden ja tietämättömyyden kokemukset ovat muuttuneet riskin ja epävarmuuden kokemuksiksi. Erilaisia katastrofeja voidaan ennakoida ja niihin voidaan varautua. Tapahtuvista onnettomuuksista pystytään minimoimaan menetykset ja arvioimaan vahingot. Toisen teesin mukaan modernissa yhteiskunnassa ulkoiset riskit pyritään näkemään rationaalisten tekniikoiden ja rutiinien avulla kontrolloitaviksi. Riskienhallinta tarvitsee kollektiivista toimintaa, mutta haluttuja hyödykkeitä, kuten vakuutusjärjestelmiä ja riskejä minimoivaa teknologiaa ei pystytä toteuttamaan vapaaehtoisvoimin. Siksi tarvitaan valtiota ja kolmas teesi kytkeytyy tähän; valtio on oleellinen ulkoisten riskien kontrolloija modernissa yhteiskunnassa. Tämä ilmenee parhaiten hyvinvointivaltiossa, jossa yksittäinen kansalainen tuntee olonsa turvatuksi niin yhteiskunnallisten kuin luonnollisten riskien suhteen. Hyvinvointivaltio vastaa viime kädessä yksilön riskinhallinnasta ja sen epäonnistumisesta. Lagerspetz toteaakin, että epävarmuus on sosialisoitu. (Lagerspetz 1997, 95-99.)

Hyvinvointivaltio on onnistunut vähentämään yksilöön kohdistuvia riskejä, mutta samalla yksilö olettaa, että kaikki riskit ovat ennakoitavissa. Kun jotain odottamatonta tapahtuu, syytetään valtiota tiedon hankkimisen ja jakamisen laiminlyönnistä. Vaikka syylliseksi voitaisiin osoittaa joku muu, valtio on aina osasyyllinen. Valtio on vastuussa teknisten järjestelyjen riittävyydestä, korvausten kattavuudesta ja kansalaisten valistuksesta. (Lagerspetz 1997, 99-100.) Tuntuu kuin ilmiöiden muuttuessa liian

ongelmallisiksi, ne pyrittäisiin siirtämään valtion harteille. Myös tietoturvallisuuden kohdalla valtiovalta huudetaan mukaan siinä vaiheessa, kun asiantuntijat eivät pystykään enää itse vastaamaan tietoturvallisuuden haasteisiin.

Taulukkoon 5.1 olen kerännyt tarinoiden toimijat. Osa toimijoista esiintyy useammassa kuin yhdessä kertomuksessa, joten loppujen lopuksi erilaisia toimijoita ei olekaan niin monta.

	Subjekti	**Auttaja**	**Vasta-subjekti**
Organisaatio tavoittelee yhteistyötä	Organisaatio	Subjekti itse eli organisaatio	Subjekti itse eli organisaatio
Hyötyohjelma torjuu hyökkäykset	Hyötyohjelma	Asiantuntija	Ei-tekninen henkilö
Haittaohjelma leviää	Haittaohjelma	Ei-tekninen henkilö	Tekniikka
Hyvä ihminen kehittää tietoturvallisuuttaan	Hyvä ihminen	Tekniikka	Asiantuntija
Paha ihminen rikkoo lakia	Paha ihminen	Ei-tekninen henkilö	Rikoksen kohde/uhri

Taulukko 5.1. Kertomusten toimijat

Selvennyksen vuoksi olen ryhmitellyt toimijat ryhmiin taulukkoon 5.2, jotta niiden lähempi pohdinta olisi helpompaa. Rikoksen kohde/uhri –toimijaa en tällä nimellä mainitse taulukossa, sillä konkreettiset toimijat sisältyvät muihin ryhmiin, kuten yritys taloudellisiin toimijoihin. Hyvä ja paha ihminen näyttäytyvät niin asiantuntijassa kuin ei-teknisessä toimijassa, koska tarinoissakin ne esiintyvät näissä erilaisissa rooleissa. Taulukosta huomaa, että osa erilaisista toimijoista on inhimillisiä (ryhmät asiantuntija ja ei-tekninen henkilö). Tähän kuuluu joukko erilaisia ihmisiä erilaisine päämäärineen ja arvoineen, kuten tuo useaan kertaan mainittu tietoturvallisuuden heikoin lenkki. Näihin toimijoihin perehdyn syvällisimmin, onhan ihminen oleellinen osa yhteiskuntaa ja sen

olemusta. Toisessa kategoriassa ovat tekniset toimijat. Tekniikalla on merkittävä asema tietoturvallisuudessa ja kuten toimijaverkkoteoriassa korostetaan, tekniikkakin voi toimijana olla vuorovaikutuksessa ihmisten kanssa. Tekniikka näyttäytyy mielenkiintoisella tavalla kertomuksissa, kuin se heräisi eloon päästyään ihmisten ilmoille. Tähänkin pureudun jäljempänä.

Organisaatiot toimivat talouselämässä ja ovat myös tärkeä osa yhteiskuntaa. Tässä yhteydessä jätän kuitenkin organisaatioiden tarkastelun vähiin, koska se olisi mielestäni hedelmätöntä. Kuten ensimmäisessä, organisaatiota käsittelevässä tarinassa kerron, organisaatiot näyttäytyvät omassa bisnesmaailmassaan, jossa muilla toimijoilla kuin yrityksillä ei ole merkittävää vaikutusta. Tämä liiketoiminnan kyllästämä todellisuus on erilainen sosiaalinen maailma kuin muissa tarinoissa. Toiminta on täysin rationaalista ilman inhimillisiä emootioita. Teknologisen determinismin näkökulmasta tätä maailmaa leimaa vapaan markkinatalouden idea. Organisaatiot pystyvät valinnoillaan ohjaamaan teknologian kehitystä liiketoimintaa tukevaan suuntaan.

Asiantuntija	Ei-tekninen henkilö	Tekniset toimijat	Taloudelliset toimijat
Asiantuntija Hyvä ihminen Paha ihminen	Hyvä ihminen Paha ihminen Ei-tekninen henkilö	Tekniikka Hyötyohjelma Haittaohjelma	Organisaatio

Taulukko 5.2. Kertomusten toimijat ryhmittäin

5.1 Tekniset toimijat

Tekniset toimijat kertomuksissa ovat hyöty- ja haittaohjelmia. Kummatkin esiintyvät subjekteina omissa tarinoissaan, ja hyvän ihmisen auttajana sekä haittaohjelman vasta-subjektina mainittu tekniikka viittaa hyötyohjelmaan. Vaikka nämä toimijat ovat periaatteessa rakenteeltaan samanlaisia ja vaikuttavat tietoturvallisuuden alueella, niistä puhutaan silti eri tavalla. Vaikka näitä kumpaakin kuvataan elävinä toimijoina monin

tavoin, niiden toimintaa ei sentään nähdä päämäärätietoiseksi. Toimintaa leimaa halu eli haittaohjelman leviäminen ja hyötyohjelman tietoturvahyökkäysten torjuminen on tavoite itsessään.

Hyötyohjelman toimintaan vaikuttavat tekijät ovat enimmäkseen sen ulkopuolisia, kuten taulukosta 5.3 selviää. Sen täytyy tunnistaa haittaohjelmat, koska se on tehty sitä varten. Hyötyohjelma on ihmisistä riippuvainen, sillä sen toimintakyky on pitkälle kiinni sen kehittäjistä ja päivittäjistä. Kehittyneemmillä ohjelmilla löytyy osaamista tunnistaa haittaohjelmat ja ne kykenevät kehittymään. Hyötyohjelman funktio on haittaohjelmien tunnistaminen ja pysäyttäminen, toisin sanoen sen olemassaolo ja ominaisuudet määrittyvät haittaohjelmien kautta.

Käyttäjiin hyötyohjelmalla ei ole valtaa, mutta käyttäjät voivat toiminnallaan vaikuttaa hyötyohjelman onnistumiseen. Hyötyohjelman nähdään silti olevan ihmistä kyvykkäämpi, koska se pystyy tekemään sellaista mitä ihminen ei pysty, kuten tunnistamaan haittaohjelmat.

> ”Palomuuri kysyy teknisillä termeillä, haluatko sallia vai estää jonkin tietyn pakettityypin, mutta käyttäjä ei ymmärrä, mitä se käytännössä tarkoittaa.”
>
> Turvallisuus 1/03 s. 30

Käyttäjä ei ymmärrä palomuurin eli hyötyohjelman kieltä, koska he eivät ole osaamiseltaan tasavertaisia. Yllä olevassa aineistolainauksessa voi nähdä yhden tavan inhimillistää tekniikkaa: palomuuri yrittää *kommunikoida* käyttäjän kanssa. Myös oppiminen ja luominen mainitaan hyötyohjelman ominaisuuksiksi.

> ”(Roskapostisuodattimen KI) oppimismoduuli oppii myös harvinaisempien roskapostien sisällöt ja luo omia organisaatiokohtaisia sääntöjä automaattisesti.”
>
> Turvallisuus 2/04 s. 22

Oppiminen ei ole varsinaisesti inhimillinen ominaisuus, mutta yleensä se liitetään johonkin elävään olentoon. Oppiminen vaatii tietoisuutta ympäristöstä, jotta asiat osaisi yhdistää oikein toisiinsa. Luominen taas tarvitsee syy-seuraus –suhteen ymmärtämistä melko kokonaisvaltaisesti.

	Endotaktinen modaalisuus	Eksotaktinen modaalisuus
Hyötyohjelma	- osaa tunnistaa haittaohjelmat	- kykenee toimimaan (päivitys) - täytyy tunnistaa haittaohjelmat (tekijät)
Haittaohjelma	- haluaa levitä - osaa hyödyntää tietoturva-aukkoja	- kykenee leviämään (tietoturvan taso)

Taulukko 5.3. Teknisten toimijoiden modaalisuuden lajit

Haittaohjelma on hyötyohjelmaa itsenäisempi toimintaan vaikuttavien tekijöiden suhteen (taulukko 5.3). Se leviää, koska se itse haluaa levitä. Lisäksi se osaa hyödyntää tietoturva-aukkoja. Ulkopuolisena tekijänä haittaohjelmaan leviämiseen vaikuttaa eri järjestelmien tietoturvan taso. Haittaohjelma on hyötyohjelmaa kehittyneempi, koska se on aina hyötyohjelmaa askeleen edellä. Hyötyohjelma voidaan luoda vasta, kun haittaohjelma on jo olemassa. Haittaohjelma ei myöskään ole tekijästään tai muista inhimillisistä toimijoista riippuvainen, sillä verkkoon päästessään se alkaa elää omaa elämäänsä ja noudattamaan omaa päämääräänsä.

Haittaohjelmaan liitetään paljon enemmän abstrakteja ominaisuuksia kuin hyötyohjelmaan, esimerkiksi oveluus ja häijyys. Elävän olennon piirteitä nähdään myös haittaohjelmassa. Siihen yhdistetään muun muassa hallitsemattomasti lisääntyvän loisen tuntomerkkejä.

> ”Elokuu 2003 oli painajaismainen kuukausi tietokonevirusten torjujille. Entistä häijympiä viruksia ja matoja sikisi kuin sieniä sateella.”
> Turvallisuus 5/03 s. 20

> ”Ne (virukset KI) tarvitsevat isännän levitäkseen. Nykyisillä viruksilla isäntänä toimii yleensä sähköpostiviesti ja siinä oleva tiedostoliite.”
> Turvallisuus 5/03 s. 20

Sikiäminen liitetään useimmiten epämiellyttävien eliöiden tai eläinten ei-toivottuun lisääntymiseen. Myös isännän tarvitseminen assosioidaan loiseläjiin. James A. Aho huomauttaa, että vihollista pidetään kaiken vääryyden, vaaran ja kuoleman perikuvana. Se on oikeastaan jätettä, joka on poistettava vaarantamasta tervettä yhteisöä. (Harle

1991, 17.) Haittaohjelma nähdään tuollaisena vihollisena, sillä siihen liitetään useaan otteeseen muun muassa tuho, vaarallisuus ja vahingoittaminen.

Vaikka virukset ja madot tuodaan esiin vihollisina, niitä myös inhimillistetään.

> ”Ympäri maailmaa leviää tieto Sobig-virusperheen uusimmasta tulokkaasta, tietokonemato Sobig.F:stä.”
>
> Turvallisuus 6/03 s. 12

Maininta virusperheestä viittaa sukulaisuusjärjestelmään ja siten tuo virukset lähemmäs sosiaalista maailmaa. Vaikka vihollinen halutaan rajata kauas itsestä, ihmisillä on silti tarve ymmärtää vihollista.

Siinä missä hyötyohjelma ei pysty vaikuttamaan käyttäjään, haittaohjelma pystyy. Se huijaa käyttäjää monella tapaa, jotta se voisi levitä mahdollisimman tehokkaasti. Haittaohjelman vaarallisuutta silti liioitellaan helposti, mikä voi aiheuttaa turhaa paniikkia.

> ”He (tietoturva-asiantuntijat KI) saavat selville, että kyse on pahamaineisen ovelasti rakennetusta operaatiosta. Internetistä löytyvän atomikellon avulla Sobif.F iskee 22.8.2003 Suomen aikaa kello 22.00 satoihin tuhansiin Internetin kautta toisiinsa synkronoituihin tietokoneisiin ja suorittaa tehtävän, jonka sisältöä ei tiedetä.”
>
> Turvallisuus 6/03 s. 12

> ”Tämä on tositarina siitä, miten tietokonemaailmassa hyvä ja paha taistelivat keskenään, ja hyvä voitti. Parillakymmenellä minuutilla.”
>
> Turvallisuus 6/03 s. 12

Kun kyseessä on vihollinen, se nähdään kaikin puolin pahana. Viholliskuvassa korostuukin hyvän ja pahan vastakkainasettelu. Viholliskuva kieltää vihollisen inhimilliset piirteet ja korostaa aggressiivisuutta, väkivaltaisuutta ja tuhoisuutta. (Harle 1991, 15.) Mielikuvituksen tuottamat ajatukset ja käsitteet koetaan joskus todellisuuden ilmentyminä. Tällöin kyseessä on *reifikaatio* eli objektivointi. Ihmisen itsensä luoma kuva sosiaalisesta todellisuudesta koetaan annetulta ja samalla kuvitellaan, ettei tuohon sosiaaliseen todellisuuteen pysty itse vaikuttamaan, saati olemaan siitä vastuussa. Vihollinen on yksi reifikaation ilmentymä. (Harle 1991, 44.) Vaikka haittaohjelman toiminnasta ei tiedettäisi paljoa, ollaan varmoja sen olevan jotain kauheaa. Tätä pahan mystifiointia on hyödynnetty tunnetusti fiktiivissä tarinoissa. Tuntematon uhka herättää mielikuvituksen valloilleen ja saa pelkäämään pahinta. Kun vielä on tunne, ettei tuohon uhkaan voi itse vaikuttaa, on paniikki enemmän kuin totta.

Vaikka hyötyohjelma nähdään käyttäjää etevämmäksi, se ei pysty vaikuttamaan käyttäjään, mutta käyttäjä pystyy vaikuttamaan siihen. Kehittyneempi haittaohjelma kykenee muokkaamaan käyttäjän toimintaa. Toimijaverkkoteorian mukaisesti osa teknisistä tietokoneohjelmat pystyy vaikuttamaan ihmiseen ja ihminen pystyy vaikuttamaan niihin. Ihmiset ja tekniikka ovat siis vuorovaikutuksessa keskenään, mutta vuorovaikutus käsitetään yleensä elävien olioiden toimintana. Tekniikan inhimillistämisen voi nähdä ratkaisuna tälle dilemmalle. Hyöty- ja haittaohjelmat näyttäytyvät aineistossa teknologisen determinismin värittämänä. Tekniikka tuntuu kehittyvän omaehtoisesti ja haittaohjelmiin vastataan vain hyötyohjelmilla. Ongelmaksi muodostuu se, että riskiyhteiskunnassa tekniset ratkaisut eivät riitä. Tietoturvallisuus vaatii monipuolisempia vastauksia.

5.2 Asiantuntijat

Kertomusten asiantuntijat ovat joko tietoturvallisuuden puolesta työskenteleviä tietoturvavastaavia ja ohjelmistojen kehittäjiä tai tietoturvallisuutta vastaan toimivia krakkereita, vakoilijoita, roskapostin lähettäjiä ja muita nettirikollisia. Tietoturvavastaava näyttäytyy yhdessä tarinassa päähenkilönä, joka on lähinnä sankarillinen johtaja. Lisäksi ohjelmistojen kehittäjät auttavat hyötyohjelmaa taistelussa haittaohjelmia vastaan. Nettirikollinen tavoittelee taloudellista hyötyä tai aatteellista voittoa omassa tarinassaan. Sen sijaan vasta-subjektina se heikentää hyvän ihmisen tietoturvallisuutta.

Tietoturvallisuuden puolesta toimivat asiantuntijat tuodaan esiin täysin ammattinsa tai kompetenssinsa kautta, ei niinkään henkilökohtaisten ominaisuuksien avulla. Heillä on osaaminen, jota he käyttävät. Heidän ammattilaisuuttaan korostetaan erilaisin tittelein ja saavutuksin.

> ”Poliisin tietohallintokeskuksen tietoturvapäällikkö Aaro Hallikainen on tietoturvallisuuden vankka ammattilainen. Hän on yksi niistä 107 suomalaisesta, joilla on tietoturvallisuuden laaja-alaisen osaamisensa vakuutena CISSP-sertifikaatti. Hallikainen on myös Tietoturva ry:n aktiivijäsen sekä kysytty luennoitsija eri tietoturvatilaisuuksissa. Lisäksi hän matkustelee tietoturva-asioissa ympäri maailmaa ja on mukana myös

> Valtiovarainministeriön asettamassa, valtionhallinnon tietoturvallisuuden johtoryhmässä VAHTIssa.”
>
> Turvallisuus 1/04 s. 12

Kuten aiemmin tuli esille, asiantuntijuuden todistamiseksi ei enää riitä pelkkä tutkintotodistus. Tässäkin sen tukena on mainittu erilaiset luottamustehtävät, titteli ja työpaikka sekä haluttuna luennoitsijana toimiminen. Kun henkilöllä on näin vankka osoitus asiantuntijuudestaan, hän on oikeutettu kommentoimaan ilmiötä uskottavasti. On myös huomioitava, että aineiston artikkelit on suunnattu turvallisuusalan ammattilaisille ja niiden sisältämien tietojen takana on vastaavat ammattilaiset. Jokinen toteaakin, että asiantuntijan sosiaaliseen asemaan liittyy tietynlainen puhetapa ja –oikeus sekä asiantuntijuutta vahvistavat muun muassa sosiaaliset verkostot ja palkkiot. Sosiaalinen ja tiedollinen asiantuntijuuden ulottuvuus vaikuttavat toisiinsa, sillä tiedon jakamisen oikeus edellyttää kuulumista tiettyyn sosiaaliseen järjestelmään. (Jokinen ym. 2001, 175.) Voikin sanoa, että alan sisäisen keskustelun avulla asiantuntijat ylläpitävät ammatti-identiteettiään ja olemassaolonsa tärkeyttä.

Tietoturva-asiantuntijat tuntuvat katsovan koko tietoturvallisuuden temmellyskenttää muiden yläpuolelta. Jos he yksin osallistuisivat tietoturvallisuuden ylläpitämiseen, ongelmia olisi huomattavasti vähemmän. Asiantuntijat hoitavat osuutensa, suurin vika on muissa. Asiantuntijoiden tavassa siirtää ongelmat muiden syyksi voi havaita Beckin mainitsemaa organisoitua vastuuttomuutta. Asiantuntijuuteensa vedoten he sysäävät liian suuret ongelmat yhteiskunnan vastuulle. Samasta syystä asiantuntijat voivat vaikuttaa merkittävästi siihen, miten Beckin nimeämiä haitakkeita jaetaan. Asiantuntijoilla on silti vastuu lausunnoistaan, sillä monet poliittiset päättäjät tukeutuvat päätöksissään asiantuntijoiden sanaan.

Myös modaalisuuden lajeja tarkasteltaessa taulukossa 5.4 voi huomata, että asiantuntijat näkevät itsensä varsin suvereenina, sillä ulkopuoliset tekijät eivät tunnu vaikuttavan heidän toimintaansa. Tietoturvallisuuden kehittämiseen vaikuttaa vain oma osaaminen ja tahto.

> ”Siksi jokaisen tietoturvallisuuden laadusta vastaavan pitää itse keksiä, miten aikoo onnistua muutosten läpiviemisessä. Antaako esimerkiksi ’terrierin’ nykiä niin kauan ylimmän johdon housunlahjetta, että hyväksyntä muutokseen lopulta saadaan. Vai kannattaako muutoksen toteuttaminen organisoida jollekin toiselle työryhmälle, ja toimia itse valmentajana. Vai kannattaako keksiä joku kolmas keino.”

Asiantuntijat ovat toki tärkeässä asemassa, sillä heidän tietämykseensä luotetaan päätöksenteossa. Heiltä vaaditaan yhä enemmän alojen rajoja ylittävää yhteistyötä ja samalla erikoistunutta osaamista. Hyvän asiantuntijan tunnistaa siitä, ettei hän jähmety tai sulje korviaan, mutta ei myöskään liioittele tietämystään (Jokinen ym. 2001, 175). Asiantuntijoiden olisi hyvä välillä katsoa peiliin ja pohtia omaa asiantuntijuuttaan sekä sen kattavuutta. Norsunluutornista ei loppujen lopuksi näe kovin kauas.

Yhden pohdittavan näkökulman tarjoaa Tiainen ATK-asiantuntisuuden maskuliinisuuteen syventyvässä tutkimuksessaan. Kun teknologian kehityksessä käytetään vain miehistä osaamista, tekninen nerous jättää helposti käyttötarkoituksen jalkoihinsa. Alan asiantuntijat tekevät yhteistyötä monien muiden asiantuntijoiden kanssa, joten toisten ymmärtäminen ja tiimityötaidot ovat tärkeitä. Nämä ominaisuudet liitetään naisiin, sen sijaan miehisinä ominaisuuksina pidetään itseriittoisuutta ja dominoivuutta. Kun asiantuntija-areenoille halutaan moniäänistä keskustelua, osanottajiksi tarvitaan myös naisia. (Tiainen 2002, 131-133.) Van Loon vertaa ilmiötä teknologiapainotteisiin tiedefiktioihin, jotka voi nähdä maskuliinisina fantasioina vallasta ja hallinnasta. Miehinen eetos on itsetuhoinen, sillä se on liian heikko ja sulkeutunut nähdäkseen riskit järkevästi. Maskuliinisuutta voi pitää käskyvaltaisena riskienhallinnan muotona, jossa ei ole juurikaan tilaa kommunikaatiolle ja ymmärrykselle. Se on liian sokea omalle epäautenttiselle olemiselleen. (Van Loon 2000, 179.) Aineistoni asiantuntijoista lähes kaikki ovat miehiä, nainen taitaa olla se poikkeus, joka vahvistaa säännön. Tiaisen näkemyksen valossa yksi asiantuntijan ja maallikon välisen kommunikaation ongelmista voi olla se, että maskuliininen asiantuntijayhteisö ei osaa eikä halua ymmärtää käyttäjää. Vaikka tekniset sovellukset tehdään juuri tuota maallikkoa varten, asiantuntija ei itseriittoisuudessaan halua laskeutua maallikon tasolle kuuntelemaan, miksi maallikko on heikoin lenkki ja mitä sen vahvistamiseksi voisi tehdä.

	Edotaktinen modaalisuus	Eksotaktinen modaalisuus
Tietoturva-asiantuntija	- tahtoo kehittää tietoturvaa - osaa kehittää tietoturvaa	
Nettirikollinen	- tahtoo rikkoa lakia - osaa tehdä rikoksen	

Taulukko 5.4. Asiantuntijoiden modaalisuuden lajit

Nettirikollisilla ja tietoturva-asiantuntijoilla on tietämyksen lisäksi yhteisenä tekijänä itsenäisyys. Taulukosta 5.4 näkyy, ettei nettirikollisen toimintaan ulkopuolisilla tekijöillä ole vaikutusta. Tahtominen ja osaaminen rikoksen tekemiseen kumpuaa tekijästä itsestään. Tästä näkökulmasta taistelu rikollisuutta vastaan on melko tehotonta, sillä mikään ulkopuolinen taho ei pysty vaikuttamaan rikollisiin. Mutta kun muistaa, että aineisto rakentuu asiantuntijoiden näkökulmasta, voi miettiä, haluaako asiantuntijayhteisö turvata selustansa. Kun pahimmat vastustajat rajataan ulottumattomissa oleviksi, oma vastuualue on helpommin hallittavissa.

Vaikka nettirikolliset kuvataan alamaailman edustajina, ei heitä nähdä yhtä pahoina kuin haittaohjelmia. Heidän teoilleen nähdään motiivit.

> ”Vakoilu on keino tehdä rahaa. Sitä tehdään, koska yritykset ja valtiot haluavat taata, että ovat olemassa vielä huomennakin.”
> Turvallisuus 4/04 s. 14

Motiivit auttavat ymmärtämään, miksi joku rikko lakia. Keino tehdä rahaa selittää tekoa, vaikka ei tee siitä oikeutettua. Toisaalta tällainen rationaalinen lähestymistapa muistuttaa taas asiantuntijuudesta. Rikokset eivät kohdistu tietoturva-asiantuntijoita vastaan, vaan pikemminkin kyse on kilpajuoksusta rikollisen ja asiantuntijan välillä: kumpi ehtii huomaamaan ensin tietoturva-aukon. Rikolliset halutaan silti rajata kauas itsestä. Kerran rikollinen mielletään aina rikolliseksi. Lisäksi vastakohtia korostetaan painokkaasti. Ranskalainen kulttuuritutkija René Girard korostaa dualististen vastakohtien merkitystä sosiaalisen järjestyksen perustana. Yhteisölliseen elämään kuuluu erottelu ystävän ja vihollisen välillä, lakien noudattajiin ja rikkojiin. Tämä erottelu on luonteeltaan myyttistä ja sitä ylläpidetään kollektiivisesti. Lisäksi myyttien avulla muodostetaan pahan illuusio. James A. Aho näkee, että sosiologisessa mielessä

vihollinen nousee yhteisön alapuolelta, alamaailmasta niin kuin arkikielessäkin rikollisia kuvataan. Se nähdään epäjärjestyksen edustajana, normaalin poikkeamana. Me siis kuvastamme oikeaa ja hyvää, kun taas vihollinen on kaiken vääryyden, vaaran ja kuoleman perikuva. (Harle 1991, 17.)

Kun rikoksia lähestyy uhrin näkökulmasta, korostuu ylläkuvattu vastakkainasettelu. Yleensä vihollisen toiminnassa päähuomio suuntautuu kielteiseen toimintaan ja siten motiivitkin voidaan selittää kielteisinä. Vihollisen hyvät teot selitetään kontekstista johtuviksi tai sillä, että taka-ajatuksena on joka tapauksessa jotain pahaa. Lisäksi sen inhimilliset ominaisuudet pyritään kieltämään, joten vihollinen nähdään ei-ihmisenä. (Harle 1991, 35-36.) Vihollinen määrittyy kulttuurin värittämänä. Vihollista kuvailtaessa korostetaan vihamielisyyttä sekä vaarallisuutta ja varsinkin kokijaan kohdistuvia uhkia. (Harle 1991, 47.) Baumeister ja Vohs puhuvat pahuudesta lähinnä väkivallan näkökulmasta, mutta heidän näkemyksiään voi soveltaa muuhunkin rikollisuuteen. Kun uhreilta ja pahantekijöiltä on kysytty selityksiä tekoon, on näiden kahden välillä selkeä ymmärryksen kuilu. Uhrin mielestä teolle ei ole mitään järkevää selitystä, kenties sen takana oli silkka ilkeys. Pahantekijä itse löytää teolleen ymmärrettävän motiivin, vaikka tietää tehneensä väärin, joskus jopa näkee tekonsa oikeutetuksi. Uhri ei halua eikä pysty ymmärtämään pahantekijänsä näkökulmaa. Uhri näkee vahingon todellista suuremmaksi, kun taas pahantekijä väheksyy sitä. Uhri tuntee itsensä täysi viattomaksi, mutta pahantekijä katsoo uhrin provosoineen tekoon. Objektiivista totuutta on lähes mahdoton määritellä, mutta kannattaa muistaa, että hyvin harva hyökkää ilman syytä. (Baumeister & Vohs 2004, 88-90.)

Baumeister on määritellyt pahuuden ydinsyyt, jotka kytkeytyvät myös tietoturvarikollisiin. Kaikki Baumeisterin mainitsemat pahuuden syyt tuodaan esiin aineistossani. Selityksiä nettirikollisuuteen tarjotaan, vaikka rikolliselta niitä ei olisi kysyttykään. Taas korostuu ihmisen tarve ymmärtää muiden toimintaa. Ensinnäkin tekijä pyrkii saamaan haluamansa keinolla millä hyvänsä. Tässä ei tavoite, esimerkiksi raha tai kunnia, ole paha, mutta keinot sen sijaan ovat. Nämä keinot näyttävät helpolta tavalta ansaita nopeasti. Tämä taktiikka ei tuota tulosta kovinkaan hyvin pitkällä tähtäimellä, sillä harva rikollinen vanhenee rikkaana ja onnellisena. (Baumeister & Vohs 2004, 91.) Monia nettirikollisia motivoi kenties nopea tapa tehdä rahaa pienellä kiinnijäämisriskillä. Toisena syynä Baumeister mainitsee uhatun egoismin. Tässä

hyökkäys tapahtuu ylpeyttä loukannutta tahoa vastaan. Kyse ei siis ole mistään materian tavoittelusta vaan kostosta. (Baumeister & Vohs 2004, 91-93.) Esimerkiksi kaunainen irtisanottu saattaa kostoksi murtautua entisen työnantajansa tietojärjestelmään ja tuhota tietoja tai varastaa liikesalaisuuksia. Kolmantena syynä pahuuteen on yritys saavuttaa hyvää. Tämä on pahuuden syistä se traagisin. Tässä tarkoitus pyhittää keinot. Taustalla on usein jokin idealismi eli moraalinen velvoite ajaa tekemään pahaa, jotta saavutettaisiin jotain hyvää. (Baumeister & Vohs 2004, 93-95.) Aatteen ajamat krakkerit saattavat vakoilla vihollistaan ja käyttää saamaansa informaatiota tätä vastaan. Viimeisenä Baumeister tuo esiin sadismin. Tämä on uhrien mukaan yleisin syy, samoin fiktiivisissä tarinoissa, mutta todellisuudessa hyvin harvinainen. Ulkopuoliset kuvittelevat, että pahantekijä nauttii aiheuttamastaan vahingosta ja satuttaa silkasta ilosta. Käsitys puhtaasta pahuudesta on myytti, sillä hyvin harva pahantekijä nauttii vahingon teosta. (Baumeister & Vohs 2004, 96-98.) Tietoturvarikoksen uhrikin helposti ajattelee, että syyllinen on halunnut vain aiheuttaa tuhoa, koska rikollinen tekee rikoksia.

Vaikka aineistossa rikollisesta toiminnasta puhutaan enimmäkseen asiantuntijoiden näkökulmasta, myös uhrin näkökulma piirtyy esiin.

> ”Koodin kirjoittajat voivat haavoittaa koko maailmaa. He voivat tehdä maailmanlaajuisen hyökkäyksen Internetiä vastaan.”
> Turvallisuus 6/03 s. 12

Koko maailman haavoittaminen lienee liioittelua, ja teon irrationalisointi viittaa tyypilliseen uhrin ajattelutapaan. Tämän näkökulman huomioiminen on mielestäni tärkeää, sillä uhri on useimmiten käyttäjä ja tämän toimijan merkitykselliseen asemaan pääsemme tutustumaan seuraavassa kappaleessa.

Asiantuntijuudella on vaikuttava rooli riskiyhteiskunnassa. Sitä tarvitaan päätöksenteossa, mutta samalla se politisoituu yhä enemmän. Ennen kuin asiantuntijoita uskoo, kannattaa pohtia, kenen intressejä tavoitellaan. Asiantuntijoiden ylivertaisuutta karakterisoi se, että muut toimijat eivät pysty vaikuttamaan siihen. Sen sijaan asiantuntijat ovat voineet määrittää muiden toimijoiden aseman. Kuten teknisten toimijoiden kohdalla, myös asiantuntijat tuodaan esiin teknologisen determinismin valossa. Erona on se, että jälkimmäisten kohdalla kyse on enemmänkin

teknokraattisesta lähestymistavasta. Tekniikkaa ei voida tässäkään ohjata, mutta asiantuntijat voivat opastaa muita sopeutumaan muuttuvaan tekniikkaan.

Nettirikolliset edustavat myös omanlaista asiantuntijuutta, vaikka sitä ei usein niin mielletäkään. Mielenkiintoinen piirre nettirikollisista puhuttaessa on niille suotu yllättävän pieni merkitys tietoturvallisuuden uhkana. Eikö tietoturvallisuuden puolesta toimivat asiantuntijat halua myöntää voimattomuuttaan vai löytyykö sittenkin parempi vihollinen?

5.3 Ei-tekniset toimijat

Ei-tekniset toimijat ovat niin sanottuja maallikoita, joiden osaaminen tietoturvallisuudesta ja tietokoneista ei ole asiantuntijatasolla. Kertomuksissa näitä ovat tietokoneen käyttäjät, yritysten työntekijät ja teinit eli script kiddiet. Jälkimmäiset tuntevat kyllä sen verran tietokoneita ja Internetiä, että osaavat etsiä käsiinsä murto-ohjelmia ja pystyvät niiden avulla murtautumaan tietojärjestelmiin. Ei-tekniset toimijat esitetään mielenkiintoisimmalla tavalla, sillä ne nähdään lähinnä tietoturvallisuuden estäjänä. Maallikko vaikeuttaa hyötyohjelmien toimintaa ja edistää haittaohjelman sekä pahan ihmisen pyrkimyksiä. Työntekijä on subjektina yhdessä tarinassa, mutta siinäkin hän tarvitsee vahvaa ohjeistusta toimiakseen oikein.

	Endotaktinen modaalisuus	Eksotaktinen modaalisuus
Käyttäjä eli maallikko		- Täytyy kehittää tietoturvallisuutta (tietoturva-asiantuntijat) - Kykenee käyttämään tekniikkaa (annetut resurssit)
Teinit		- Täytyy murtautua (sosiaalinen paine) - Kykenee käyttämään murto-ohjelmia (ohjelmien saatavuus)

Taulukko 5.5. Ei-teknisten toimijoiden modaalisuuden lajit

Käyttäjä näyttäytyy melko avuttomana toimijana tarinoissa. Toiminnan motivaation lähde on ulkopuolella, sillä tietoturva-asiantuntijoiden kehotusten myötä käyttäjän täytyy kehittää tietoturvallisuutta (taulukko 5.5). Käyttäjän onnistuminen riippuu siitä, miten hänelle on suotu resursseja, esimerkiksi yrityksessä työntekijän käytettävissä olevat tekniset sovellukset. Kun maallikko estää hyötyohjelmaa toimimasta, auttaa haittaohjelmaa tai rikollista tietoturvan vastaisessa toimissa, syynä nähdään maallikon tietämättömyys ja tyhmyys. Maallikko ei siis edes tiedä toimivansa tietoturvallisuuden estäjänä. Ei-tekninen toimija näyttää olevan kuin vetelä räsynukke, jota muut toimijat heittelevät miten haluavat.

Käyttäjän ongelmallisuus tulee esiin hyvin ilmaisuissa, joita tästä käytetään. Ensimmäiseksi ongelmaksi mainitaan tietämättömyys ja tyhmyys.

> ”Tietoturvallisuuden ehkä suurin ongelma on tänä päivänä, että käyttäjä on niin sanottu ei-tekninen henkilö.”
>
> Turvallisuus 1/03 s. 30

> ”Vielä vakavampaa on pahaa-aavistamattoman kotikäyttäjän koneen valjastaminen verkossa tehtäviä hyökkäyksiä ja tietomurtoja varten. (…) hyväuskoinen tietokoneen omistaja joutuu vähintäänkin kiusalliseen tilanteeseen.”
>
> Turvallisuus 2/03 s. 18

> ”Jos tekijä ajautuu agentiksi ymmärtämättömyyttään, jossakin vaiheessa hän ryhtyy ihmettelemään ’että mitä kumman outoa ympärilläni oikein tapahtuu.’”
>
> Turvallisuus 4/04 s. 12

> ”Kuvittelemme, että luottavaisin mielin, että sähköposti olisi yhtä turvallinen kuin vaikkapa kännykkäpuhelu tai tekstiviesti.”
>
> Turvallisuus 5/03 s. 18

Käyttäjän sanotaan olevan suurin ongelma sen takia, ettei hän ole tekninen henkilö. Se, että käyttäjä ei tunne läpikotaisin ohjelmistojen ja järjestelmien toimintaa ja jargonia, koetaan siis suurimmaksi pulmaksi. Eikö tätä voisi ajatella niin päin, että teknisten ratkaisujen toimintaa ja käytettyä kieltä tulisi muuttaa käyttäjäystävällisemmäksi? Pahaa-aavistamaton ja hyväuskoinen maallikko luottaa tietokoneensa turvallisuuteen eikä osaa odottaa sen kaappausta. Jos kone kaapataan, miksi käyttäjä joutuu kiusalliseen tilanteeseen? Eihän käyttäjä edes tiedä, että kone on kaapattu. Jos auto varastetaan ja

sitä käytetään pankkiryöstössä, autonomistaja ei joudu samalla tavalla kiusalliseen tilanteeseen. Jos omistaja ei tiedä autovarkaudesta esimerkiksi matkoilla olon takia, ei häntä syyllistetä. Tuntuu kuin maallikko nähtäisiin täysin negatiivisena, kaikki positiiviset ominaisuudet on käännetty heikkouksiksi. Tietämättömyys, ymmärtämättömyys ja luottavaisuus ovat nousseet suuriksi tietoturvallisuuden riskeiksi.

Lisäksi maallikon heikkoutena tuodaan esiin asenne.

> ”Kantona kaskessa ovat käyttäjät, joiden mielestä on hauska klikkailla kavereitten lähettämiä hupiohjelmia ja tiedostoliitteitä.”
> Turvallisuus 5/03 s. 20

> ”Yksikään turvaohjelma ei pysty suojelemaan käyttäjää kaikilta vaaroilta, jos tämä itse toimii ohjeista piittaamatta.”
> Turvallisuus 3/04 s. 14

Käyttäjä vaarantaa siis tietoturvallisuuden avaamalla kavereiltaan tulleita hauskoja viestejä ja niiden liitteitä. Neuvo, joka kehottaa suhtautumaan epäluuloisesti vierailta tuleviin sähköposteihin on järkevä, mutta jos tutuilta tulleita posteja ei suositella avaamaan, herää kysymys, mitä varten sähköposti on olemassa? Pitäisikö aina ennen viestin lähettämistä soittaa vastaanottajalle, että lähetän viestin ja se on tarkistettu virusten varalta. Käyttäjiä neuvotaan innokkaasti monenlaisilla sääntö- ja kieltolistoilla, mutta vaarana on, että liiallinen valistaminen turruttaa ja saa viittaamaan kintaalla kaikille ohjeille.

Maallikon syyllistäminen näkyy monin muodoin tarinoissa. Tietoturvallisuusasiat pitäisi tuntea.

> ”Siksi yleisten virusmerkkien tunnistaminen on osa 2000-luvun kansalaistaitoa, jota tämän päivän maailmassa edellytetään kaikilta työelämässä toimivilta.”
> Turvallisuus 3/04 s. 14

> ”Vaarallisia (yrityssalaisuuksien vuotamisessa KI) ovat eritoten entiset työkaverit, jotka ovat vaihtaneet kilpailijan palvelukseen, sillä ystävyyssuhteet eivät noudata organisaatiorajoja.”
> Turvallisuus 1/04 s. 16

Maallikolta edellytetään virusten tunnistamista, jotta tämä olisi kelvokas kansalainen. On tietysti vakuuttavampaa vedota pelkän henkilökohtaisen turvallisuuden lisäksi

kansalliseen turvallisuuteen ja velvollisuuden tuntoon. Aika rajulta tuntuu vihjaus, että ystävyyssuhteet voisivat vaarantaa yrityssalaisuudet. Ystävyys ei yleensä pääty samalla kuin työsopimus eikä pitäisikään. Todellinen ystävyys rakentuu muiden tekijöiden kuin hyväksikäytön varaan ja puheenaiheet koskevat useimmiten muuta kuin yrityssalaisuuksia, joten mielestäni tämä ei ole kovin tähdellinen riskitekijä tietoturvallisuudessa.

Kun ensin maallikon ymmärrys, asenne ja useimmat inhimilliset ominaisuudet on kyseenalaistettu, niin tuntuu paradoksaaliselta kieltää maallikon mahdollisuudet vaikuttaa tietoturvaongelmiin.

> ”Vain lainsäädäntö yhdistettynä teknisiin estoihin ja käyttäjien kouluttamiseen voi hillitä aikamme pahinta verkkosairautta (roskapostia KI).”
>
> Turvallisuus 1/04 s. 16

> ”Ihminen on ja pysyy tietoturvan heikkona lenkkinä. Siksi virusten kirjoittajat tulevat jatkossakin hyödyntämänä inhimillisiä heikkouksia.”
>
> Turvallisuus 3/04 s. 14

Vain valtiovalta ja tekniikka pystyvät taltuttamaan roskapostin. Käyttäjien toimintaa voi kehittää vain kouluttamisella eikä käyttäjällä itsellään ole juurikaan mahdollisuutta oma-aloitteiseen itsensä kehittämiseen. Toisaalta mitä turhaan kouluttaa käyttäjää, jos tämä kuitenkin pysyy tietoturvallisuuden heikoimpana lenkkinä.

Käyttäjä tuodaan esiin myös uhrina.

> ”Kun uhri avaa liitteen napsauttamalla kahdesti sen kuvaketta, virus aktivoituu.”
>
> Turvallisuus 5/03 s. 20

Kun käyttäjä esitetään uhrina, ensiksi se vaikuttaa jonkinlaisena empatian osoituksena. Mutta itse asiassa kyse on enemmänkin vallan käytöstä. Uhri kaipaa apua, koska on jäänyt alakynteen. Tarvetta neuvoa uhria ei tarvitse perustella. William Ryan huomauttaa, että omien uskomusten ja näkemysten vahvistamiseksi saatetaan käyttää uhrin syyllistämistä. Uhrin syyllistäminen voi olla tiedostamatonta. Se perustuu käsitykseen, jonka mukaan jollakin on vähemmän, koska tämä ansaitsee vähemmän. (Batson, Ahmad & Stocks 2004, 365.) Useimmiten syyllistäjä on hyvässä asemassa uhriin nähden, esimerkiksi asiantuntijalla on selkeästi enemmän tarvittavaa

kompetenssia tietoturvallisuudesta kuin maallikolla. Syyttämällä uhria sosiaalisesta epäoikeudenmukaisuudesta syyllistäjä pystyy selittämään itselleen hyväksyttävästi oman suhteellisen ylivoimansa uhriin nähden ja samalla näkemään maailman oikeudenmukaisena. (Batson ym. 2004, 365.)

Kuvaillessani maallikon asemaa esiin on usein noussut asiantuntija. Polaarinen jako maallikon ja asiantuntijan välillä onkin tyypillistä juuri riskikeskustelulle. Politiikan näkökulmasta tarkasteltuna maallikkous assosioituu päätöksentekoon, altistujien ja päättäjien kahtiajakoon. Asiantuntijoita on luonnollisesti vähemmän kuin maallikoita, mutta tämä ei suoraan viittaa harvainvaltaan. Keskusteleva yhteistyö erilaisten asiantuntijoiden välillä on vaihtoehto maallikoiden yläpuolella valtaa käyttävän asiantuntijajärjestelmän tilalle. Joka tapauksessa riskin käsite nivoutuu koulutukseen perustuvaan asiantuntijuuteen. Riskikeskustelulle onkin tyypillistä tieteellisten käsitteiden suosiminen parempina. Maallikoiden näkemyksiä pidetään alkukantaisina sekä vinoutuneina ja poikkeamat asiantuntijoiden näkemyksistä ovat lähinnä väärinkäsityksiä. Sitä, muodostuvatko maallikoiden käsitykset eri uskomuksista ja pyrkivätkö he eri tavoitteisiin kuin asiantuntijat, ei ole nähty tarpeelliseksi pohtia. Asiantuntijoiden toiminta ymmärretään faktojen pohjalta tapahtuvana järkeviin tavoitteisiin pyrkimisenä. Se sijaan maallikkojen käyttäytyminen nähdään suuntautuvan väärin olosuhteista johtuen. Päätöstentekijöiden ja heitä avustavien asiantuntijoiden tehtävänä nähdään sosiaalisten järjestelmien ohjaaminen tunnettujen säännönmukaisuuksien mukaan. Tässä maallikon eli toimijan omien näkemysten ymmärtämistä ei ole nähty tarpeelliseksi. (Jokinen ym. 2001, 173-174.)

Vertailtaessa maallikoiden ja asiantuntijoiden tiedon prosessointia kiinnitetään huomio maallikon vähemmän eriytyneeseen tapaan kuvata ja käsittää todellisuutta. Asiantuntijat kykenevät yhdistämään ilmiöt maallikkoja paremmin teoriaan ja tunnistamaan käyttökelpoisen tiedon rajat. (Jokinen ym. 2001, 175.) Joidenkin mukaan maallikot pelkäävät mahdollisuuksia, joiden toteutuminen on epätodennäköistä tai tuntematonta. Maallikoiden nähdään olevan ties minkä hysterian uhrina. Kuitenkin varovaisuusperiaatteen mukaan konservatiivisuus on viisasta tietämättömyyden vallitessa. Jos toiminnan seurauksen otaksutaan olevan kohtalokas, on järkevää olla toimimatta. (Jokinen ym. 2001, 178-179.)

Asiantuntemuksen hajaantuminen kaipaa keskustelua. Vaikka maallikko jää teknisen riskikeskustelun ulkopuolelle, hänen mielipiteensä on tärkeä teknologisten riskien arvioinnissa. Ensinnäkin maallikon näkökulma empiirisenä tosiasiana on osa sitä toimintaympäristöä, jossa päätökset tehdään. Asemansa säilyttämisen lisäksi päättäjät joutuvat ottamaan huomioon kansalaiset useiden riskeihin vaikuttavien päätösten tekijöinä. Näiden mielipidettä ei siis voi syrjäyttää vedoten taloudellisiin syihin. Toiseksi maallikoiden näkökulmat pitävät sisällään perusteltuja kannanottoja normatiivisina ohjeina, joita eettisesti järkevä päätöksenteko ei voi ohittaa. Esimerkiksi riskin hyväksyttävyyteen vaikuttaa haittojen ja hyötyjen jakautuminen. (Jokinen ym. 2001, 176.)

Teinien tietoturvallisuudelle vahingollinen toiminta selitetään ikään kuuluvana kapinointina eikä sitä pidetä tietoisena rikollisuutena. Tätä oikeastaan vähätellään.

> ”Kun teinipoika nyt purkaa turhautumistaan kirjoittamalla viruksen, sen kohteena ovat ehkä kotikoneet.”
>
> Turvallisuus 3/04 s. 12

Teinit eivät tarkoita pahaa eivätkä ymmärrä tekojensa seurauksia. Myös modaalisuuden lajien tarkastelu viittaa samaan taulukossa 5.5. Sosiaalinen paine pakottaa teinit murtautumaan tietojärjestelmiin. Onnistuminenkin on kiinni siitä, minkälaisia murto-ohjelmia Internetissä on tarjolla.

Vaikka sekä käyttäjä että järjestelmään murtautuva teini kuvataan olevan täysin riippuvaisia ulkopuolisista tekijöistä, niihin suhtaudutaan eri tavalla. Teini, joka tekee rikoksen, saa hyssyttelyä ja pääsee kuin koira veräjästä. Käyttäjä, joka haluaisi edistää tietoturvallisuutta, nähdään silkkana ongelmana. Maallikko julistetaan tietoturvallisuuden pahimmaksi uhaksi, vaikka häntä varten tietoturvallisuutta pitäisi rakentaa. Maallikoiden, niin kotikäyttäjien kuin työntekijöiden, ansiosta tietokoneista ja Internetistä on tullut menestys ja palvelut kannattavat. Käyttäjäkin haluaa, että hän voisi käyttää tietokonettaan turvallisesti. Ei maailma ole täynnä masokisteja.

6 Lopuksi

Olen pyrkinyt työssäni valottamaan tietoturvallisuutta kulttuurisena ilmiönä sekä kuvaamaan siinä esiintyvät toimijat. A. J. Greimasin aktanttimallin avulla olen hahmottanut nuo toimijat ja ne narratiiviset rakenteet, joiden kulisseissa toimijat nähdään. Viisi esimerkkitarinaa toi esiin toimijat erilaisine tavoitteineen tietoturvallisuuden näyttämöllä. Sen lisäksi, että pohdin toimijoita osana kertomuksia, tarkastelin niitä osana riskiyhteiskuntaa ja tietoturvallisuutta. Tämä syvempi havainnointi selvensi eri toimijoiden suhteita toisiinsa ja sitä, miten toimijat käsitteellistetään.

Tarinoissa subjektit tavoittelevat erilaisia päämääriä tietoturvallisuuteen liittyen. Organisaatio käyttää yhteistyötä parantaakseen tietoturvallisuuttaan ja sitä kautta turvatakseen menestyksensä markkinoilla. Organisaatio on erillinen toimija muihin toimijoihin nähden eikä se kohtaa muita toimijoita tarinoissa ollenkaan. Hyötyohjelma pyrkii torjumaan kaikki tietoturvahyökkäykset, koska se on tehty sitä varten. Sen toiminta on melko passiivista hyökkäyksiin vastaamista eikä sisällä lainkaan ennakointia. Sitä auttaa asiantuntijat ja hidastavat maallikot. Haittaohjelma taas pyrkii leviämään nopeasti mahdollisimman moneen tietojärjestelmään. Haittaohjelmaa estää tekniset ratkaisut kuten hyötyohjelma. Auttajana esiintyy maallikko. Hyvä ihminen eli asiantuntija tai työntekijä pyrkii kehittämään aktiivisesti tietoturvallisuutta, jotta työpaikka olisi turvattu. Asiantuntija on etevä tietoturvallisuuden guru, joka osaa johdattaa muita parempaan tietoturvallisuuteen, jos saa vain mahdollisuuden. Työntekijä taas kaipaa tarkkaa ohjeistusta, jotta osaisi toimia oikein. Tekniikka edistää subjekteja tietoturvallisuuden kehittämisessä ja vasta-subjektina esiintyy asiantuntija, esimerkiksi krakkeri. Viimeisessä tarinassa paha ihminen rikkoo lakia saavuttaakseen jotain hyötyä. Useimmiten nettirikollisen syynä on taloudellisen hyödyn tavoittelu. Osan toimintaa ohjaa aate, ja teinit haluavat mainetta kavereitten keskuudessa. Maallikko auttaa pahaa ihmistä useimmiten tietämättään ja rikoksen uhri pyrkii estämään rikollista objektin saavuttamisessa.

Teknisiä toimijoita tarinoissa ovat hyöty- ja haittaohjelmat. Hierarkisesti ajateltuna haittaohjelma on hyötyohjelmaa korkeammalla, sillä haittaohjelma ohjaa hyötyohjelman kehittymistä. Päästyään leviämisen makuun haittaohjelma muuttuu itsenäiseksi

toimijaksi, johon ihminen ei voi vaikuttaa. Tekniset toimijat ovat vuorovaikutuksessa ihmisten kanssa ja niillä on vaikutuksia toisiinsa, kuten toimijaverkostoteoriassa korostetaan. Tekniset toimijat kuvataan teknologisen determinismin näkökulmasta. Tekniikan kehityksen ohjaamiselle ei nähdä keinoja, vaan tekniikkaan voi vastata vain tekniikalla. Riskiyhteiskunnan kannalta on paradoksaalista, että riskejä pyritään hallitsemaan tekniikalla ja samalla nuo tekniikat luovat uusia riskejä, ja uusia riskejä varten kehitetään uutta tekniikka. Näin noidankehä on valmis. Miksi teknologian kehitys nähdään yksisuuntaisena prosessina? Teknologian tuottaminen on osa yhteiskuntaa, joten yhteiskunnalla ja sen jäsenillä on vaikutusvaltaa sen kehittymiseen. Vaikka jo vuosia on puhuttu, että teknologian pitäisi olla käyttäjälähtöistä, se ei sitä vieläkään ole. Miksi asiantuntijakulttuurissa yhä tuotetaan teknologiaa teknispainotteisesti?

Asiantuntijalla on merkittävä rooli riskiyhteiskunnassa ja niin myös näissä tarinoissa. Asiantuntijuutta tarvitaan yhä enemmän riskien hallinnassa, mutta samalla riskien monimutkaistuessa asiantuntijoiden työ vaikeutuu. Asiantuntijat joutuvat todistamaan pätevyyttään toistuvasti, ja odotukset kovenevat jatkuvasti. Kenties asiantuntijat voisivat ottaa oppia hakkerietiikan korostamasta avoimuudesta ja innosta. Jaettu tietämys ja intohimoinen suhtautuminen työhön saattaisi olla toimiva ratkaisu. Yllä esitellyillä tarinoilla on tietoturvallisuuden lisäksi toinen yhteinen tekijä: ne ovat asiantuntijoiden dialogin tulosta. Asiantuntijat ovat määrittäneet asemansa suhteessa toisiin toimijoihin ja vahvistaneet eksistenssinsä oikeutusta. Tässä valossa on ymmärrettävää, miksi asiantuntijat ilmenevät niin tärkeässä asemassa.

Asiantuntijoiden keskinäisessä keskustelussa ei näytä olevan tilaa itsekritiikille. Ongelmat siirretään muiden syyksi eikä asiantuntijat ota niistä vastuuta. Mikä asiantuntijakulttuurissa estää myöntämästä omia puutteitaan? Myös asiantuntijat näkevät teknologian kehittymisen varsin yksisuuntaisena, mihin ihminen ei voi vaikuttaa. Asiantuntijat voivat vain neuvoa maallikoita sopeutumaan teknologisiin muutoksiin. Tietoturvallisuusasiantuntijat ovat yleensä saaneet teknisen koulutuksen ja ovat keskittyneet työssään tekniikkaan, joten sinänsä ei ole ihme, että tietoturvallisuuteenkin suhtaudutaan tekniikkalähtöisesti. Asiantuntijoilta tarvitaan aloja ylittävää ymmärrystä, jotta tietoturvallisuus ilmiönä hahmottuisi kokonaisvaltaisemmin. Käyttäjät ja yhteiskunta vaikuttavat tietoturvallisuuteen ja ne pitäisikin huomioida

paremmin vastaisuudessa. Kenties asiantuntijoiden kannattaisi nähdä tietoturvariskit Kristevan mainitsemina abjekteina. Kohteen tulkinnassa huomioidaan paikallisuuden ja vuorovaikutuksen merkitys sekä siitä neuvotellaan muiden toimijoiden kanssa. Tehtävä on haasteellinen, sillä asiantuntijat eivät voi enää tukeutua pelkästään oman tietämyksensä varaan.

Rikolliset asiantuntijat edustavat itsenäistä alamaailmaa. Heihin ei juurikaan voi vaikuttaa, ainoastaan rikollisen uhri voi pyrkiä suojautumaan paremmin. Rikollisista puhutaan vähän ja se ylläpitää heistä mystistä ja myyttistä käsitystä. Jos rikolliset henkilöitäisiin, se rikkoisi manikealaisen illuusion. Hyvä ja paha ei enää vastakohtina pystyisikään erottelemaan meitä hyviä toisista pahoista rikollisista. Vaikka rikolliset symboloivat sitä negatiivista ja pahaa toista, he eivät näyttäydy tietoturvallisuuden pahimpana uhkana asiantuntijoille. Tietoturvallisuuden murheenkryyni kun on maallikko.

Maallikko, käyttäjä ja ei-tekninen henkilö ovat eri nimityksiä samalle toimijalle, jota kutsutaan myös tietoturvallisuuden heikoimmaksi lenkiksi. Käyttäjän heikkouksina mainitaan muun muassa tietämättömyys ja kovapäisyys. Tietoturvallisuuden kenttä muuttuu jatkuvasti uusien ongelmien ja teknisten sovellusten myötä. Asiantuntijoillekin kehityksen mukana pysyminen on haasteellista, joten maallikolle se on lähes mahdotonta. Miksi käyttäjän pitää tietää niin paljon tietoturvallisuudesta? Tietokone on työkalu käyttäjälle eikä muidenkaan työkalujen toimintaa tarvitse tuntea tarkkaan, kunhan sitä osaa käyttää. Maallikkoa soimataan myös väärästä asenteesta, koska maallikko ei piittaa säännöistä. Tietoturvallisuutta koskevia sääntöjä on todella paljon ja niitä tuputetaan joka käänteessä. Osa näistä säännöistä ei toimi käytännössä ja niiden täydellinen noudattaminen tekisi lähinnä paranoidiksi. Käyttäjän syyllistämiseltä syö pohjaa se, että tämä nähdään muuttumattomana. Jos ihminen on ja pysyy tietoturvallisuuden heikoimpana lenkkinä, mitä hyötyä syyllistämisestä on?

Vaikka olen työssäni jättänyt tekniikan tarkastelun minimiin, se ei tarkoita, että pitäisin sitä jotenkin turhana. Tekniikka on tärkeä osa tietoturvallisuutta, mutta sitä on käsitelty muissa yhteyksissä runsaasti. Sosiologina näen, että tietoturvallisuus kokonaisena ilmiönä on hedelmällisempi tutkimuskohde ja lisäksi melko tutkimatonta maaperää. Asiantuntijoiden asema on päässyt työssäni tehotarkkailuun. Tarkoitukseni ei ole ollut

väheksyä asiantuntijuuden merkitystä, vaan kyseenalaistaa sen ylivaltaa. Asiantuntijoiden olisi hyvä välillä pysähtyä miettimään omaa asiantuntijakulttuuriaan ja sen kehittymistä. Voisiko tekniikkaa luoda teknologisen voluntarismin viitoittamalla tiellä yhteistoiminnan kautta vai onko se vain optimistista utopiaa?

Tietoturvallisuuden suurimmat uhat ovat viime vuosina muuttuneet viruksista phishingiin. Kiusanteko on vaihtunut ammattirikollisten järjestäytyneeseen toimintaan. Ihan uusimpana uhkana siintää *pharming*. Tällöin selaimen osoitekenttään kirjoitettu osoite ei viekään oikeille sivuille, vaan identtisennäköisille huijarisivuille. Esimerkiksi tutun verkkokaupan osoite onkin käännetty huijarisivuille dns- eli verkkotunnuspalvelinta sorkkimalla eikä käyttäjä voi mistään aavistaa ettei luottokortin numeroa kannata antaa. Uusien haastavampien uhkien rantautuessa syyllistäminen ei vie pitkälle. Tietoturvallisuuden tavoitteena on estää uhkia aiheuttamasta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille. Jotta tämä tavoite toteutuisi, on asiantuntijan ja maallikon opittava ymmärtämään toisiaan.

Lähteet

Ahponen, Pirkkoliisa (1997) Elämän riskiytyminen epävarmuuden yhteiskunnassa. Teoksessa Pirkkoliisa Ahponen (toim.) Riskikirja: uhat, mahdollisuudet ja asiantuntijuus epävarmuuden yhteiskunnassa. Jyväskylän yliopisto, 21-37.

Batson, C. Daniel & Ahmad, Nadia & Stocks, E. L. (2004) Benefits and Liabilities of Empathy-Induced Altruism. Teoksessa Arthur G. Miller (toim.) The Social Psychology of Good and Evil. Guilford Press, New York, 359-385.

Baumeister, Roy F. & Vohs, Kathleen D. (2004) Four Roots of Evil. Teoksessa Arthur G. Miller (toim.) The Social Psychology of Good and Evil. Guilford Press, New York, 85-101.

Beck, Ulrich (1990) Riskiyhteiskunnan vastamyrkyt. Suomentanut Heikki Lempa. Vastapaino, Tampere. Saksankielinen alkuteos 1988.

Beck, Ulrich & Giddens, Anthony & Lash, Scott (1995) Nykyajan jäljillä: refleksiivinen modernisaatio. Suomentanut Leevi Lehto. Vastapaino, Tampere. Englanninkielinen alkuteos 1994.

Greimas, Algirdas Julien (1980) Strukturaalista semantiikkaa. Suomentanut Eero Tarasti. Gaudeamus, Helsinki. Ranskankielinen alkuteos 1966.

Harle, Vilho (1991) Hyvä, paha, ystävä, vihollinen. Rauhan- ja konfliktintutkimuslaitoksen tutkimuksia nro 44. Rauhankirjallisuuden edistämisseura, Helsinki.

Himanen, Pekka & Torvalds, Linus & Castells, Manuel (2001) Hakkerietiikka ja informaatioajan henki. Suomentanut Pekka Himanen. WSOY, Helsinki. Englanninkielinen alkuteos 2001.

Jokinen, Pekka & Kamppinen, Matti & Raivola, Petri (2001) Riskit yhteiskunnassa ja kulttuurissa. Teoksessa Matti Kamppinen, Petri Raivola, Pekka Jokinen & Hasse Karlsson Riskit yhteiskunnassa: maallikot ja asiantuntijat päätösten tekijöinä. Gaudeamus, Helsinki, 126-180.

Konttinen, Esa (1997) Professionaalinen asiantuntijatyö ja sen haasteet myöhäismodernissa. Teoksessa Juhani Kirjonen & Pirkko Remes & Anneli Eteläpelto (toim.) Muuttuva asiantuntijuus. Koulutuksen tutkimuslaitos, Jyväskylän yliopisto, 48-61.

Korhonen, Inkeri & Oksanen, Katja (1997) Kertomuksen semiotiikkaa. Teoksessa Pekka Sulkunen & Jukka Törrönen (toim.) Semioottisen sosiologian näkökulmia. Sosiaalisen todellisuuden rakentuminen ja ymmärrettävyys. Gaudeamus, Helsinki, 54-71.

Kotilainen, Lauri (2005) Opiskelijat testataan, vaan mistä johtajat tulevat? Turvallisuus 21:2, 5.

Lagerspetz, Eerik (1997) Epävarmuuden aika. Teoksessa Pirkkoliisa Ahponen (toim.) Riskikirja: uhat, mahdollisuudet ja asiantuntijuus epävarmuuden yhteiskunnassa. Jyväskylän yliopisto, 91-105.

Latour, Bruno (1991) Technology is Society Made Durable. Teoksessa John Law (toim.) A Sociology of Monsters. Essays on Power, Technology and Domination. Routledge, London, 103-131.

Leskinen, Jaakko (2000) Michel Callon ja sosiologian materialisointi. Teoksessa Tarmo Lemola (toim.) Näkökulmia teknologiaan. Gaudeamus, Helsinki, 176-192.

Miettinen, Reijo (1998) Materiaalinen ja sosiaalinen: toimijaverkkoteoria ja toiminnan teoria innovaatioiden tutkimuksessa. Sosiologia 35:1, 28-42.

Niiniluoto, Ilkka (2000) Tekniikan filosofia. Teoksessa Tarmo Lemola (toim.) Näkökulmia teknologiaan. Gaudeamus, Helsinki, 16-35.

Pantzar, Mika (1996) Kuinka teknologia kesytetään. Kulutuksen tieteestä kulutuksen taiteeseen. Hanki ja jää. Tammi, Helsinki.

Peltomäki, Päivi & Harjumäki, Piia & Husman, Kaj (2002) Muuttuva auttamistyön asiantuntijuus – kriisityön ja työterveyshuoltotoiminnan tarkastelua. Teoksessa Ilkka Pirttilä & Susan Eriksson (toim.) Asiantuntijoiden areenat. SoPhi, Jyväskylän yliopisto, 81-103.

Pirttilä, Ilkka (1997) Teoria, markkina-analyysi ja futurologinen silmä eksperttiyden ehtona. Teoksessa Juhani Kirjonen & Pirkko Remes & Anneli Eteläpelto (toim.) Muuttuva asiantuntijuus. Koulutuksen tutkimuslaitos, Jyväskylän yliopisto, 73-82.

Ruohonen, Mika (2002) Tietoturva. Docendo Finland Oy, Jyväskylä.

Sulkunen, Pekka (1997) Todellisuuden ymmärrettävyys ja diskurssianalyysin rajat. Teoksessa Pekka Sulkunen & Jukka Törrönen (toim.) Semioottisen sosiologian näkökulmia. Sosiaalisen todellisuuden rakentuminen ja ymmärrettävyys. Gaudeamus, Helsinki, 13-53.

Sulkunen, Pekka (1999) Johdatus sosiologiaan –käsitteitä ja näkökulmia. WSOY, Porvoo.

Sulkunen, Pekka & Törrönen, Jukka (1997a) Arvot ja modaalisuus sosiaalisen todellisuuden rakentamisessa. Teoksessa Pekka Sulkunen & Jukka Törrönen (toim.) Semioottisen sosiologian näkökulmia. Sosiaalisen todellisuuden rakentuminen ja ymmärrettävyys. Gaudeamus, Helsinki, 72-95.

Sulkunen, Pekka & Törrönen, Jukka (1997b) Puhujakuva: enonsiaation rakenteet. Teoksessa Pekka Sulkunen & Jukka Törrönen (toim.) Semioottisen sosiologian näkökulmia. Sosiaalisen todellisuuden rakentuminen ja ymmärrettävyys. Gaudeamus, Helsinki, 96-126.

Tiainen, Tarja (2002) Piilotettu maskuliinisuus atk-asiantuntijuudessa. Teoksessa Ilkka Pirttilä & Susan Eriksson (toim.) Asiantuntijoiden areenat. SoPhi, Jyväskylän yliopisto, 119-136.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI (2003) Valtion Tietohallinnon Internet-tietoturvallisuusohje 1/2003. Valtiovarainministeriö, Helsinki.

Van Loon, Joost (2000) Virtual Risks in an Age of Cybernetic Reproduction. Teoksessa Barbara Adam & Ulrich Beck & Joost Van Loon (toim.) The Risk Society and Beyond: Critical Issues for Social Theory. London, Sage, 165-182.

Veivo, Harri & Huttunen, Tomi (1999) Semiotiikka. Merkeistä mieleen ja kulttuuriin. Edita, Helsinki.

Liitteet

Liite 1: Aineistona käytetyt Turvallisuus-lehden artikkelit

Turvallisuus 19:1, 30-32: Kihl, Merja (2003) Palomuuri - virustentorjuntaohjelma ratkaisee monta pulmaa. Hyödynnä hankinnassa puolueetonta testilaitosta.

Turvallisuus 19:2, 14-16: Könönen, Ilari (2003) Verkkosota ulottuu myös Suomeen. Internetistä tulee taistelutanner.

Turvallisuus 19:2, 18-19: Könönen, Ilari (2003) Suojaamattomat tietokoneet yhteiskunnalle kuin ladattu ase.

Turvallisuus 19:2, 20-21: Sipilä, Marja (2003) Turva-alan yritykset tarjoavat tietoturvaa.

Turvallisuus 19:3, 21-22: Kotilainen, Lauri (2003) Tietokoneet kiertoon ehjinä – ilman tietoturvariskiä. Suomalaisohjelma on tiedostojen täystuho.

Turvallisuus 19:3, 24-25: Mäki, Erkki (2003) Tietoturvarikokset voidaan todistaa tietohakujen avulla.

Turvallisuus 19:4, 12-14: Kotilainen, Lauri (2003) Näin rakennan oikein yrityksen tietoturvan.

Turvallisuus 19:4, 16-17: Oraskari, Jyrki (2003) Langattomat tietoverkot alttiita luvattomalle kuuntelulle. Turvallisuutta voi parantaa pienin konstein.

Turvallisuus 19:4, 18-19: Koskivirta, Paula (2003) On rahan arvoista ymmärtää varoitukset ja hälytykset. Virusraportteja saa suomen kielellä.

Turvallisuus 19:5, 18-19: Järvinen, Petteri (2003) Petteri Järvisen järkevät tietoturvaohjeet: Näin salaat sähköpostiviestit sivullisilta.

Turvallisuus 19:5, 20-22: Järvinen, Petteri (2003) Mitä tehdä, jos virus ehtii iskeä? Mitä tehdä ennen sitä? Elokuun viruspainajainen näpäytti.

Turvallisuus 19:6, 12-13: Koskivirta, Paula (2003) Oliko Sobig.F:n tarkoitus kaataa Internet? Taistelu aikaa vastaan.

Turvallisuus 19:6, 14-16: Kotilainen, Lauri (2003) Tietoturvan kolmas aste Suomesta: Ehkäise tunkeutuminen.

Turvallisuus 20:1, 12-15: Koskivirta, Paula (2004) ”Pitää huolehtia, että parannukset toteutuvat myös käytännössä.” Näin johdat tietoturvaa oikein.

Turvallisuus 20:1, 16-17: Järvinen, Petteri (2004) Jo puolet liikenteestä on roskaa! Näin suojaudun roskapostilta.

Turvallisuus 20:2, 16-17: Koskivirta, Paula (2004) Ulkoistaminen – tietoturvallisuuden hoidon hyvä apu. Maatiaisjärkeä, paljon muistettavaa ja kovaa työtä.

Turvallisuus 20:2, 18-19: Kotilainen, Lauri (2004) Mikä tietoturvassa maksaa? Miten sen kustannuksissa voisi säästää?

Turvallisuus 20:2, 20-21: Koskivirta, Paula (2004) ”Toistasataatuhatta järjestelmää toimii itsekseen.” Turvajärjestelmän palvelin voi olla tietoturvariski.

Turvallisuus 20:2, 22-23: Kotilainen, Lauri (2004) Älykäs roskapostisuodatin nappaa viruksetkin.

Turvallisuus 20:3, 12-13: Kotilainen, Lauri (2004) Pankit, rautatiet, lentoyhtiöt, ydinvoimalat… Virukset vaarantavat jo kriittiset palvelut.

Turvallisuus 20:3, 14-16: Järvinen, Petteri (2004) Erota sähköpostin virusviesti hyötyviestistä. Näin tunnistat tietokoneviruksen.

Turvallisuus 20:4, 12-14: Koskivirta, Paula (2004) ”Mun ympärillä tapahtuu outoa…” Aukot yritysturvallisuudessa tekevät vakoilusta jopa helppoa.

Turvallisuus 20:4, 15-17: Koskivirta, Paula (2004) Mistä sivuillemme ilmestyi Che Guevaran kuva? ”Koska yritysten levytilan varastaminen on niin helppoa.”

Turvallisuus 20:4, 18-19: Kotilainen, Lauri (2004) Hätääntyneitä kansalaisia, häiriköitä, lobbareita, roskapostihyökkääjiä… Eduskunnan tietoturva on kovaa työtä

Turvallisuus 20:5, 14-16: Kihl, Merja (2004) Passi huippusalaisille maailman markkinoille on uusi laki kansainvälisistä tietoturvallisuusvelvoitteista.

Turvallisuus 20:5, 17-18: Kotilainen, Lauri (2004) Kun kone piippaa, toiminta hidastuu, palvelin kaatuilee, lokitiedot muuttuvat, operaattori ilmoittaa häiriöstä, outo käyttäjänimi ilmaantuu… Epäile tietomurtoa ja toimi jämptisti.

Turvallisuus 20:5, 20-21: Kotilainen, Lauri (2004) Verkkorikollisuus on nyt alamaailman liiketoimintaa. Internetin pimeä puoli.

Turvallisuus 20:6, 24-26: Porvari, Paavo (2004) Näin räätälöidään yritykselle toimiva tietoturvastrategia.

Turvallisuus 20:6, 26-27: Kyrölä, Tuija (2004) Tietoriskien hallinnan seitsemän sudenkuoppaa.