LAUREA AMMATTIKORKEAKOULU Uuden edellä

# Sosiaalisen median riskit ja tiedonhankinta

Bunda, Jari

2012 Leppävaara

**Laurea-ammattikorkeakoulu**
Leppävaara

# Sosiaalisen median riskit ja tiedonhankinta

Jari Bunda
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Lokakuu, 2012

Laurea-ammattikorkeakoulu
Laurea, Leppävaara
Turvallisuusalan koulutusohjelma

Tiivistelmä

Jari Bunda

**Sosiaalisen median riskit ja tiedonhankinta**

Vuosi 2012 Sivumäärä 72

Sosiaalinen media on muuttanut olennaisesti meidän tapaamme löytää, luoda ja jakaa tietoa. Se nähdään kanavana, joka mahdollistaa ihmisten välisen vuorovaikutuksen ja sisällön tuottamisen Internetissä tavalla jota ei ole ennen koettu. Samalla asiantuntijoilla on huoli sosiaalisen median vaikutuksista tietoturvallisuuteen.

Asiantuntijat varoittavat haittaohjelmista, jotka leviävät sosiaalisen median kautta sekä sosiaalisen median aiheuttamista riskeistä tiedon luottamuksellisuudelle.

Tämän opinnäytetyön tarkoituksena on tutkia sosiaalisen median käyttöön liittyviä riskejä ja sitä kuinka sosiaalista mediaa voidaan käyttää hyväksi tiedonhankintaan.

Opinnäytetyö vastaa kahteen kysymykseen:

- Onko sosiaalisen median riskien taustalla yhdistäviä tekijöitä, jotka edesauttavat sosiaalisen median kautta tapahtuvaa tiedonhankintaa?
- Miten sosiaalista mediaa voidaan käyttää hyväksi tiedonhankinnassa?

Ensimmäistä kysymystä lähestytään tutkimalla sosiaalisen media riskejä neutraloimisteorian ja neutraloimistekniikoiden avulla. Tavoitteena on löytää riskien taustalta sellaisia yhdistäviä tekijöitä jotka vastaisivat esitettyyn tutkimuskysymykseen.

Vastausta toiseen kysymykseen haetaan tutkimalla käytännössä, kuinka tietoa voidaan hakea sosiaalisen median kautta. Tutkimuskohteena on kaksi suosittua sosiaalisen median palveluntarjoajaa: Facebook ja Twitter.

Opinnäytetyö osoittaa, että sosiaalisen median riskien taustalta on kolme yhteistä tekijää, jotka mahdollistavat sosiaalisen median kautta tapahtuvan tiedonhankinnan. Nämä tekijät ovat: sosiaalisuuden tarve, luottamuksen ilmapiiri ja ”Minulla ei ole mitään salattavaa.”

Toiseen kysymykseen vastataan näyttämällä käytännössä miten tietoa voidaan hakea Facebookista ja Twitteristä käyttämällä heidän omia kehitystyökaluja.

Sosiaalinen media, tiedonhankinta, riskit, Facebook, Twitter

**Laurea University of Applied Sciences** **Abstract**
Laurea, Leppävaara
Bachelor's Degree Programme in Security Management

Jari Bunda

**Social Media Risks and Information Gathering**

Year 2012 Pages 72

Social Media has become an integral part of our life. It has changed the way we find, create and share information. Social Media can be seen as a channel that allows interaction and content creation never seen before.

At the same time the impact of social media in information security has also increased. Information security experts are worried about malicious programs that spread through social media and people who disclose sensitive information about themselves and organizations they represent.

Purpose of this thesis is to conduct a research about social media risks and how social media is used as an information gathering platform. This thesis corresponds to the two research questions:

- Is there any common factor behind social media risks that makes possible to gather information through social media?
- How social media can be used for information gathering?

The first question is approached by analyzing social media risks using neutralization theory and techniques of neutralization. The objective is to discover unifying elements that would correspond to the question.

The answer to the second research question is applied in practice by investigating how information is gathered through social media. Two popular social media sites are used as a research object: Facebook and Twitter.

The conclusion of thesis is that there are three unifying elements behind social media risks. These elements are: need to socialize, relation of trust and "I've got nothing to hide" -mentality.

Additionally this thesis shows in practice how information can be gathered through Facebook and Twitter by using their development tools.

Social media, information gathering, risks, Facebook, Twitter

Sisällys

# 1 Johdanto

Sosiaalisen median suosio on kasvanut räjähdysmäisesti hyvin lyhyessä ajassa (Dwyer, Hiltz & Passerini 2007). Samalla se on muuttanut merkittävällä tavalla ihmisten tapaa käsitellä, tuottaa ja julkaista eri muodoissa olevaa tietoa (Gundecha, Barbier & Liu 2011). Sosiaalinen media nähdään uudenlaisena kanavana, joka mahdollistaa ihmisten välisen vuorovaikutuksen ja sisällön tuottamisen Internetissä tavalla, jota ei ole ennen nähty. Ihmisille on annettu täysin uudenlaiset työkalut tiedon jakamiseen ja tuottamiseen. (Isokangas & Vassinen 2010, 15–19.)

Toisenlaista näkökulmaa edustaa huoli riskeistä, joita sosiaalisen median käyttö aiheuttaa yrityksille sekä ihmisten yksityisyydelle. Tutkimukset ovat osoittaneet, että ihmiset julkaisevat sosiaalisessa mediassa tietoa, joka vaarantaa heidän yksityisyytensä sekä yritysten tietojen luottamuksellisuuden (Gross & Acquisti 2005; Acquisiti & Gross 2006; Tuunanen, Pitkänen & Hovi 2009; Molok, Chang & Ahmad 2010). Tietoturvallisuusasiantuntijat ovat huolissaan sosiaalisten verkostojen kautta leviävistä haittaohjelmista sekä yrityssalaisuuksien vuotamisesta (Cert.fi 2010). Pelko sosiaalisen median aiheuttamista riskeistä on johtanut siihen, että esimerkiksi Ernst & Youngin (2011) maailmanlaajuisessa tutkimuksessa 53 % yritysjohtajista ilmoitti kieltäneensä pääsyn sosiaalisen median palveluihin yrityksen tietoverkosta.

# 2 Opinnäytetyön tarkoitus, tavoitteet ja tutkimuskysymykset

Sosiaalisen mediaan liittyviä riskejä voidaan tarkastella kahdesta näkökulmasta: jos tarkastelukulmana on tietoturvallisuus, silloin sosiaalisen median riskejä arvioidaan sen perusteella miten ne vaikuttavat tiedon luottamuksellisuuteen, eheyteen ja käytettävyyteen (Vahti 4/2010). Jos tarkastelukulmana on organisaation maine ja vision toteuttaminen, riskejä arvioidaan sitä kautta, miten sosiaalinen media huomioidaan organisaation strategiassa, miten sosiaalisen mediaan suhtaudutaan ja miten sen käyttö suunnitellaan (Scott & Jacka 2011, 83-102).

Opinnäytetyön tarkastelukulma on tietoturva. Opinnäytetyön tarkoituksena on kartoittaa sosiaalisen median riskien taustalla olevia tekijöitä ja sitä, kuinka sosiaalista mediaa voidaan käyttää hyväksi tiedonhankintaan esimerkiksi kohdistettujen hyökkäysten valmisteluvaiheessa. Tutkimuksen lähestymistapa on laadullinen tutkimus ja tutkimusstrategiaksi valittiin toimintatutkimus. Työn tarkoitus voidaan kiteyttää kahteen pääkysymykseen:

1. Onko sosiaalisen median riskien taustalla yhdistäviä tekijöitä, jotka edesauttavat sosiaalisen median kautta tapahtuvaa tiedonhankintaa?
2. Miten sosiaalista mediaa voidaan käyttää hyväksi tiedonhankinnassa?

Kahden tutkimuskysymyksen esittämisen avulla selvennetään käsiteltävää aihetta ja muodostetaan kuva tarvittavasta aineistosta. Tutkimuskysymysten avulla estetään myös se, että tutkimus ei jää pelkästään aineiston luokittelun tasolle (Hirsijärvi, Remes, Sajavaara 2006, 116–117). Ensimmäistä tutkimuskysymystä lähestytään kartoittamalla sosiaalisen median riskejä neutraloimisteorian ja neutraloimistekniikoiden avulla. Tavoitteena on löytää riskien taustalta sellaisia yhdistäviä tekijöitä jotka vastaisivat esitettyyn tutkimuskysymykseen.

Käsitykseni mukaan tätä lähestymistapaa ei ole aikaisemmin juurikaan käytetty. Sosiaalisen median riskejä on tutkittu yksittäisen uhkan tai yksityisyyden suojan näkökulmasta (Gross & Acquisti 2005; Acquisiti & Gross 2006; Tuunanen ym. 2009; Molok ym. 2010), mutta niiden väliset mahdolliset yhdistävät tekijät ovat jääneet huomioimatta. Molok ym. (2011) ovat julkaisseet tutkimussuunnitelman jossa he käsittelevät sitä miksi ihmiset vuotavat tietoa sosiaalisessa mediassa ja kuinka organisaatiot voivat suojautua tietovuodoilta. Tutkimuksen julkaisuajankohdaksi on arvioitu lokakuu 2012 (Molok ym. 2011).

Toisessa tutkimuskysymyksessä tutkitaan Internetin hiljaista tietoa: miten sosiaalista mediaa voidaan käyttää tiedonhankintaan? Tutkimuskysymystä lähestytään käytännön esimerkkien avulla. Kahden pääkysymyksen lisäksi kolmantena kysymyksenä tässä opinnäytetyössä käsitellään sitä, miten organisaatiot voivat suojautua sosiaalisen median kautta tapahtuvalta tiedonhankinnalta.

## 2.1 Opinnäytetyön rajaaminen

Sosiaalisen median rooli esimerkiksi kohdistetuissa hyökkäyksissä voidaan jakaa kolmeen kokonaisuuteen. Sitä voidaan käyttää tiedusteluun, hyökkäysreittinä kohteeseen tai tiedonsiirtokanavana, jossa kaapattua tietoa siirretään hyökkääjälle (Moyer & Hamiel 2008; Alridge 2012; Gunter & Sonya 2012). Tässä opinnäytetyössä keskitytään ainoastaan ensimmäiseen vaiheeseen eli tiedonhankintaan.

Opinnäytetyötä rajataan edelleen niin, että tutkielmassa ei käsitellä lainsäädäntöön liittyviä kysymyksiä muutamaa oleellista viittausta lukuun ottamatta. Myös sosiaalisen median käsitettä rajataan siten, että tarkastelun kohteena on kaksi sosiaalisen median palveluntarjoajaa: Facebook ja Twitter. Valinta perustui näiden suosioon; kyseisillä palveluntarjoajilla on globaalisti yhteensä noin 1,5 miljardia käyttäjää (Dugan 2012; The Sociable 2012).

Lisäksi opinnäytetyötä rajataan edelleen siten, että työssä esiteltävät tiedonhankintamenetelmät eivät riko rikoslain säännöksiä tietomurrosta. Tämä tarkoittaa, että työssä keskitytään passiiviseen tiedonhankintaan. Passiivista tiedonhankintaa voi kuvailla lyhyesti sellaisen tiedon hakemiseksi, jonka voisi ruudulta muutenkin lukea.

## 2.2 Opinnäytetyön eteneminen ja tärkeimmät käsitteet

Opinnäytetyö etenee niin, että johdantokappaleen jälkeen kappaleissa kaksi ja kolme kerrotaan opinnäytteen tarkoitus ja tavoitteet, sekä tutkimuksellinen viitekehys. Kappaleessa neljä kuvataan Internetin kehitystä aina sosiaalisen mediaan asti. Kappaleessa viisi käsitellään verkkorikollisuutta ja sen kehittymistä. Kappaleiden neljä ja viisi tarkoituksena on kuvata sitä toimintaympäristöä, jota tämä työ käsittelee. Kappaleessa kuusi vastataan ensimmäiseen tutkimuskysymykseen. Kappaleessa seitsemän tutkitaan toista tutkimuskysymystä käytännön esimerkkien avulla. Kappaleessa kahdeksan käsitellään sitä, miten organisaatiot voivat suojautua sosiaalisen median kautta tapahtuvalta tiedonhankinnalta. Kappaleessa yhdeksän pohditaan työn onnistumista. Kappaleessa kymmenen on yhteenveto koko opinnäytetyöstä sekä annetaan suosituksia jatkotutkimusten aiheiksi.

Tämän työn kannalta keskeisimmät käsitteet ovat **sosiaalinen media**, **verkkorikollisuus**, **kohdistetut hyökkäykset**, **JSON** ja **tiedonhankinta**. Käsitteitä avataan tarkemmin työn edetessä.

**Sosiaalisella medialla** tarkoitetaan Internet-pohjaisia sovelluksia, jotka mahdollistavat käyttäjälähtöisen sisällön tuottamisen ja jakamisen (Kietzmann, Hermkens, McCarthy & Silvestre 2011).

**Verkkorikollisuudella** tarkoitetaan tässä työssä kaikkea verkossa tapahtuvaa laitonta toimintaa. Olipa taustalla sitten yksittäinen tekijä, rikollisjärjestö, aktivistiryhmä tai valtion tukema toimija.

**Kohdistetuilla hyökkäyksillä** tarkoitetaan tässä työssä tietyn kohteen digitaaliseen tietopääomaan ja immateriaalioikeuksiin kohdistuvaa tietojen anastusta, joka on hyvin suunniteltu, johdettu sekä organisoitu ja jossa tunkeudutaan kohteen tietojärjestelmiin käyttäen hyväksi sellaisia keinoja, joita on erittäin vaikea havaita tavanomaisin menetelmin.

**JSON** (JavaScript Object Notation) on yksinkertainen ja kevyt tiedonsiirtoprotokolla, jota on helppo käyttää JavaScript – ohjelmissa. Nimestään huolimatta kyseessä ohjelmointikielestä riippumaton protokolla, joka määrittelee periaatteet, miten hakea informaatiota (JSON.org 2012).

**Tiedonhankinnalla** tarkoitetaan tässä työssä kaikkea sitä toimintaa, jonka tarkoituksena on informaation kerääminen päätöksenteon tueksi. Tässä työssä tiedonhankintaan sisältyy myös tiedustelu ja vakoilu.

# 3 Opinnäytetyön tutkimuksellinen viitekehys

Tutkimuksessa on pohjimmiltaan aina kyse jonkun ilmiön kuvaamisessa, selittämisessä, tulkinnasta tai ymmärtämisestä. Usein pyritään myös hakemaan kuvailtavan ilmiön taustalta tekijöitä, jotka auttavat sen ymmärtämisessä. Tutkimuskohteita voidaan käsitellä monesta eri näkökulmasta ja tutkimus voidaan suorittaa monin eri menetelmin. (Puusa & Juuti 2011, 12.)

Hirsjärven ym. (2006, 114) mukaan, jonkun ilmiön tutkiminen on valintojen ja päätösten tekemistä, joihin liittyy aina ongelmia. Tehdyt valinnat voivat liittyä esimerkiksi tutkittavan kohteen valitsemiseen, aineiston keräämiseen tai tutkimuksellisen lähestymistavan valintaan. Näihin valintoihin ei ole olemassa oikeita vastauksia, vaikka valinnat sekä päätökset ovat tärkeitä tutkimuksen onnistumisen kannalta. Lähestymistavan valinta vaikuttaa aina lopputulokseen. Tutkimus ei ole välttämättä parempi tai huonompi, vaan siitä tulee erilainen, kuin toisella tutkimustavalla.

Opinnäytetyöt etenevät harvoin niin selkeästi kuin valmiista opinnäytetyöraportista voisi päätellä. Opinnäytetyön edetessä eteen tulee useita haasteita, ja opinnäytetyötä tekevän on tehtävä valintoja. Esimerkkejä näistä valinnoista ovat käsiteltävän aiheen valinta, lähestymistapa, tutkimuskysymysten muodostaminen ja niin edelleen. Opinnäytetyö etenee harvoin lineaarisesti ja valintoja joudutaan tekemään osin päällekkäin, ne voivat kytkeytyä toisiinsa ja tätä kautta ne ohjaavat opinnäytetyötä eteenpäin. (Häikiö, Niemenmaa 2007, 41.)

## 3.1 Laadullisen tutkimusmenetelmän valinnan haasteet

Tämän opinnäytetyön lähestymistavan kartoitus alkoi aihealueen valinnalla. Valintaan vaikutti henkilökohtainen mielenkiinto tietoturvallisuuteen ja etenkin tiedon tehokkaampaan hallintaan ja käsittelyyn turvallisuuden näkökulmasta. Toinen aihealueen valintaan vaikuttava tekijä oli kirjoittajan kasvava kriittisyys tämän hetken keskusteluun sosiaalisen median riskeistä. Tältä pohjalta muodostuivat alustavat tutkimuskysymykset, joita tässä opinnäytetyössä tarkastellaan.

Lähestymistavaksi valittiin laadullinen tutkimus. Se soveltuu tutkimuksen lähestymistavaksi eritäin hyvin silloin, kun

1. ollaan kiinnostuneita tapahtumien yksityiskohtaisista rakenteista eikä niinkään niiden yleisluontoisesta jakaantumisesta,
2. ollaan kiinnostuneita tietyissä tapahtumissa mukana olleiden yksittäisten toimijoiden merkitysrakenteista,

3. halutaan tutkia luonnollisia tilanteita, joita ei voida järjestää kokeeksi tai jossa ei voida kontrolloida läheskään kaikkia vaikuttavia tekijöitä, tai
4. halutaan saada tietoa tiettyihin tapauksiin liittyvistä syy- seuraussuhteista, joita ei voida tutkia kokeen avulla. (Syrjälä 1994, 12-13, Metsämuurosen 2008, 14 mukaan.)

Laadullisen tutkimuksen puolesta puhuu myös se, että sen tutkimusprosessi on joustava. Laadullinen tutkimus lähtee liikkeelle esiymmärryksestä, joka syventyy kirjallisuuskatsauksen avulla. Kirjallisuuskatsauksen jälkeen on mahdollista tarkentaa alkuperäistä käsitystä tutkimuskohteesta ja sille asetetuista kysymyksistä. Samalla myös tutkimuksen rajaus voi tarkentua. Tutkimusprosessi siis elää ja muovautuu koko ajan aina siihen asti, kunnes tutkimus on saatu julkaistavaan muotoon. (Puusa, Juuti 2011, 51.)

Laadullisen tutkimusmenetelmän kartoitus aloitettiin suppealla kirjallisuuskatsauksella, jossa tarkasteltiin laadullista tutkimusta käsittelevää tutkimuskirjallisuutta. Kirjallisuuskatsaus suuntasi ja tarkensi edelleen tutkimuksen aikana tehtäviä valintoja (Hirsjärvi ym. 2006, 98). Tutkimusmenetelmän valintaan vaikuttivat tavoitteet, alustavat tutkimuskysymykset, kirjoittajan näkemys aiheesta, millaista tietoa pyritään saavuttamaan sekä kohteen rajaus (Puusa & Juuti 2011, 23-24).

Kirjallisuuskatsauksen aikana tehtyjä havaintoja vertailemalla sekä tarkastelemalla asetettuja tavoitteita ja alustavia tutkimuskysymyksiä valinta tarkentui kolmeen mahdolliseen tutkimusmenetelmään. Tätä työtä voi lähestyä **tapaustutkimuksen**, **toimintatutkimuksen** tai **konstruktiivisen tutkimuksen** kautta.

Jos työtä lähestytään **tapaustutkimuksena**, on kyse empiirisestä tutkimuksesta, joka monipuolisilla ja monilla tavoilla hankittuja tietoja käyttäen tutkii nykyistä tapahtumaa tai toimivaa ihmistä tietyssä ympäristössä. (Yin 1982, 23, Metsämuurosen 2008, 16 mukaan.) Tapaustutkimuksen piirteisiin kuuluu se, että yksittäisestä tapauksesta tai pienestä joukosta toisiinsa suhteessa olevista tapauksista, tuotetaan yksityiskohtaista sekä intensiivistä tietoa (Saarela-Kinnunen & Eskola 2010, 190).

**Toimintatutkimuksena** tämä työ olisi tutkimusta, jonka avulla pyritään ratkaisemaan erilaisia käytännön ongelmia. Toimintatutkimuksessa pyritään siis vastaamaan johonkin käytännön toiminnassa olevaan ongelmaan (Metsämuuronen 2008, 29). Toimintatutkimuksena ei kuitenkaan pidetä mitä tahansa toimintaa, vaan siihen tulee liittyä sosiaalinen toiminta. Vaikka toimintatutkimusta on sovellettu esimerkiksi tietokoneohjelmien kehittämiseen tai maanviljelymenetelmien parantamiseen, näissä molemmissa on taustalla ihmisten välinen toiminta. (Heikkinen 2010, 214-215.) Toimintatutkimuksessa teoria ja käytäntö nähdään toisiaan tukevina kokonaisuuksina. Toimintatutkimusta kuvaa hyvin lause: mikään ei ole niin käytännöllistä

kuin hyvä teoria. Hyvä toimintatutkimus on laadukasta käytännön työtä yhdistettynä filosofiseen ajattelun taitoon. (Heikkinen 2010, 215.)

**Konstruktiivinen tutkimus** yhdistetään monesti toimintatutkimukseen. Se nähdään toimintatutkimuksen yhtenä muotona ja erityisesti kirjallisuudessa työkaluja kehittävät tutkimukset on monesti nimetty toimintatutkimukseksi (Uusitalo & Kohtamäki 2011, 282). Esimerkiksi Nykänen (2011, 78–80) kuvaa väitöskirjaansa toimintatutkimukseksi, jossa sovelletaan konstruktiivista tutkimusotetta, kun tarkoituksena on ratkaista todellisen elämän ongelmia ja tuottaa sitä kautta uutta tietoa.

Tutkimusmenetelmän valinnan haasteellisuutta lisää se, että kaikki kolme tutkimusmuotoa, voidaan nähdä myös laajemmin tutkimustapana tai tutkimusstrategiana, joiden sisällä voidaan käyttää useita eri metodeja tai toinen voi olla toisen menetelmän sisällä (Laine, Bamberg & Jokinen 2007, 9; Heikkinen 2010, 214; Uusitalo & Kohtamäki 2011, 283). Esimerkiksi tapaustutkimuksessa konstruktiivinen tutkimus tapahtuu tapauksen kontekstissa (Uusitalo & Kohtamäki 2011, 283), kun taas toimintatutkimus perustuu aina johonkin tapaukseen, joten se voidaan nähdä yhtenä tapaustutkimuksen versiona (Lehtonen 2007, 245).

## 3.2 Toimintatutkimus

Tässä työssä sovelletaan toimintatutkimusta, mutta jos sitä tarkastellaan pelkkänä tutkimusmenetelmänä, antaa se työprosessista väärän kuvan. Tässä työssä toimintatutkimus on ymmärrettävä tutkimusstrategiana, joka sisältää useita eri työvaiheita: kirjallisuuskatsauksen avulla muodostuu kuva tutkimusmenetelmistä sekä työn taustalla vaikuttavista teorioista. Aineistoanalyysin avulla tarkastellaan Internetistä kerättyä tietoa sosiaalisen median riskeistä ja niiden taustalla vaikuttavista tekijöistä. Toimintatutkimuksen ja konstruktiivisen tutkimuksen keinoin tutkitaan kahden sosiaalisen median palveluntarjoajan kehitysympäristöä ja esitellään käytännössä miten niitä voidaan käyttää tiedonhankintaan.

Opinnäytetyön tutkimus suoritetaan oikeassa kohdeympäristössä, ja sen tarkoituksena on käsiteltävän aiheen syvällinen ymmärtäminen (Cohen & Manion 1995, 186; Baskerville & Wood-Harper 1998, Nykasen 2011, 77 mukaan). Tavoitteena on saada välitöntä hyötyä tutkimuksesta ja sille on tunnuksenomaista toiminnan ja tutkimuksen samankaltaisuus (Heikkinen 2010, 214).

Toimintatutkimus määritellään tilanteeseen sidotuksi (Situational), yhteistyötä vaativaksi (Collaborative), osallistuvaksi (Participatory) ja itseään tarkkailevaksi (Self-evaluative ). Menetelmä liittyy usein työyhteisöjen ja organisaatioiden muutosprosessiin. (Nykänen 2011, 77.) Toimintatutkimus soveltuu erittäin hyvin esimerkiksi tietojärjestelmätieteen tutkimuk-

seen, koska se mahdollistaa hyvin erilaisten käytänteiden, menetelmien ja näkökulmien huomioimisen (Baskerville & Wood-Harper 1996; Baskerville 1999, Nykäsen 2011, 79 mukaan). Toimintatutkimukselle on ominaista reflektiivinen ajattelu. Sen tarkoituksena on ymmärtää käsiteltävää kohdetta uudella tavalla. Reflektiivisyys näkyy toimintatutkimuksessa spiraalimaisena kehänä, jossa toiminta, sen havainnointi, reflektointi ja uudelleensuunnittelu seuraavat toisiaan. (Heikkinen 2010, 219-220.)

Toimintatutkimus koostuu viidestä eri vaiheesta. Toimintatutkimus alkaa diagnoosivaiheella (Diagnosing), jossa tunnistetaan ne olennaiset tekijät, joiden avulla saadaan vastaukset tutkimuksen pääkysymyksiin. Tämän jälkeen siirrytään suunnitteluvaiheeseen (Action planning), jossa määritellään päämäärät sekä suunnitellaan ja sovelletaan tutkimuksen viitekehystä. Suunnitteluvaiheen jälkeen alkaa toteutusvaihe (Action taking), jonka aikana toteutetaan tehdyt suunnitelmat asetettujen tavoitteiden mukaisesti. Arviointivaiheessa (Evaluating) arvioidaan kriittisesti, onko halutut päämäärät saavutettu. Oppimisvaiheessa (Specifying) tarkastellaan tutkimustulosten merkittävyyttä ja mahdollisia kehittämiskohteita. (Susman & Evered 1978; Susman 1983; Baskerville & Wood-Harper 1998; Baskerville 1999, Nykäsen 2011, 81 mukaan.)

Toimintatutkimusta kohtaan on esitetty myös arvostelua. Sitä on kritisoitu sen kaavamaisuudesta (Hopkins 1995, Heikkisen 2010, 221 mukaan). On väitetty, että se jopa haittaa toimintatutkimuksen tekijää, koska toiminnan etenemisessä ei voida todellisuudessa erottaa eri vaiheita. Lisäksi tutkimus on luonteeltaan sellainen, ettei sitä voi tiivistää yhteen eteenpäin menevään spiraaliin. On luonnollista, että tutkimuksen edetessä tulee yllättäviä sivujuonteita, joita ei ole voitu ottaa huomioon suunnitteluvaiheessa. (Heikkinen 2010, 221.) Tästä syystä on hyvä pitää mielessä se, että spiraali antaa vain periaatteellisen kuvan. Tosiasiassa tutkimuksen vaiheet menevät osittain toistensa päällä ja sivujuonteet kuuluvat tutkimuksen kulkuun (Kemmis 1994, 42, Heikkisen 2010, 221 mukaan). Toimintatutkimusta on arvosteltu myös siitä, että tutkimuskohde on yleensä hyvin rajattu, eikä siis ole edustava. Myös tavoitteet ja käytetyt metodit jäävän usein epäselväksi ja myös teorian ja käytännön yhdistäminen jää usein vaillinaiseksi (Metsämuuronen 2008, 32).

## 3.3 Aineiston hankinta ja käsittely

Tässä työssä aineiston hankinta on tärkeä osa työn etenemistä aivan alusta lähtien. Alustavat tavoitteet ohjasivat aineiston hankintaa ja uusi aineisto muokkasi tavoitteiden asettelua koko työn ajan. Työn haastavuutta aineiston osalta lisäsi se, että sitä on saatavilla erittäin paljon, joka teki käytettävän aineiston valinnasta haastavaa.

Työssä käytettyä aineistoa haettiin useasta eri lähteestä. Aihetta käsitteleviä artikkeleita ja tutkimuksia haettiin Nelli-, Worldcat-, Mendeley- ja AIS Electronic Library –tietokannoista. Tietokantojen lisäksi aineistoa haettiin Googlen ja Google Scholarin avulla. Lisäksi aineiston haussa käytettiin Copernic Agent Pro – hakuohjelmaa, jonka avulla oli mahdollista suorittaa hakuja samanaikaisesti 22 eri hakukoneella. Hakukoneiden avulla tietoa haettiin esimerkiksi keskustelupalstoilta. Aineiston luotettavuus ja käytettävyys olivat erityisen huomion kohteena, koska yhtenä tavoitteena oli tutkia Internetin hiljaista tietoa aiheesta. Tällaisissa tapauksissa aineisto ei välttämättä ollut lehtiartikkelin tai tutkimuksen muodossa, vaan se saattoi olla hakkeriyhteisön keskustelufoorumilla oleva kommentti

Hakukoneiden käytössä haasteena oli niiden kaupallinen rooli. Internetin suurimmat hakukonejätit Google, Bing ja Ask ovat kaupallisia yrityksiä. Mainostajat ovat näiden yritysten tärkein prioriteetti, koska ne tuovat yrityksille tuloja. Hakukoneiden käyttäjät ovat täten toisarvoisia (Appel 2011, 55). Esimerkiksi Googlella on käytössään 57 erilaista kriteeriä, jonka perusteella yritys luokittelee käyttäjänsä (Lifehacker.com 2012). Kriteerien perusteella Google luo profiilin käyttäjästä, jota Google myy eteenpäin yritysasiakkaille Googlen käyttäjiin kohdistuvana mainontana. Käyttäjille profilointi näkyy mainoksina ja siinä, että käyttäjästä luodun profiilin perusteella tietyt sivustot ovat hakutuloksissa korkealla. (Opsahl 2009.) Tämä ongelma ratkaistiin estämällä esimerkiksi Googlen keksien (cookies) asennus tietokoneelle sekä käyttämällä Copernic Agent Pro –hakuohjelmaa, joka estää kohdistetut hakutulokset.

Vaikka aineistoa oli käytettävissä erittäin paljon, siitä huolimatta eteen tuli kysymys sopivasta määrästä. Tutkielmia on usein arvioitu työmäärän perusteella ja aineiston keräämisprosessin vaikeutta on korostettu, vaikka lopputulos on voinut olla se, että aineistosta ei ole saatu sitten mitään irti (Hirsjärvi ym. 2006, 168; Saarela-Kinnunen & Eskola 2010, 189). Hirsjärven ym. (2006, 171) mukaan aineiston riittävyyttä voidaan tarkastella saturaation kautta. Saturaatiolla tarkoitettaan sitä, että aineistoa kerätään niin paljon, että samat asiat alkavat kertautua, jolloin on löydetty se määrä aineistoa, jonka avulla päästään teoreettisesti merkittävään tulokseen.

Vaikka monet pitävät saturaatioon perustuvaa aineiston hankintaa ohjenuorana, siihen liittyy ongelmia. Miten voidaan olla varmoja, että enää ei ole mahdollista löytää uutta tietoa? Lisäksi aineiston löytämiseen vaikuttaa aina tutkijan oma kyky löytää aineistoa ja huomata uusia näkökulmia. Laadulliseen tutkimukseen liittyy myös ajattelu, että jokainen tapaus on ainutlaatuinen, ei ole olemassa kahta samanlaista tutkimusta. (Hirsjärvi ym. 2006, 171.)

Toinen aineiston monimutkaisuuteen, luotettavuuteen ja valintaan liittyvä käsite on triangulaatio. Triangulaation käsite tulee navigoinnista ja sotastrategioista, jossa tietyn pisteen sijainti pyritään löytämään triangulaation avulla esimerkiksi mittaamalla kahden tunnetun si-

jainnin kulmat suhteessa tuntemattomaan sijaintiin. (Blaikie 1991; Massey 1999, Laineen ym. 2007, 23 mukaan.) Laadullisessa tutkimuksessa ei ole mahdollista löytää täsmällistä tietoa (pistettä), vaan triangulaatiolla tarkoitetaan kohteen tarkastelua eri näkökulmista (Laine ym. 2007, 23).

Triangulaatiota toteutettiin hakemalla tietoa useista erilaisista lähteistä. Aineiston hankinta saattoi lähteä liikkeelle yhdestä lehtiartikkelista, jota tarkennettiin hakemalla lisäinformaatiota muista vastaavista lehtiartikkeleista, sähköisistä tietokannoista ja aihepiiriä käsittelevästä kirjallisuudesta. Vertailemalla eri lähteitä varmistettiin työssä käytettävän aineiston luotettavuus. Saturaatiota sovellettiin samalla periaatteella: tässä työssä käytettävästä aineistosta tuli löytää havainto vähintään kahdesta eri lähteestä. Aineiston käsittelyä jatkettiin tiivistämällä aineiston sisältö ja sen jälkeen ne ryhmiteltiin sisällön ydinkohtien perusteella. Ryhmittelyn avulla saatiin selville aineiston väliset suhteet sekä varmistettiin aineiston käyttökelpoisuus.

### 3.4 Työhön liittyvät eettiset kysymykset sekä lainsäädäntö

Tutkimuksen etiikkaan liittyvissä kysymyksissä lähtökohtana on, että opiskelijan pitää toimia työssään hyvän tieteellisen käytännön mukaan. Vastuu tästä on ensisijaisesti opiskelijalla itsellään. Tiedon hankintaan ja julkistamiseen liittyvistä periaatteista ollaan laajasti yksimielisiä ja ne ovat yleisesti hyväksyttyjä. (Hirsjärvi ym. 2006, 25.) Ongelmalliseksi muodostuu kuitenkin kysymys siitä, mikä on tieteen ja tutkimustoiminnan vastuu tiedon käytöstä ja sen mahdollisista seurauksista yhteiskunnalle (Kuitunen 1995, Hirsjärven ym. 2006, 26 mukaan).

Tutkimukseen liittyvien eettisten kysymysten lisäksi käsiteltävään aiheeseen liittyi huomioitavaa lainsäädäntöä. Vaikka tämän tutkimuksen painopiste ei ole lainsäädännössä, tutkimuskysymysten asettelussa ja tehtyjen havaintojen esittelyssä tuli huomioida se, että tutkimus ei missään vaiheessa riko voimassaolevaa lainsäädäntöä. Lähtökohdat tälle vaatimukselle tulevat **perustuslaista**, **rikoslaista** ja **henkilötietolaista**.

Perustuslain (PL, 1999/731) 10 pykälä määrittelee yksityiselämän suojasta. Lain mukaan ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.” (Perustuslaki 1999/731.)

Rikoslain (RL, 1889/39) 38 luvun 8 §:ssä määritellään rangaistukset tietomurrolle ja sen yritykselle. Lain mukaan ”joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja,

taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.” (Rikoslaki 1889/39.)

Oleellista rikoslain tietomurtosäännöksessä on se, että aktiivinen porttiskannaus täyttää tietomurron yrityksen tuntomerkit, vaikka skannauksella ei olisikaan mitään erikoista tarkoitusta (Korkeimman oikeuden ennakkopäätös 2003:36). Vaikka korkeimman oikeuden ennakkopäätöksessä on kyse porttiskannauksessa, voidaan kuitenkin päätellä, että myös muut aktiiviset skannaukset voivat täyttää tietomurron tunnusmerkistön.

Kolmantena ohjaavana lakina käytettiin henkilötietolakia (HTL, 1999/523). Lain 3 luvun 11 §:ssä kielletään arkaluonteisten henkilötietojen käsittely, joita on esimerkiksi rotu, etninen alkuperä, poliittinen vakaumus, seksuaalinen suuntautuminen ja niin edelleen. (Henkilötietolaki 1999/523.) Näiden kolmen lainkohdan perusteella tässä työssä esitellään ainoastaan sellaista tiedon hankintaa, jonka jokainen voisi tietokoneruudultaan normaalisti lukea.

Toinen huomioitava seikka on Facebookin omat käyttöehdot. Käyttöehdoissa kohta C määrittelee tiedon keräämisen seuraavasti:

> *”If you collect content and information directly from users, you will make it clear that you (and not Facebook) are collecting it, and you will provide notice about and obtain user consent for your use of the content and information that you collect. Regardless of how you obtain content and information from users, you are responsible for securing all necessary permissions to reuse their content and information.*
> *You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.”*
> (Facebook.com 2012a.)

Facebook käytännössä kieltää tiedon keräämisen muilta kuin sen hyväksymiltä kaupallisilta toimijoilta. Tässä opinnäytetyössä kyseistä käyttöehtoa ei rikottu, koska tietoa ei kerätty. Lisäksi tiedonhankinnan mallintamisessa käytettiin Facebookin omaa käyttöliittymää.

# 4 Internetistä sosiaaliseen mediaan

Suuren yleisön tietoisuuteen tietoverkkojen käyttö alkoi tulla vasta 1990-luvulla, kun Sir Timothy Berners-Lee alkoi kehittää järjestelmää, jossa jokainen dokumentti olisi mahdollista linkittää toisiin dokumentteihin. Tämän hypertekstijärjestelmän oli tarkoitus parantaa tiedon leviämistä. Järjestelmälle annettiin nimeksi World Wide Web (WWW). Varsinainen läpimurto tapahtui kuitenkin vasta vuonna 1993, kun Marc Andersson kehitti ensimmäisen graafisen Mosaic-selaimen, joka mahdollisti Internetin sisällön käytön myös tavalliselle ihmiselle. Tästä alkoi ajanjakso, joka muutti ihmisten välistä yhteydenpitoa ennen näkemättömällä tavalla ja on lopulta johtanut nykytilaan. (Tirronen 2010, 11.)

Tällä hetkellä vallalla on käsitys, että elämme Internetin toista tulemista, jota kutsutaan valtamedioissa nimellä Web 2.0. Sen katsotaan saaneen alkunsa vuonna 2004 IT-kuplan puhkeamisen jälkeen. Nimi ei kuitenkaan tarkoita WWW:n uutta ohjelmistopäivitystä, vaikka sen voisi helposti näin käsittää. Web 2.0 kutsutaan uudeksi yläkäsitteeksi uusille toimintatavoille WWW:n käytössä. (Tirronen 2008, 18.)

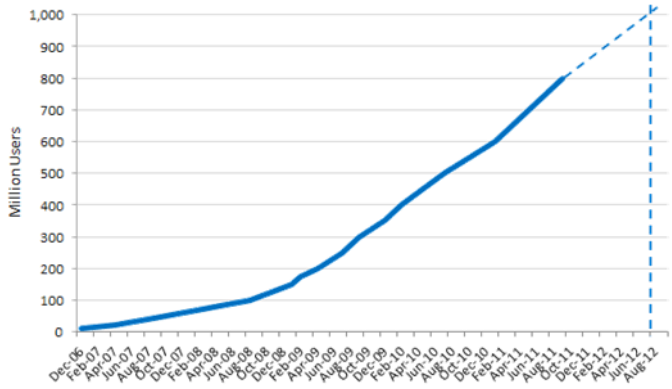
Web 2.0 kannattajat puhuvat kahdesta löytämästään päälinjasta: siirtymisestä WWW-pohjaisiin sovelluksiin ja sosiaalisemman lähestymistavan sisällön tuottamiseen ja jakamiseen. Internet on muuttunut staattisista sivustoista dynaamiseksi ja joustavaksi kokonaisuudeksi, jossa WWW:n käyttäjien keskinäinen vuorovaikutus on moninkertaistunut. (Tirronen 2008, 19.)

Uutta käsitettä kohtaan on myös esitetty kritiikkiä. Arvostelun mukaan kaikki edellä kuvatut asiat ovat olleet olemassa jo 1960-luvulta lähtien, kun kiinnostus laajojen tietoverkkojen tarjoamista mahdollisuuksista laajeni suuren yleisön keskuuteen. Alussa WWW:n perimmäinen tarkoitus oli sotilaallinen; kehittää järjestelmä, joka tarjoaisi toimivat tietoliikenneyhteydet jopa ydinsodan syttyessä. Kehitysvaiheessa huomattiin nopeasti, että verkon suosituimmaksi sovellukseksi kasvoi sähköposti eikä tiedonsiirto ja tietokoneiden etäkäyttö. Tänä päivänä teknologian kehitys on mahdollistanut eri asioiden toteuttamisen, mistä on unelmoitu jo WWW:n alusta lähtien. (Anderson 2006; Tirronen 2008, 8-9.)

## 4.1 Sosiaalinen media

Sosiaalisen median kehittyminen nykyiseen muotoon voidaan katsoa alkaneeksi vuonna 1978, jolloin julkaistiin ”Computerized Bulletin Board System”, joka ensimmäistä kertaa mahdollisti useamman henkilön keskustelun sähköisesti (Scott & Jacka 2011, 17). Todellinen sosiaalisen median esiintulo alkoi kuitenkin vasta Internetin toisen tulemisen aikakaudella. Juuri sosiaalinen media on ollut se tekijä, joka on muuttanut kaikkein voimakkaimmin ihmisten suhtautumista tietoon ja sen levittämiseen. Raja yksityisen ja julkisen tiedon sekä työn ja vapaa-ajan välillä on hämärtymässä ja kaikki nämä elementin ovat sekoittumassa keskenään. (Bhatti 2012, 57.)

Palvelut, jotka keskittyvät sosiaalisiin verkostoihin, ovat kasvattaneet käyttäjämääriään kaikkein eniten. Esimerkiksi tämän hetken suosituimmalla sivustolla Facebookilla oli joulukuussa 2011 845 miljoonaa kuukausittaista käyttäjää. Kasvu edellisen 12 kuukauden aikana oli 39 % (The Sociable 2012). Joulukuussa 2011 esitettiin arvio, että nykyisellä kasvuvauhdilla Facebookin käyttäjämäärä ylittäisi miljardin käyttäjän rajan elokuussa 2012 (Lyons 2012).




Taulukko 1: Facebookin käyttäjämäärien kasvu ja arvio (Lyons 2012).

Facebook ilmoitti saavuttaneensa miljardin käyttäjän rajan lokakuussa 2012 (Helsingin Sanomat 2012), eli arvio elokuusta ylittyi kahdella kuukaudella. Tämä ei kuitenkaan kerro koko totuutta, koska on arvioitu, että Facebookin ilmoittamasta luvusta jopa 83 miljoonaa on vääriä käyttäjätilejä (BBC News 2012; Hearn 2012).

Suurin osa sosiaalisen median kasvusta on tapahtunut viimeisen viiden vuoden kuluessa. Merkillepantavaa on miten paljon palveluiden käyttäjät tuottavat sisältöä verkkoon. On arvioitu, että Facebookissa käyttäjä luo noin 70 merkintää kuukaudessa ja Twitterissä käyttäjät luovat 70 miljoonaa viestiä, tweettausta, yhden päivän aikana. (Bhatti 2012, 58.)

Vaikka sosiaalisesta mediasta on tullut erittäin merkittävä osa ihmisten päivittäisessä elämässä, sille ei ole vielä olemassa selkeää määritelmää, vaan sosiaalisen median käsitteeseen liitetään eri tekijöitä (Erkkola 2008, 81). Esimerkiksi valtiovarainministeriön sosiaalisen median tietoturvaohjeessa (VAHTI 4/2010, 11) sosiaalinen media on tietoverkkoja ja tietotekniikkaa hyödyntävä viestinnän muoto, jossa käsitellään vuorovaikutteisesti ja käyttäjälähtöisesti tuotettua sisältöä ja luodaan ja ylläpidetään ihmisten välisiä suhteita.

Yleisesti sosiaalista mediaa kuvataan kertomalla mistä se koostuu ja mitä sillä voi tehdä. Sosiaalista mediaa on kuvattu sen tarjoamien palveluiden kautta tai sitten eri yhteisöpalveluiden piirteiden avulla. (Erkkola 2008, 81.) Taulukossa 2 on koottu esimerkkejä sosiaalisesta mediasta sen palveluiden kautta kuvattuna.

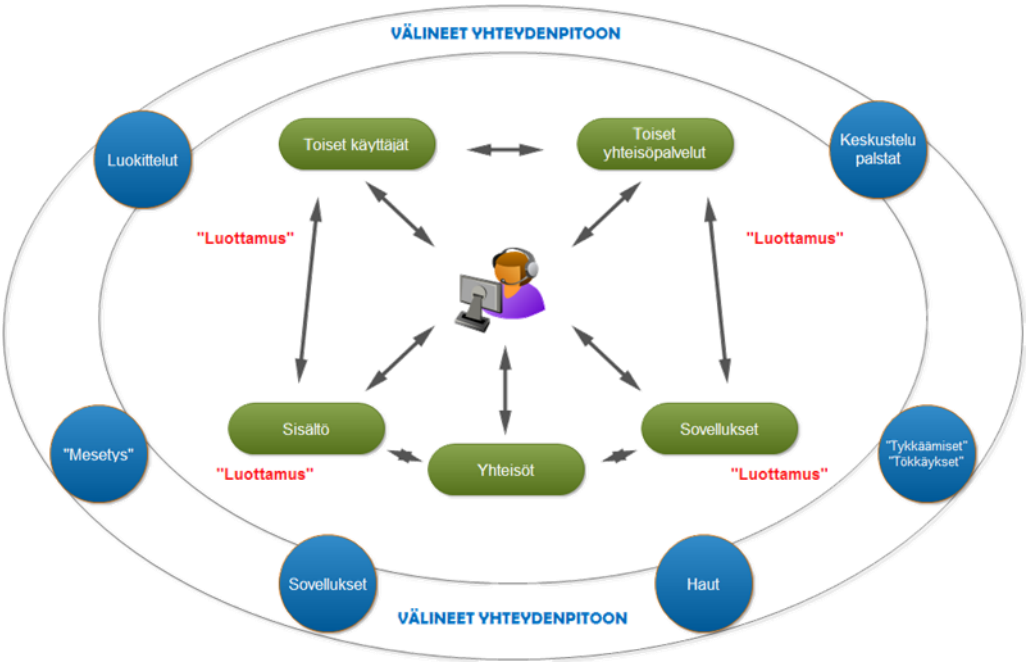
| Palvelu: | Esimerkkejä: |
|---|---|
| **Uutisten ja linkkien jakopalvelut:** | *Delicious* (kirjanmerkkien jakopalvelu)<br>*Digg* (uutistenjakopalvelu)<br>*Furl* (kirjanmerkkien jakopalvelu) |
| **Blogit:** | *WordPress* (mm. blogipalvelu)<br>*LiveJournal* (blogipalvelu, jossa myös mahdollisuus yhteydenpitoon ja vuorovaikutukseen)<br>*Vuodatus* (suomalainen blogipalvelu) |
| **Mikroblogit:** | *Twitter* (tunnetuin mikrobloggaus palvelu)<br>*Jaiku* (mikrobloggauspalvelu, joka oli erittäin suosittu suomessa) |
| **Wikit ja muut yhteisöpalvelut:** | *Wikipedia* (avoin tietosanakirja)<br>*Mediawiki* (wikiohjelmisto) |
| **Mediapalvelut:** | *Flickr* (kuvien jakopalvelu)<br>*SlideShare* (powerpoint esitysten jakopalvelu)<br>*Youtube* (videoiden jakopalvelu) |
| **Yhteisöt:** | *Facebook* (Yhteisöpalvelu)<br>*Linkedin* (ammattilaisille tarkoitettu verkostoitumispalvelu)<br>*Suomi24* (Suomen suurin yhteisöpalvelu) |
| **Virtuaalimaailmat:** | *Second Life*<br>*Habbo Hotel* |

Taulukko 2: Sosiaalisen median palveluita (mukaillen Kalliala & Toikkanen 2012).

Toinen tapa kuvata sosiaalista mediaa on eri palveluiden yhteisten piirteiden kautta. Useimmille palveluille on yhteistä esimerkiksi:

- ystävä- tai kaverilistat,
- kaveriverkostojen luominen,
- henkilökohtaisten tietojen (nimi, sähköpostiosoite, puhelinnumero, kotikaupunki, sukulaiset jne.) julkaiseminen henkilökohtaisen käyttäjäprofiilin kautta,
- toisten profiilien kommentointi (tykkäämiset jne.)
- sivuston sisäinen viestittelykanava, jonka avulla käyttäjät voivat keskustella,
- sivuston ylläpitäjän ansaintamekanismi perustuu käyttäjille kohdistettuun mainontaan. (Gross & Acquisiti 2005; Edwards & Brown 2009; Tuunainen ym. 2009.)

Tämän opinnäytetyön kannalta tärkeämpää on ymmärtää mistä kaikista osista sosiaaliset verkostot koostuvat. Yhden käyttäjän profiili koostuu useasta eri tekijästä, joita kutsutaan tässä työssä entiteeteiksi ja jotka linkittyvät toisiinsa. Näiden entiteettien ei tarvitse välttämättä olla toisia käyttäjiä.




Kuvio 1: Sosiaalisten yhteisöpalveluiden rakenne (mukaillen Moyer & Hamiel 2008).

Kuten kuviosta 1 voidaan nähdä, niin yhteisöpalveluiden käyttäjä luo verkoston, ei pelkästään toisiin käyttäjiin, vaan myös sisältöön, eri yhteisöihin, sovelluksiin ja toisiin yhteisöpalveluihin. Välineinä verkoston eri osatekijöiden, entiteettien, välisessä yhteydenpidossa toimivat luokittelut, ”mesetys”, sovellukset, erilaiset haut, ”tykkäämiset” ja keskustelupalstat. Tärkeimpänä tekijänä tässä mallissa on huomata se, että verkoston eri entiteettien välillä on oltava jonkinlainen luottamukseen perustuva suhde. (Moyer & Hamiel 2008.)

Sosiaalisesta mediasta on tullut niin merkittävä osa ihmisten elämää, että henkilöitä, joilla ei ole esimerkiksi omaan Facebook -profiilia, pidetään outoina ja epäilyttävinä (Manjoo & Yoffe 2012; Schulze 2012). Saksalainen toimittaja Schulze (2012) kirjoitti artikkelissaan, että Facebook -profiilin puuttuminen voi olla ensimmäinen merkki mahdollisesta sarjamurhaajasta. Hän perusteli väitteensä sillä, että Norjan joukkosurmaajalla Anders Breivikillä ja Auroran ampujalla ei ollut omaa profiilia Facebookissa (Schulze 2012). Farhad Manjoo on samalla linjalla Schulzen kanssa. Manjoo väittää, että jos esimerkiksi deittikumppanista ei löydy mitään tietoja Facebookista, se voi indikoida, että hänellä on jotain salattavaa ja sen takia häneen tulisi suhtautua hyvin varovaisesti (Manjoo & Yoffe 2012).

Edellä kuvattuun kahteen esimerkkiin tulee suhtautua kriittisesti. Ne kertovat enemmän suuria ikäluokkia vaivasta epävarmuudesta siihen, miten suhtautua vallitsevaan muutokseen ihmisten suhtautumisessa yksityisyyteen ja tiedon jakamiseen. Nopean kasvun haittana on se, että sosiaalisesta mediasta on tullut entistä tärkeämpi osa rikollisten toimintakenttänä (Gragido & Pirc 2001, 13). Suuri käyttäjämäärä tarjoaa verkkorikollisille uuden kanavan etsiä uusia

potentiaalisia uhreja, levittää haittaohjelmia sekä hyökätä organisaatioiden tietoverkkoja vastaan (Gragido & Pirc 2011, 14).

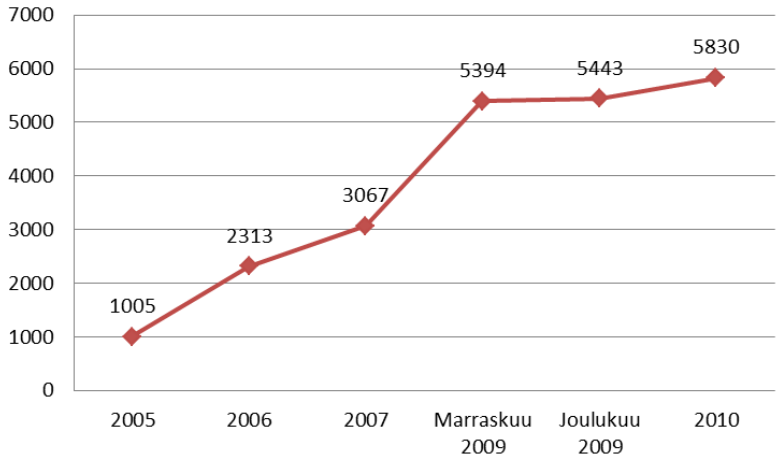
## 4.2 Facebook ja Twitter

Tässä kappaleessa käydään läpi lyhyesti kaksi sosiaaliseen verkostoitumisen palvelua: Facebook ja Twitter. Kyseiset palveluntarjoajat valittiin, koska niiden yhteinen käyttäjämäärä ylittää 1,5 miljardia käyttäjää. Suuren käyttäjämäärän takia ne ovat verkkorikollisuuden kannalta, erittäin hyviä paikkoja etsiä mahdollisia uhreja. Lisäksi molemmat palveluntarjoajat noudattavat hyvin aikaisemmin esitettyä kuvausta yhteisöpalveluiden rakenteesta.

### 4.2.1 Facebook

Facebook aloitti toimintansa vuonna 2004 aluksi yliopistojen opiskelijoiden yhteydenpitovälineenä. Vuonna 2006 palvelu avattiin kaikille Internetin käyttäjille ja sen jälkeen Facebookin käyttäjämäärät ovat kasvaneet erittäin nopeasti. (Dey, Jelveh & Ross 2012.) Koska Facebook oli tarkoitettu alussa pelkästään opiskelijoiden väliseksi yhteydenpitovälineeksi, sen lähestymistapa yksityisyyteen oli verkostokeskeinen. Kaikki tieto oli jokaisen verkoston jäsenen nähtävissä. (Mahmood & Desmedt 2012, 1.)

Palvelun avauduttua kaikille on Facebook joutunut muuttamaan yksityisyyden suojan politiikkaansa useaan kertaan. Kuvaavaa tässä kehityksessä on ollut se, että esimerkiksi yksityisyyden suojan politiikka oli vuonna 2005 ainoastaan 1004 sanaa pitkä, kun taas vuonna 2010 pituus oli jo 5830 sanaa. (New York Times 2010.)




Taulukko 3: Facebookin yksityisyyden suojan politiikan sanojen määrän kasvu (New York Times 2010).

Vaikka yksityisyyden suojan politiikkaa on päivitetty useaan kertaan, Facebook saa kritiikkiä juuri käyttäjien yksityisyyden suojan laiminlyömisestä. Suurimpina kritiikin kohteina ovat olleet seuraavat ominaisuudet:

- oletusasetukset vaarantavat käyttäjän yksityisyyden jakamalla liian paljon tietoa,
- politiikan muuttuessa ennestään yksityiseksi merkityt tiedot muuttuvat julkiseksi,
- yksityisyysasetukset ovat liian monimutkaiset,
- käyttäjän tietoja voi jakaa toiset käyttäjät (kaverit) tai palvelut ilman erillistä lupaa,
- uudet palvelut mahdollistavat käyttäjän tiedon jakamisen ja julkaisemisen myös kolmannen osapuolen nettisivuilla,
- Riippuen käyttäjän asetuksista, kolmannen osapuolen nettisivut ja Facebook voivat jakaa tietoja keskenään. (Bhatti 2012, 63-64.)

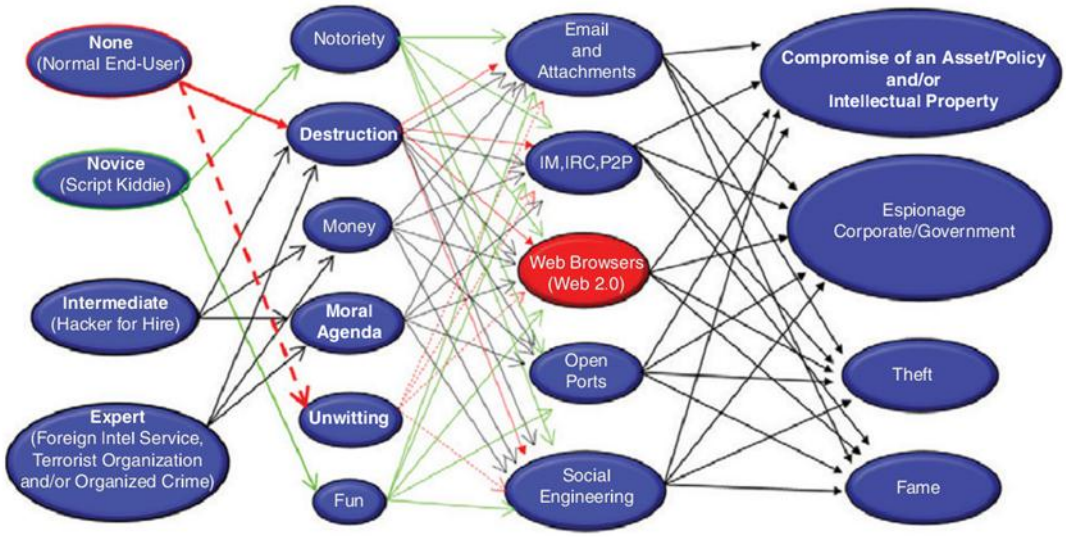
### 4.2.2 Twitter

Twitter on toinen kansainvälisesti erittäin suosittu sosiaalisen median palvelu. Twitteristä on tullut kuudessa vuodessa yksi suosituimmista Internetin verkkosivusta, jolla oli vuonna 2012 yli 500 miljoonaa aktiivista käyttäjää (Dugan 2012).

Twitter eroaa Facebookista siten, että vaikka Twitterissä käyttäjän voi luoda profiilin, se on toisarvoinen ominaisuus. Twitterin pääasiallinen tarkoitus on olla mikrobloggauspalvelu, jossa käyttäjät voivat lähettää ja lukea lyhyitä maksimissaan 140 merkin pituisia viestejä eli tweettejä (Chahal 2011, Smythin 2011 mukaan). Tweetit ovat julkisesti kaikkien nähtävissä, mutta käyttäjän on mahdollista rajoittaa niiden näkyvyyttä pelkästään omalle kaveripiirilleen (Smyth 2011). Twitterin käyttäjä voi myös tilata toisten käyttäjien tweettauksia, jota kutsutaan Twitterissä seuraamiseksi (Smyth 2011). Twitteriä voidaankin kutsua netin tekstiviestipalveluksi (D'Monte 2009).

## 5 Verkkorikollisuus

Viime vuosien aikana, myös verkkorikollisuus on muuttunut. Siitä on tullut entistä ammattimaisempaa ja röyhkeämpää. Lisäksi verkon kautta saatavilla olevat haittaohjelmat helpottavat verkkohyökkäyksen suunnittelua ja toteutusta. (Sophos 2012, 1-2.) Samalla myös verkkorikollisuuden toimijat ovat muuttuneet. Amatöörikrakkereiden rinnalle on tullut toimijoita, joilla on selkeä taloudellinen, poliittinen tai ideologinen motivaatio (Gragido & Pirc 2011, 115). Näiden verkkorikollisten ammattitaidon taso, menetelmät sekä resurssit vaihtelevat nollasta aina huippuammattilaisiin ja valtioiden tukemiin toimijoihin. Verkkorikollisia voidaan luokitella heidän ammattitaidon, motivaation, taustalla vaikuttavan ideologian ja heidän käyttämiensä menetelmien mukaan. (Gragido & Pirc 2011, 115-117.)




Kuvio 2: Verkkorikollisten luokittelu Gragido & Pirc:n (2001, 116) mukaan.

Vaikka verkkorikollisuus on muuttunut ammattimaisemmaksi, siitä huolimatta rikolliset käyttävät edelleen hyväksi automatisoituja massahyökkäyksiä, kuten portti- tai haavoittuvuusskannauksia. Tämän tyyppisissä hyökkäyksissä kiinnijäämisriski on pieni ja tuotot voivat olla suuria. Automatisoidut hyökkäykset soveltuvat hyvin pehmeisiin kohteisiin, eli esimerkiksi sellaisiin yrityksiin, joissa ei ole resursseja tai osaamista panostaa tietojärjestelmien suojaukseen ja tietoturvallisuuteen. (Gragio & Pirc 2011, 9-11; Verizon 2012, 1.) Automatisoitua hyökkäystä voidaan myös käyttää harhautuksena, jonka avulla verkkorikollinen siirtää kohdeorganisaation huomion toisaalle ja mahdollistaa paljon tehokkaamman hyökkäyksen tai tunkeutumisen kohteen tietojärjestelmiin.

Massahyökkäysten rinnalle on tullut uudenlainen menetelmä, jolla verkkorikolliset yrittävät tunkeutua tietojärjestelmiin. Menetelmä poikkeaa massahyökkäyksistä siten, että se on erittäin hyvin suunniteltu, kohdistuu yksittäiseen kohteeseen, esimerkiksi yritykseen ja hyökkääjällä on selkeä motiivi ja tavoite. Näiden lisäksi hyökkääjä pyrkii toimimaan mahdollisimman huomaamattomasti. (Mcclure, Scambray & Kurtz 2012, 313.) Tästä menetelmästä käytetään termiä Advanced Persistent Threat tai kohdistetut hyökkäykset.

## 5.1 Kohdistetut hyökkäykset (Advanced Persistent Threat)

Valtiovarainministeriön tietoturvaohjeessa (VAHTI 6/2009, 9) kohdistetut hyökkäykset määritellään jonkin tietyn tiedon kaappaamiseksi tai tietyn kohteen toiminnan haittaamiseksi, joka kohdistuu tiedon luottamuksellisuuteen ja eheyteen ja jota on erityisen hankala havaita ja estää käytössä olevilla torjuntamalleilla. Ensimmäisen kerran kohdistettujen hyökkäysten käsitteen määrittelivät Yhdysvaltain ilmavoimien tutkijat vuonna 2006 yrittäessään selvittää tunkeutujan profiilia, tavoitteita ja tunkeutujan organisaation rakennetta mahdollisimman

lyhyesti (Mcclure ym. 2012, 318). Tutkimuksen lopputuloksena syntyi termi Advanced Persistent Threat (APT).

Käsitteen taustalla vaikuttivat Yhdysvaltain hallintoon ja puolustusteollisuuteen kohdistuneet tietomurrot, kuten esimerkiksi vuonna 2003 paljastunut tapaus, jolle Yhdysvaltain hallitus antoi nimen Titan Rain. Kyseisessä tapauksessa Yhdysvaltain viranomaisten ja puolustusteollisuuden tietojärjestelmiin oli tunkeuduttu ja tunkeutujat latasivat järjestelmällisesti tietoa eri tietolähteistä, mitä he sitten lähettivät eteenpäin. Tunkeutumisen jäljet päättyivät Quandongiin Kiinaan. Vaikka tapauksen kaikki yksityiskohdat eivät ole selvillä, yleisesti uskotaan että kyseessä oli Kiinan Tasavallan organisoima vakoilu, joka kohdistui Yhdysvaltoihin. (Graham 2005; Thonburg 2005.)

Edellä kuvatun tapauksen vuoksi, APT:tä kohtaan on myös esitetty kritiikkiä. Sitä on kritisoitu markkinointitermiksi, jonka avulla voidaan myydä uusia turvallisuutta parantavia ratkaisuja. Lisäksi APT:tä on kritisoitu siitä, että sillä tarkoitetaan vain tiettyjen valtioiden, erityisesti Kiinan ja Venäjän, suorittamaa vakoilua, jolloin esimerkiksi järjestäytyneen rikollisuuden tekemät tietomurrot jäävät määritelmän ulkopuolelle. (Carr 2011.)

## 5.2 Kohdistettujen hyökkäysten rakenne

Kohdistetut hyökkäykset eroavat muusta verkkorikollisuudesta siten, että kohdistetuissa hyökkäyksissä on selkeät vaiheet, joiden kautta hyökkäys etenee. Valtiovarainministeriön tietoturvaohjeiden (Vahti 6/2009, 18–20) mukaan nämä vaiheet ovat **tiedustelu**, **haittakoodin ujutus**, **haittakoodin aktivoituminen**, **tiedonkeruu** ja **tiedon lähettäminen ulos organisaatiosta**.

**Tiedusteluvaiheessa** hyökkääjä pyrkii hankkimaan kohteesta niin paljon tietoja kuin mahdollista. Tiedustelu voi tapahtua sosiaalisen tai teknisin menetelmin käyttämällä hyväksi erilaisia julkisia lähteitä kuten kohteen verkkosivuja tai sanomalehtiä. Myös tietoverkoissa käytettävät reitittimet ja kytkimet voivat luovuttaa epäsuorasti tietoja, jotka paljastavat kohteen tietoverkon rakenteet. (Vahti 6/2009 18.)

Saatuaan kohdeorganisaatiosta riittävästi tietoa, seuraava vaihe on **haittakoodin ujuttaminen kohdeorganisaatioon**. Tämä voi tapahtua useammassa osassa esimerkiksi sähköpostin liitetiedostona, jolloin ensimmäisessä vaiheessa sähköpostin liitetiedostona siirtyy pieni pala ohjelmakoodia, jonka tarkoituksena on hakea verkosta varsinainen haittaohjelma. (Vahti 6/2009, 18.)

**Haittakoodin aktivoitumisvaiheessa** kohdeorganisaation tietoverkkoon ujutettu haittaohjelma aloittaa varsinaisen toimintansa. Hyökkääjä on voinut asettaa haittaohjelmalle viiveen ennen aktivoitumista, jonka avulla hän yrittää välttää haittaohjelman havaitsemisen kohdeorganisaation toimesta. (Vahti 6/2009, 19.)

**Tiedonkeruussa** kohdeorganisaation tietojärjestelmiin ujutettu haittaohjelma aloittaa varsinaisen työnsä, johon se on ohjelmoitu. Tarkoituksena on päästä käsiksi kohteena olevaan tietoon. Tämä voi tapahtua joko haittaohjelmaan ohjelmoidulla tavalla tai etäohjattuna, jolloin hyökkääjä valitsee haittaohjelman löytämästä tiedosta sen, mitä pitää tärkeimpänä oman tehtävänsä onnistumisessa. (Vahti 6/2009, 19.)

Viimeisessä vaiheessa haittaohjelman avulla löydetty tieto **lähetetään ulos kohdeorganisaatiosta**. Käytettävät menetelmät ovat usein suoraviivaisempia kuin haittaohjelman ujuttamisessa, koska tietoverkoissa valvotaan usein vain ulkoapäin tulevaa liikennettä. (Vahti 6/2009, 19.)

Yhteistä kaikille kohdistetuille hyökkäyksille on se, että tavoitteeseen päästäkseen hyökkääjä yrittää aiheuttaa mahdollisimman vähän häiriötä kohteen tietojärjestelmissä varmistaakseen oman toimintansa onnistumisen. Tiedossa on jopa tapauksia, jossa hyökkäyksen suorittaja on suojannut kohteen tietojärjestelmiä toisilta tunkeutujilta ja haittaohjelmilta. (Mcclure ym. 2012, 315.)

# 6 Sosiaalisen median riskien taustalla vaikuttavat tekijät

Käsitteenä riskille ei ole olemassa yksiselitteistä määritelmää, kuten sillä ei ole myöskää mitään selkeää rajaa, jolloin riski olisi hyväksyttävällä tasolla (Cendrowski & Mair 2009, 9). Yleensä riski mielletään vaaraa tai uhkaa tarkoittavaksi (Juvonen, Korhonen, Ojala, Salonen & Vuori 2008, 7). Siihen sisältyy ajatus, että voi tapahtua jotain epäedullista. Jotta voimme puhua riskistä, siihen tulee liittyä kolme eri osatekijää, joita ovat *epävarmuus* siitä, että jotain voi tapahtua sekä *odotukset*, eli sen miten koemme riskin ja sen mahdollisen toteutumisen. Viimeisenä osatekijänä on riskin *laajuus* ja *merkityksellisyys*, jotka kertovat sen, miten vakavaksi riski koetaan. (Juvonen ym. 2008, 8.) Riskiin sisältyy myös mahdollisuus. Liiketoiminnassa riskin ottaminen on usein välttämätöntä, jolloin riskiin liittyy uhkan lisäksi myös mahdollisuus taloudellisen menetyksen saamiselle. (Juvonen ym. 2008, 11.)

Tässä työssä sosiaalisen median riskien tarkastelun näkökulma on tietoturvallisuudessa ja miten ne vaikuttavat tiedon luottamuksellisuuteen, eheyteen ja käytettävyyteen. Valtiovarainministeriön tietoturvaohjeissa (Vahti 4/2010, 13–22) riskejä käsitellään tietoaineistoon liitty-

vinä riskeinä, teknisinä uhkina ja maineeseen vaikuttavina riskeinä. Näistä riskeistä on koottu yhteenveto taulukossa 4.

| **Uhka** | **Selitys:** |
|---|---|
| **Käyttäjä vuotaa tietoa** | *Käyttäjän sinänsä harmittomat viestit, esim. tilapäivitykset eivät yksittäin muodosta uhkaa, mutta useista eri palveluista kerättyjen tietojen avulla on mahdollista muodostaa hyvin tarkka tilannekuva käyttäjästä ja hänen edustamastaan organisaatiosta.* |
| **Toinen käyttäjä vuotaa tietoa** | *Vaikka palvelun käyttäjä ei lähettäisikään luottamuksellista tietoa, toinen käyttäjä voi omassa palvelussaan paljastaa tietoa esim. kommentoimalla valokuvaa tai julkaisemalla valokuvan, jossa käyttäjä esiintyy.* |
| **Laaja kaveripiiri mahdollistaa vakoilun** | *Sosiaalisessa mediassa käyttäjä helposti hyväksyy kaveripiiriinsä henkilön, jota he eivät kunnolla tunne. Tämä mahdollistaa soluttautumisen käyttäjän kaveripiiriin.* |
| **Some -palveluissa käytettyjen sähköpostiosoitteiden kautta tapahtuva hyökkäys** | *Sosiaalisen median palveluun kirjautuminen edellyttää sähköpostiosoitteen ilmoittamista. Usein sähköpostiosoite myös näkyy käyttäjän profiilissa. Profiileista kerättyjä sähköpostiosoitteita on mahdollista käyttää hyväksi lähettämällä niihin viestejä, jotka sisältävät haitallista koodia.* |
| **Identiteettivarkaus** | *Rikollinen voi yrittää kaapata käyttäjän profiilin ja esiintyä käyttäjänä.* |
| **Lyhennyspalvelun avulla naamioidaan haittasivusto** | *Esimerkiksi bit.ly ja tinyurl.com - palveluiden tarkoituksena on lyhentää url-osoite. Tämän tarkoituksena on säästää tilaa esimerkiksi twitterissä, jossa viestin enimmäispituus on rajattu 140 merkkiin. Tätä ominaisuutta on mahdollista käyttää hyväksi, niin että sillä naamioidaan haittasivusto. Käyttäjä ei voi tietää lyhennettyä osoitetta napauttaessaan mihin www-osoitteeseen hänen ohjataan.* |
| **Käyttäjien kaikkien tietojen oikeudet ovat palveluntarjoajalla** | *Pahimmillaan käyttäjä luovuttaa palveluntarjoajalle kaikki oikeutensa profiilinsa sisältämään aineistoon.* |
| **Palvelun tarjoaja on ulkomailla** | *Jos sosiaalisen median palvelun tarjoaja on ulkomailla, niin silloin palveluntarjoaja noudattaa kotimaansa lainsäädäntöä. Tämä voi aiheuttaa sen, että omien tietojen poistaminen voi olla hyvin vaikeaa tai jopa mahdotonta.* |

| | |
|---|---|
| **Väärän tiedon levittäminen** | *Sähköisessä muodossa olevan tiedon levittämistä on käytännössä mahdotonta valvoa, kuten myös tiedon todenperäisyyttä. Tämä mahdollistaa väärän tiedon levittämisen käyttäjästä tai hänen edustamasta organisaatiosta* |
| **Väärennetty profiili ihmisestä tai yrityksestä** | *Sosiaalisessa mediassa voi olla ihmistä tai organisaatiota jäljitteleviä profiileja. Näiden valeprofiilien kautta on mahdollista kerätä tietoa, levittää haittaohjelmia tai vuotaa väärää tietoa* |

Taulukko 4: Sosiaalisen median uhkatekijät (mukaillen VAHTI 4/2010).

Sosiaalinen media kehittyy ja muuttaa muotoaan jatkuvasti. Samalla muuttuvat myös siihen liittyvät uhkatekijät. Keskittymällä liikaa yksittäisiin uhkiin organisaatiot ajavat itsensä tilanteeseen, jota voidaan kutsua tulipalojen sammuttamiseksi. Toiminta keskittyy liikaa yksittäisiin uhkatekijöihin ja kokonaisuus unohtuu. Painopistettä tulisi siirtää yksittäisistä riskeistä niiden taustalla vaikuttaviin tekijöihin, eli riskin syihin.

## 6.1 Neutralisointiteoria ja neutralisointitekniikat

Tässä työssä sovelletaan neutralisointiteoriaa sosiaalisen median riskien tarkastelussa. Neutralisointiteoria soveltuu hyvin tietoturvatutkimuksiin, joilla pyritään vaikuttamaan työntekijöiden tietoturvakäyttäytymiseen ja ohjeistuksien noudattamiseen. (Siponen & Vance 2010, Nykäsen 2011, 47-48 mukaan). Sitä on sovellettu esimerkiksi tutkittaessa miten yliopisto-opiskelijat rationalisoivat digitaalisen laittoman kopioinnin (Moore & McMullan 2009). Neutralisoimisteorian avulla on tutkittu miksi työntekijät eivät noudata tietoturvapoliitikoita (Vance 2010), sekä arvioitu tietoturvakoulutuksen vaikuttavuutta (Nykänen 2011).

Neutralisointiteoria on amerikkalaisten kriminologien Gresham Sykesin ja David Matzan kehittämä teoria siitä, kuinka rikolliset perustelevat tekonsa itselleen. Heidän mukaansa rikolliset eivät poikkea niin sanotuista kunnon kansalaisista, vaan he tuntevat syyllisyyttä teoistaan aivan samalla tavalla kuin muutkin ihmiset. Neutralisointitekniikoiden avulla rikolliset perustelevat tekojensa oikeutuksen itselleen ja näin vähentävät teoista aiheutuvaa syyllisyyden tuntoa. (Laine 2007, 121–122.)

Sykesin ja Matzan mukaan neutralisoimistekniikoita voidaan löytää viisi eri variaatiota:

- vastuun kieltäminen,
- vahingon kieltäminen,
- uhrin kieltäminen,
- tuomitsijoiden tuomitseminen,
- vetoaminen korkeampiin velvollisuuksiin.
  (Laine 2007, 122.)

Vaikka neutralisoimisteorian lähtökohta on kriminologiassa ja sen tutkimuksessa, sitä on käytetty hyvällä menestyksellä myös muiden tieteenalojen tutkimuksessa (Nykänen 2011, 47). Neutralisoimisteoriaa sovellettu mm. tutkimuksessa, jossa tutkittiin naisten, lääkäreiden ja hoitajien suhtautumista aborttiin (Brennan 1974, Nykäsen 2011, 47 mukaan). Sitä on sovellettu edelleen myös tutkittaessa lukiolaisnuorien normeja rikkovaa käyttäytymistä (Mitchell & Dotter 1984, Nykäsen 2011, 47 mukaan). Tässä työssä sosiaalisen median riskejä tarkastellaan neutralisoimistekniikoiden kautta. Näin pyritään vastaamaan kysymykseen, miksi ihmiset eivät noudata esimerkiksi työnantajan antamia ohjeita sosiaalisen median käytöstä.

**Vastuun kieltämisessä** on kyse neutralisointitekniikasta, jossa henkilö siirtää henkilökohtaista vastuuta omasta teostaan muualle yhteisiä normeja rikottaessa (Sykes & Matza 1957; Rogers & Buffalo 1974, Nykäsen 2011, 53 mukaan). Vastuun kieltämistä kuvaa hyvin lause ”kuka tahansa muukin olisi tehnyt samoin kuin minä” (Coleman 1987, Nykäsen 2011, 53 mukaan). Näin esimerkiksi yrityksen sosiaalisen median pelisääntöjä rikkova perustelee oman toiminnan hyväksyttävyyttä ja siirtää mielessään vastuuta työyhteisössä muualle.

**Vahingon kieltämisestä** on kyse silloin kun sääntöjen rikkovat uskovat, että heidän käyttäytymisestään ei aiheudu mitään haittaa organisaatiolle, joten silloin se hyväksyttävää, vaikka se olisi ristiriidassa organisaation sisäisten ohjeiden kanssa (Sykes & Matza 1957, Nykäsen 2011, 49 mukaan). Yrityksellä voi olla ohjeet esimerkikisi luottamuksellisen tiedon käsittelystä, joka kieltää niiden lähettämisen web-pohjaiseen sähköpostiosoitteeseen, kuten Googlen Gmail -palveluun. Siitä huolimatta yrityksen myyntipäällikkö käyttää Gmailia asiakastietojen säilytykseen.

**Uhrin kieltämisessä** henkilö näkee eräänlaisena kostajana eräänlaisena Robin Hoodina, joka varastaa rikkailta ja antaa köyhille (Laine 2007, 122). Esimerkiksi yrityksestä irtisanottu voi perustella yritystä loukkaavan kirjoittelun Facebookissa tämän tekniikan avulla.

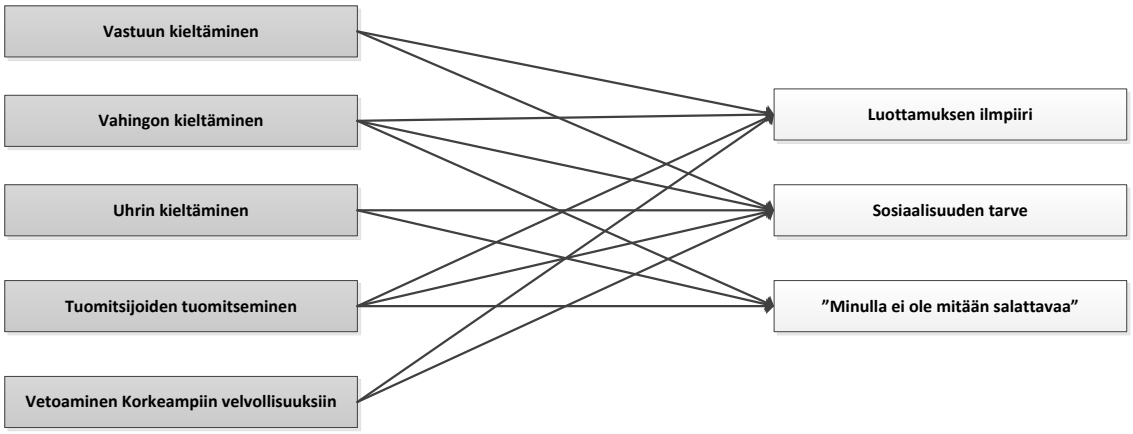
**Tuomitsijoiden tuomitseminen** -tekniikalla ”neutralisoidaan toimintaa, jonka tarkoituksenmukaisuutta, vaikutusta tai kohdetta ei tunneta riittävän hyvin” (Bayers ym 1999, Nykäsen 2011, 52 mukaan). Tietoturvaohjeita laiminlyödään perustelemalla se sillä, että ohjeet ovat

epäselvät (Siponen & Vance 2010, Nykäsen 2011, 52 mukaan). Ohjeita noudattavat voidaan nähdä tekopyhinä henkilöinä (Laine 2007, 122).

**Vetoaminen korkeampiin velvollisuuksiin** -tekniikassa henkilö rikkoo normeja ja ohjeita omien henkilökohtaisten syiden johdosta. Hän uskoo, että sääntöjen rikkomiselle on yksilöllinen oikeutus ja sääntöjen rajat ovat häilyviä. (Sykes & Matza 1957; Minor 1980, Nykäsen 2011, 50 mukaan.) Henkilö voi perustella Facebookin käyttöä työaikana esimerkiksi sillä, että hän tekee sen ainoastaan tauolla.

Neutralisoimisteoria antaa mahdollisuuden tarkastella sosiaaliseen mediaan liittyviä riskejä niiden taustalla vaikuttavien inhimillisten tekijöiden kautta. Johtoajatuksena on se, että riskillä voi olla monta siihen vaikuttavaa syytä, ja yksittäinen syy voi vaikuttaa moneen riskiin. Sosiaalisessa mediassa kyse on ennen kaikkia ihmisistä ja ihmisten välisestä vuorovaikutuksesta. Neutralisoimisteoria auttaa ymmärtämään niitä riskitekijöitä, joissa vaikuttaa käyttäjän oma toiminta.

Neutralisoimisteoria toimii tässä työssä yläkäsitteenä, jonka avulla on mahdollisuus ymmärtää paremmin sosiaalisen median riskien syitä. Vertailemalla työssä käytettyä aineistoa neutralisointitekniikoihin, voidaan neutralisoimisteoriasta tiivistää kolme erillistä tekijää, jotka yhdistävät kaikkia tähän mennessä tunnettuja sosiaalisesta mediasta esitettyjä riskejä. Nämä tekijät kuvaavat samalla sosiaalisen median luonnetta. Tekijät ovat **luottamuksen ilmapiiri**, **sosiaalisuuden tarve** ja **”minulla ole mitään salattavaa”**.

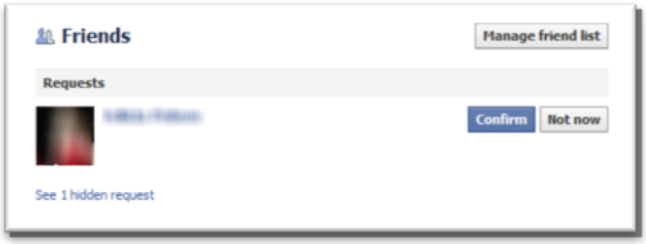



Kuvio 3: Neutralisoimisteoria ja sosiaalisen median riskeihin vaikuttavat tekijät.

Kuten kuviosta kolme voidaan todeta, esimerkiksi ”minulla ei ole mitään salattavaa” –ajatuksen taustalla vaikuttaa vahvasti kolme erilaista neutralisointitekniikkaa.

## 6.2 Luottamuksen ilmapiiri

Kappaleessa neljä kuvattiin sosiaalisen median palveluiden rakennetta yleisellä tasolla. Sosiaalisen median yksi olennaisimmista piirteistä on se, että palvelun eri toimijat (sovellukset, ihmiset, yhteisöt, sisältö) muodostavat verkoston, joka edellyttää aina jonkintasoista luottamusta toimijoiden välillä. Käytännössä luottamus näkyy tässä esimerkissä: käyttäjä hakee Facebookista vanhaa koulukaveriaan. Löydettyään tämän hän lähettää hänelle kaveripyynnön. Ennen kuin käyttäjä pääsee näkemään vanhan koulukaverin käyttäjäprofiilin, pyynnön vastaanottajan tulee hyväksyä hänen kaveripyyntönsä.



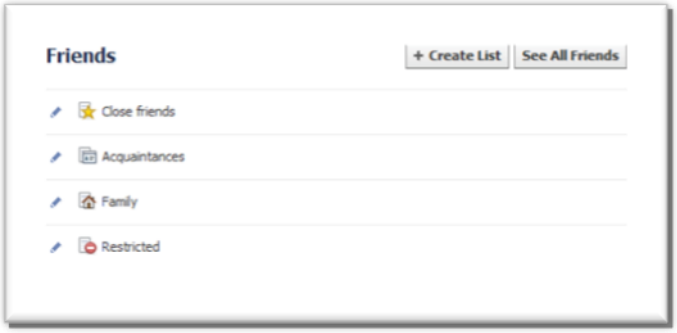

Kuva 1: Facebookin kaveripyyntö (Friends Request).

Samalla periaatteella toimivat myös kolmannen osapuolen sovellukset. Ennen kuin sovellusta voi käyttää, tulee käyttäjän hyväksyä sovelluksen käyttöehdot ja suostua siihen, että sovelluksella on oikeus käyttää käyttäjän profiilissa olevia tietoja.

Ensimmäinen ongelma luottamuksen ilmapiirissä liittyy ihmisten väliseen vuorovaikutukseen. Etenkin sosiaalisen median verkostoissa kynnys muodostaa sosiaalisia suhteita alenee, joten palvelun käyttäjä luo helpommin siteen toiseen käyttäjään, kuin mitä hän tekisi todellisuudessa (Sørensen 2009). Tällaisista siteistä käytetään monesti termiä heikko side (Ellison, Lampe & Steinfield 2009, Innon 2012, 19 mukaan). Heikolla siteellä tarkoitetaan sellaista ihmissuhdetta, jolla ei ole niin suurta merkitystä ihmisen päivittäisessä elämässä (Into 2012, 19). Sosiaalisessa mediassa tämä voi tarkoittaa sitä, että käyttäjällä voi olla jopa satoja kavereita, joilla on pääsy hänen profiiliinsa, mutta joita käyttäjä tuntee erittäin huonosti tai hän ei pysty varmistamaan, onko kaveriprofiilin takana todellinen henkilö (Gross & Acquisiti 2005).

Moyer ja Hamiel (2008) käyttivät hyväksi luottamukseen liittyvää ongelmaa ja testasivat sen mahdollisuuksia luomalla valeprofiilin tunnetusta tietoturva-asiantuntijasta. Profiili luotiin käyttämällä ainoastaan julkisista lähteistä saatua tietoa. Valeprofiili oli niin tehokas, että se sai kaveripyyntöjä, jopa kohteen perheenjäseniltä. (Moyer & Hamiel 2008.) Eräässä toisessa kokeessa tutkija huomasivat, että käyttäjät hyväksyvät kaveripyynnöt ”puolitutuilta” helpommin, jos hän on jo jonkun toisen tutun kaverilistalla (Bilge, Strufe, Balzarotti & Kirda 2009, 552).

Facebook on antanut käyttäjilleen mahdollisuuden luokitella kavereitaan sen mukaan, miten hyvin käyttäjä tuntee kyseisen kaverin. Luokittelulla käyttäjä voi rajoittaa oman profiilinsa näkyvyyttä esimerkiksi perheenjäsenten ja puolituttujen kesken. Tämän ominaisuuden käytöstä ei ole tutkittua tietoa, joten se miten paljon tätä ominaisuutta käytetään jää tässä vaiheessa avoimeksi.

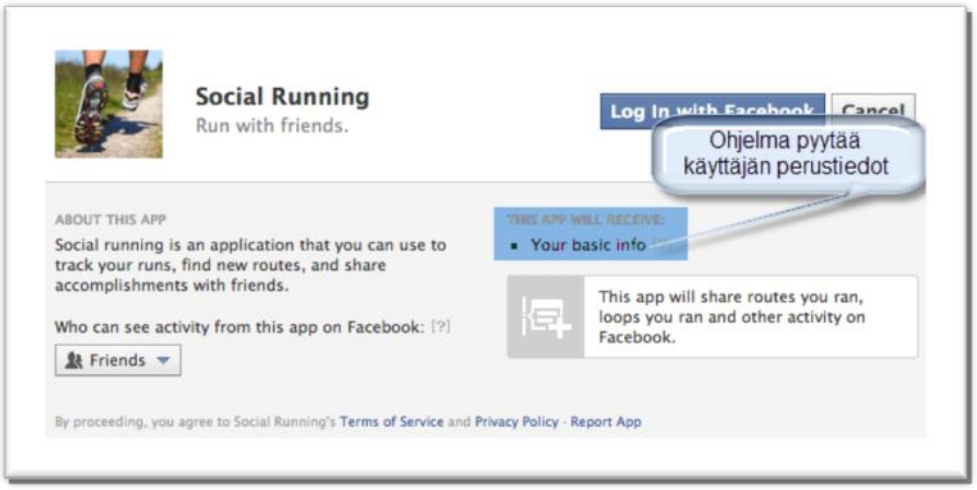



Kuva 2: Facebookin kavereiden luokittelu.

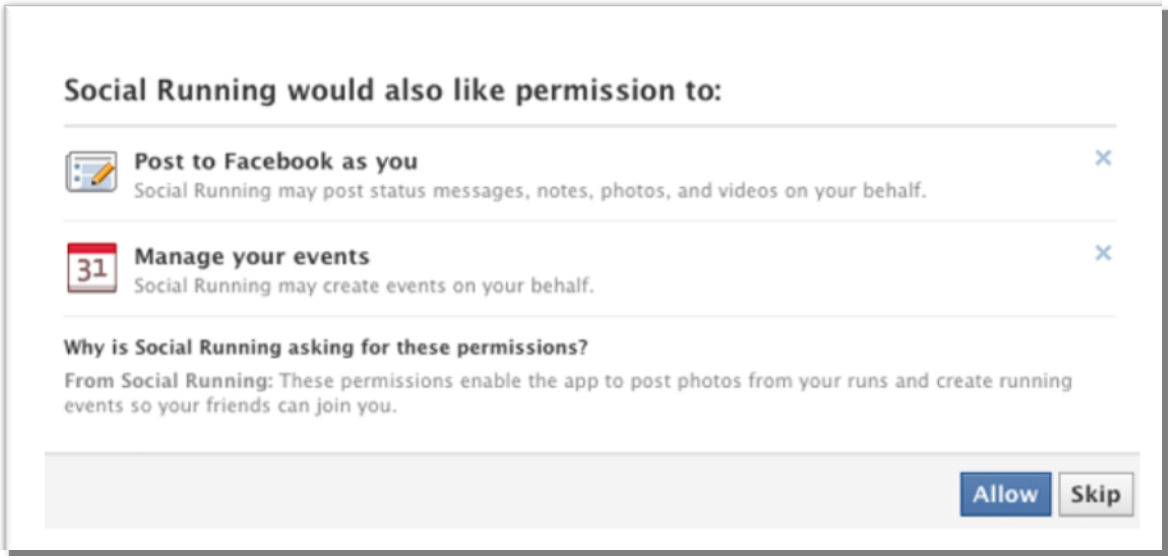
Toinen luottamukseen liittyvä ongelma liittyy sovelluksiin. Sovelluksen käyttö edellyttää sitä, että käyttäjä hyväksyy käyttöehdot, johon liittyy sovelluksen oikeus päästä käyttäjän profiilin tietoihin. Esimerkiksi Facebookilla (Facebook Developers 2012) on käytössään viisi erilaista tasoa sovellusten käyttöoikeuksista:

- perustiedot (Basic Information),
- käyttäjä- ja kaveritiedot (User and Friend Permissions),
- laajennetut oikeudet (Extended Permissions),
- open Graph –oikeuded (Open Graph Persmissions),
- sivuston oikeudet (Page Permissions).

Perustiedot sisältävät tiedot käyttäjän tunnisteesta (id), nimestä, sukupuolesta ja paikkatiedosta. Facebookin sovellukset saavat nämä oikeudet automaattisesti. Jos sovellus haluaa laajemmat oikeudet käyttäjän tietoihin, niin silloin se pyytää niitä käyttäjiltä erikseen. Tätä kirjoittaessa Facebookin sovelluskehittäjillä oli käytössään perustietojen lisäksi 45 eri kohtaa, joihin sovellukset voivat pyytää pääsyä. (Facebook Developers 2012.)




Kuva 3: Sovellus pyytää käyttäjän perustietoja (mukaillen Facebook Developers 2012).

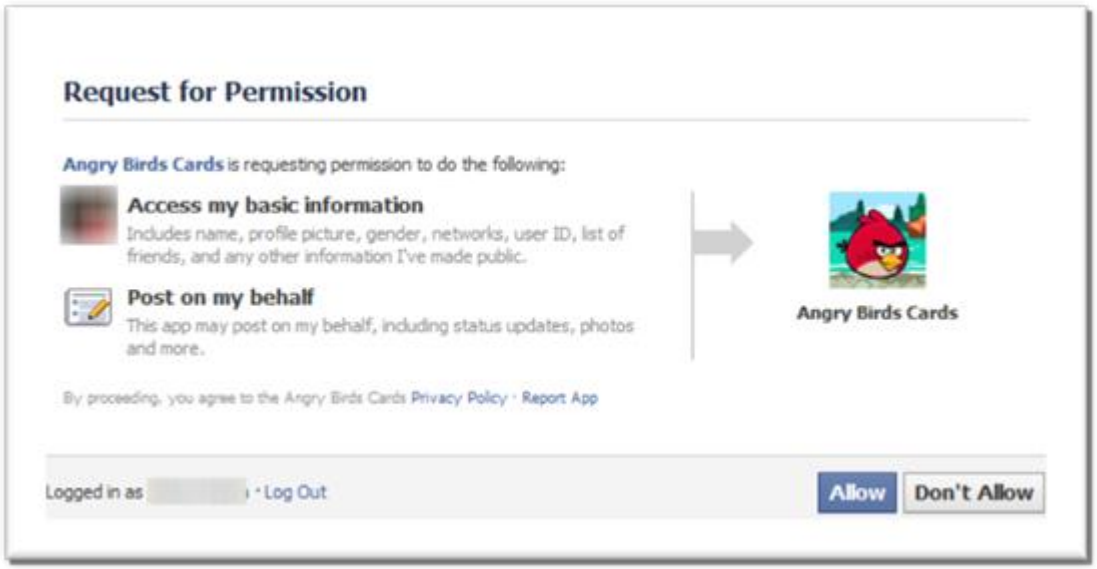



Kuva 4: Sovellus pyytää pääsyä perustietoja laajempiin oikeuksiin (Facebook Developers 2012).

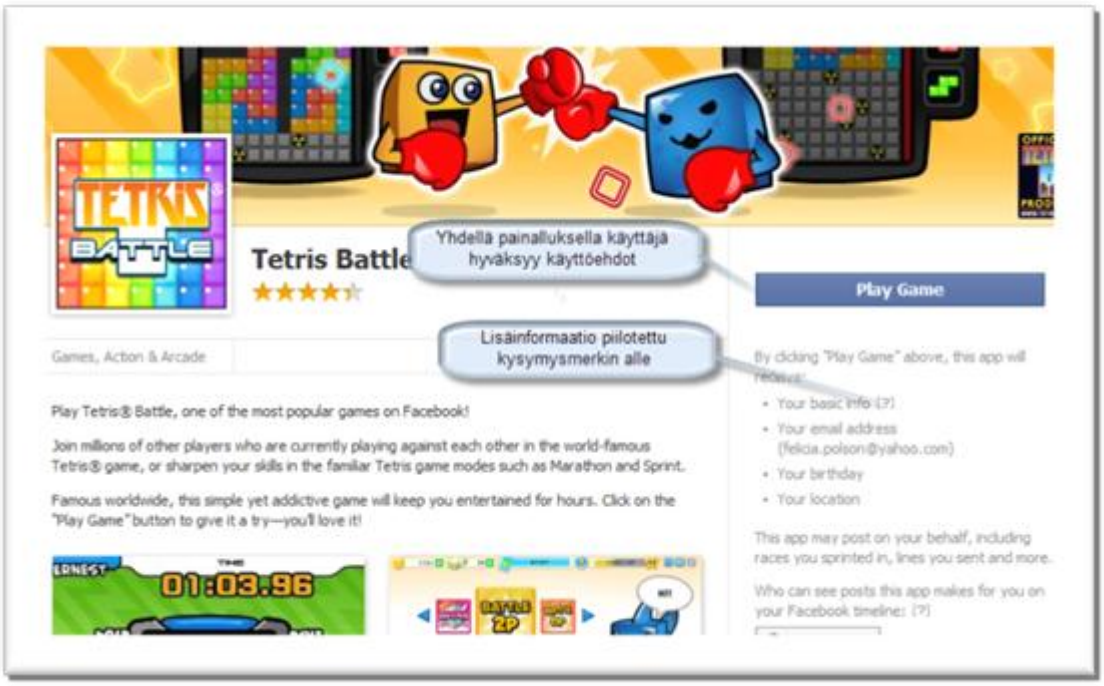
Kuten edellä kuvatusta ilmenee, sovelluksilla ei ole oikeuksia päästä käyttäjän profiilin, ellei käyttäjä anna sille erillistä lupaa. Tämä edellyttää luottamusta käyttäjän ja sovelluksen sekä sovelluksen kehittäjän kanssa. Ongelmaksi muodostuu se, että käyttäjät eivät välttämättä tiedä tai ymmärrä mihin he itse asiassa suostuvat, kun he esimerkiksi pelaavat Facebookin kautta tarjolla olevia nettipelejä (Wrenn 2012b). Myös se, että kuka tahansa voi tehdä ohjelman ja jakaa sitä Facebookin välityksellä aiheuttaa riskin. Ohjelma voi toimia pelkästään porttina, jolla kerätään käyttäjistä tietoa.

Etenkin Facebookia on kritisoitu yksityisyyden suojaan liittyvistä ongelmia ja siitä, että profiilin perusasetukset paljastavat liikaa tietoa käyttäjistä (Gross & Acqusiti 2005; Tuunainen ym. 2009, 6). Sovellusten kohdalla on havaittu, että Facebook pyrkii kehittämään sovelluspalvelujaan niin, että käyttäjät eivät huomaisi antavansa sovelluksille ja niiden kehittäjille oikeuksia käyttäjän profiilin tietoihin (Wrenn 2012a).

Facebookin julkistamassa uudessa sovelluskeskuksessa (App Center) tätä ajattelua on sovellettu uudella tavalla. Kuvassa 5 näkyy vanha sovellusten aloitusruutu. Siinä käyttäjä näkee selkeästi, että ohjelma pyytää lupaa käyttää käyttäjän profiilin tietoihin. Lisäksi käyttäjä joutuu tekemään selkeästi päätöksen sovelluksen käytöstä (Wrenn 2012a).




Kuva 5: Pelisovelluksen vanha ruutu (mukaillen Wrenn 2012a).




Kuva 6: Sovelluskeskuksen uusi käyttöliittymä (mukaillen Wrenn 2012a).

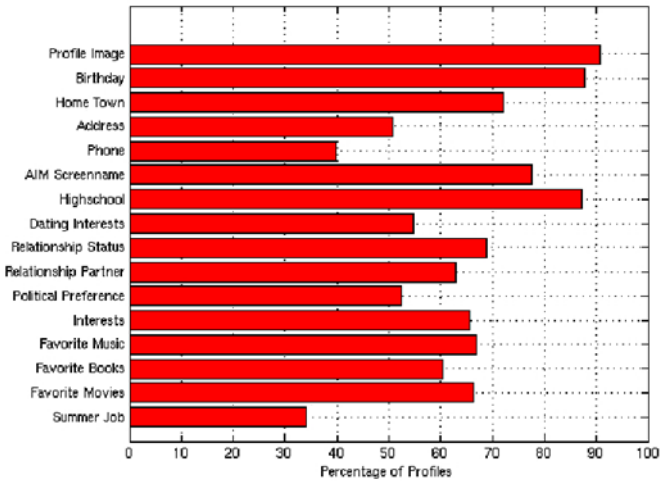
Kuvassa 6 on uuden sovelluskeskuksen aloitusruutu. Kuvasta ilmenee, että kaikki toiminnot on siirretty yhden painalluksen taakse. Play Game –komennolla käyttäjä hyväksyy käyttöehdot ja luovuttaa sovelluksen vaatimat tiedot ilman, että käyttäjä välttämättä tiedostaa koko asiaa. Myös kaikki lisäinformaatio on piilotettu huomaamattomasti kysymysmerkin taakse. (Wrenn 2012a.)

## 6.3 Sosiaalisuuden tarve

Sosiaaliseen mediaan liittyy vahvasti tirkistelyn ilmapiiri. Tämän seurauksena ihmiset pyrkivät luomaan itsestään verkkoprofiilia, joka korostaa käyttäjän persoonan hyviä puolia. Verkkoprofiili voi kertoa enemmän siitä, millaisena profiilin omistaja näkee itsensä tai millainen hän haluaisi olla. (Moyer & Hamiel 2008.) Sama kehitys on nähtävissä myös työelämässä. Linkedin palvelun mahtipontiset ansioluettelot ja työkavereiden molemminpuolinen hyväksyntä auttaa luomaan verkostokansalaisen identiteettiä (Moyer & Hamiel 2008). Verkostoidentiteetin luomiseen jopa kannustetaan. Esimerkiksi Isokangas ja Vassinen (2011) neuvovat kirjassaan Digitaalinen jalanjälki, kuinka luoda itsestään ammatillisesti ihanteellinen profiili.

Kehityksen kääntöpuolena on se, että ihmiselle tulee pakonomainen tarve näkyä verkossa. Tämä ilmenee monen eri tavoin, kuten esimerkiksi Facebook -profiilin jatkuvana päivittämisenä. Henkilö saattaa vaihtaa profiilikuvaansa päivittäin, kirjoittaa kymmeniä statuspäivityksiä ja kommentoida innokkaasti muiden päivityksiä ja niin edelleen. Työelämässä tämä voi näkyä esimerkiksi yli-innokkaana blogikirjoitteluna ja osallistumisena verkkokeskusteluihin.

Kehitys on johtanut siihen, että ihmiset julkaisevat hyvin avoimesti itsestään tietoa. Esimerkisi Grossin ja Acqusitin (2005) julkaiseman tutkimuksen mukaan 89 % Facebookin käyttäjistä on profiili omalla nimellä, 90,8 % on profiilissa kuva, josta hänet voi tunnistaa helposti. Lisäksi 87,7 % käyttäjistä ilmoittaa profiilissaan syntymäpäivänsä ja näistä 98,5 % ilmoittaa koko syntymäaikansa. Tämä kaikki tapahtuu siitäkin huolimatta, vaikka Facebookin käyttöehdot eivät niitä suoraan vaadi (Gross & Acquisiti 2005). Vaikka tutkimus on jo seitsemän vuotta vanha ja ihmisten käyttäytyminen on muuttunut, tästä huolimatta tutkimus kuvaa hyvin sitä, miten avoimesti ihmiset paljastavat itsestään tietoja. Samansuuntaisia tuloksia on saanut myös Tuunainen ym. (2009) tutkimuksessaan *Users' Awareness of Privacy on Online Social Networking sites – Case Facebook*. Yleisenä sääntönä voidaankin pitää sitä, mitä enemmän tietoja henkilö julkaisee itsestään profiilissa, sitä enemmän hänellä on myös kavereita. Hän on myös useamman ryhmän jäsen ja päivittää profiilinsa statusta aktiivisemmin. (Tuunainen ym. 2009, 10.)




Taulukko 5. Mitä tietoja käyttäjät paljastavat Facebookissa (Gross & Acqusiti 2005).

Sosiaalisuuden tarpeeseen liittyy myös laajat kaveripiirit. Henkilöllä voi olla useita satoja kavereita, joista valtaosa kuuluu niin sanottuihin heikkoihin siteisiin. Yhdistävänä tekijänä voi olla työpaikka, harrastus tai muu vastaava tekijä. Laaja kaveripiiri toimii tällöin sosiaalisena pääomana omistajalleen. (Into 2012, 19.) Tästä syystä suurin osa käyttäjistä on valmis hyväksymään kaverikseen henkilön, jota ei itse asiassa tunne tai josta ei voi olla varma, onko kyseessä henkilö se, joka väittää olevansa (Gross & Acquisiti 2005). Sosiaalisuuden tarve riskejä edesauttavana syynä muodostuu edellä kuvattujen osa-alueiden yhdistelmänä. Kun on pakko saada huomiota verkossa, ihminen helposti paljastaa itsestään, lähipiiristään tai edustamastaan organisaatiosta tietoa, joka aiheuttaa vahinkoa asianomaisille.

Ihmisten suhtautuminen siihen, miten paljon he ovat valmiita julkaisemaan itsestään sosiaalisessa mediassa, näyttäisi olevan muuttumassa. Dey ym. (2012) tutkivat vuosien 2010 ja 2011

välisenä aikana 1,4 miljoonan New Yorkissa asuvan henkilön Facebook profiilia ja he havaitsivat, että ihmiset ovat kiristäneet profiilinsa yksityisyysasetuksia. Esimerkiksi marraskuussa 2010 ainoastaan 17,2 % otannasta oli rajoittanut kaverilistansa näkyvyyttä. Kesäkuussa 2011 sama luku oli 52,6 %. (Dey ym. 2012.) Vaikka tutkimus oli maantieteellisesti rajattu, oletus on, että sama ilmiö toistuu globaalisti. Taulukossa 6 on yhteenveto Dey ym. (2012) tutkimuksen havainnoista.

| Attribute | March 2010 | June 2011 |
|---|---|---|
| % users with friend list public | 82.7 | 47.4 |
| % users with networks public | 25.1 | 21.4 |
| % users with relationship info public | 11.3 | 4.9 |
| % users with HS name and graduation year public | 13.4 | 9.1 |
| % users with gender public | 58.9 | 52.8 |
| % users with age public | 1.5 | 1.4 |
| % users with “interested in” public | 7.7 | 6.4 |
| % users with hometown public | 10.4 | 24.0 |
| % users with current city public | 31.3 | 36.5 |

Taulukko 6: Big-Picture View of Privacy Trends (Dey ym. 2012).

Yllä olevaa taulukkoa voidaan tulkita myös toisella tavalla. Vaikka 52,6 % Facebookin käyttäjistä on suojannut kaverilistansa, edelleen Facebookissa on varovaisesti arvioiden noin 450 miljoonaa avointa kaverilistaa.

### 6.4 ”Minulla ei ole mitään salattavaa”

Tämä lause ja sen erilaiset variaatiot ovat hyvin yleinen puolustus sille, millä sosiaalisen median käyttäjä perustelee omaa käytöstään ja motiiveja paljastaa itsestään sellaista informaatiota, mitä ei normaalisti tekisi (Solove 2007, 747). Lause kuvastaa hyvin yksityisyyden suojaan liittyvää paradoksia. Ihmiset esittävät samanaikaisesti huolensa yksityisyydestä, mutta jakavat itsestään tietoa vapaaehtoisesti sosiaalisen median palveluissa (Tuunainen ym. 2009, 10–11). Taustalla voi vaikuttaa myös se, että ihmiset käsittävät henkilökohtaisen tiedon, intiimit tiedot ja yksityisyyden eri tavalla. Intiimit tiedot halutaan suojata, mutta esimerkiksi uskonnollista vakaumusta, poliittista suuntautumista, syntymäaikaa ja niin edelleen, voidaan käsittää yksityisenä tietona, mutta ei intiiminä. Yksityiseen tietoon ei suhtauduta samanlaisella vakavuudella kuin intiimeihin tietoihin. (Solove 2007, 755.)

Toisenlainen variaatio voidaan havaita keskusteluista, jotka liittyvät siihen, miten paljon yritykset tai viranomaiset voivat käyttää hyväksi sosiaalisen median kautta saatavaa informaatiota. Tässäkin argumenttina käytetään usein seuraavaa: jos sinulla ei ole mitään salattavaa, sinulla ei ole mitään piiloteltavaa tai jos et ole tehnyt mitään laitonta, sinulla ei ole myös-

kään mitään pelättävää. (Solove 2007, 747–748.) Esimerkiksi Yhdysvalloissa viranomaiset vetoavat viimeksi mainittuun väitteeseen. Ja kääntäen: jos olet tehnyt jotain laitonta, sinulla ei ole laillista oikeutta vaatia yksityisyyttä. (Solove 2007, 746.)

Sosiaalisen median käyttäjien tulisi muistaa se, että tietoa kerätään ja käsitellään jatkuvasti jotakin tarkoitusta varten. Kuinka sosiaalisen median käyttäjä voi olla varma siitä, että säilytetäänkö tietoa asianmukaisesti, kuinka pitkään tietoa säilytetään, miten sen voi poistaa ja mihin toissijaisiin tarkoituksiin tietoa käytetään? (Solove 2007 760–764; Europe versus Facebook 2012.) Facebook esimerkiksi ilmoittaa tietosuojakäytännössään avoimesti, että jakaa käyttäjistään kokoamaansa tietoa yhteistyökumppaneille, sivustosta mainostilaa ostaville mainostajille ja kehittäjille (Facebook.com 2012b).

# 7 Sosiaalinen media tiedonhankinnan välineenä

Kun puhutaan tiedonhankinnasta, esiin nousevat usein käsitteet tiedustelu ja vakoilu. Näistä puhuttaessa on syytä ymmärtää käsitteiden ero. Suomen kielessä tiedustelu (*intelligence*) tai vakoilu (*espionage*) ymmärretään helposti toistensa synonyymeinä. Ero näiden kahden termin välillä on se, että vakoilu mielletään laittomaksi toiminnaksi. (Juutilainen 2008, 37.) Kolmas, kirjallisuudessa (Andress & Winterfeld 2011, 157; Faircloth 2011, 29) esiintyvä englanninkielinen termi tiedustelulle on *reconnaissance* tai *recon*. Kyseessä on alun perin sotilaallinen termi tiedonhankinnalle, jonka tarkoituksena on hankkia tietoa vihollisen joukoista visuaalisella tarkkailulla tai muilla keinoilla. (US Army 2001.)

Tiedustelusta puhuttaessa on kyse epävarmuuden vähentämisestä konfliktitilanteissa. Tiedustelu ei yritä ratkaista konfliktia, vaan se pyrkii hankkimaan tietoa toiselle konfliktin osapuolelle, mikä parantaisi tämän asemaa konfliktitilanteissa. (Juutilainen 2008, 37.) Tiedustelu jaetaan vielä alalajeihin sen mukaan, mikä on käytettävä menetelmä, jolla tietoa kerätään. Esimerkiksi tiedustelua, joka kohdistuu ihmisiin ja perustuu ihmisten kertomaan tietoon, käytetään termiä Human Source Intelligence, HUMINT (Gragido & Pirc 2011, 97). Taulukkoon 7 on koottu joitain tiedustelun alalajeja.

Edellä kuvattujen määritelmien taustalla on osittain sotilaallinen tai valtiollinen näkökulma. Mutta tiedonhankintaa tai tiedustelua tapahtuu päivittäin yksilötasolla. Ihminen hankkii Googlen avulla tietoa esimerkiksi ostopäätöksen tueksi. Yritysmaailma tuntee Business Intelligence -käsitteen, jolla tarkoitetaan yritysten järjestelmällistä tiedon hankintaa, säilytystä, käsittelyä ja jonka tarkoituksena on auttaa yritysjohtajia päätöksenteossa (Vercellis 2009, 12-14). Lisäksi yritysmaailmassa käytetään käsitettä Competitive Intelligence, kun puhutaan tiedonhankinnasta, jossa kerätään ja analysoidaan tietoa, jotka liittyvät yrityksen kilpailijoihin (Au-

roraWDC.com 2012). Yritysvakoilu (Corporate Espionge) käsittää tiedonhankinnan laittoman toiminnan.

| Tiedustelumuoto | Selitys |
|---|---|
| **HUMINT (Human Source Intelligence)** | *Ihmisiin ja heidän kertomaansa tietoon perustuva tiedustelumuoto. Edellyttää luottamusta.* |
| **COMINT (Communication Intelligence)** | *Signaailien ja viestin sieppaaminen sekä salauksen murtamiseen perustuvaa tiedustelua* |
| **IMINT (Imagery Intelligece)** | *Ilma ja satelliittikuvaukseen perustuva tiedustelumuoto* |
| **WEBINT (Web Source Intelligence)** | *Internetissä olevaan tietoon perustuvaa tiedustelua* |
| **OSINT (Open Source Intelligence)** | *Avoimiin lähteisiin perustuva tiedustelu. Käyttää hyväksi kaikkea vapaasti saatavilla olevaa tietoa.* |

Taulukko 7: Tiedustelun alalajeja (mukaillen Juutilainen 2008; Gragido & Pirc 2011).

***Tässä työssä tiedustelusta, vakoilusta tai reconnaissancesta pyritään käyttämään termiä tiedonhankinta. Tarkoituksena on tietoisesti välttää kuvaa, että kyseessä olisi pelkästään sotillaallista tai tiedustelupalvelujen harjoittamaa toimintaa. Lisäksi tiedonhankinta – termillä halutaan korostaa sitä, että tiedonhankintaa tapahtuu hyvin monella tasolla.***

On tärkeää ymmärtää, että tiedonhankinta on ollut merkittävässä roolissa ihmiskunnan kehityksessä siitä asti, kun se on alkanut muodostaa perhekuntaa isompia sosiaalisia ryhmiä. Tietoisuus ympäristöstä ja yhteisöä mahdollisesti uhkaavista tekijöistä on ollut olennainen osa ihmisten selviytymistä. Tieto on ollut aina valtaa ja tästä syystä niin pitkään kuin kirjoitettu kieli on ollut olemassa, on tunnettu myös vakoilun käsite. (Gragido & Pirc 2011, 81–82.)

Nykypäivänä tiedon ja tiedonhankinnan tarve ei ole muuttunut ja siihen liittyvät elementit, kuten esimerkiksi vakoilu on todellinen osa nykymaailmaa, vaikkei tätä välttämättä aina ymmärretä (Gragido & Pirc 2011, 81). Internet on muuttanut tätä aluetta tuomalla siihen suunnattoman määrä tietoa kaikkien saataville. Tiedonhankinta ei ole enää valtioiden harjoittama yksinoikeus, vaan sitä suorittavat myös yritykset, rikolliset sekä aktivistit. Hyvä ja kattava tiedonhankinta onkin tärkein tekijä onnistuneelle verkkohyökkäykselle tai tietojen kaappaamiselle. (Mcclure ym. 2009, 7-8; Street & Nabors 2010, 131; Faircloth 2011, 29.)

Andress & Winterfeld (2011, 157) jakavat Internetin kautta tapahtuvan tiedonhankinnan kolmeen kokonaisuuteen: avointen lähteiden kautta tapahtuvaan tiedusteluun (OSINT), passiiviseen tiedusteluun (passive reconnaissance) ja kohdistettuihin hyökkäyksiin (APT). Heidän mukaansa verkkotiedustelu aloitetaan avointen lähteiden tiedustelulla. Tarkoituksena on kerätä mahdollisimman paljon tietoa kohteesta ilman suoranaista kontaktia kohteeseen. Sen jälkeen siirrytään passiiviseen tiedonhankintaan, jotta saadaan sellaista tarkempaa tietoa, jota ei ole muuten mahdollista saada. (Andress & Winterfeld 2011, 157.)

Sosiaalisen median rooli tiedonhankinnassa on se, että siitä on tullut viime vuosina yksi merkittävimmistä tiedonhankintakanavista (Sophos 2010, 1). Sosiaalisen median alkuaikoina yritykset olivat huolissaan enemmän siitä, miten paljon työntekijöiden työaikaa menee sosiaalisessa mediassa. Tällä hetkellä yritykset ovat enemmän huolissaan siitä, miten paljon luottamuksellista tietoa vuotaa sen kautta (Gaudin, 2009; Sophos 2010).

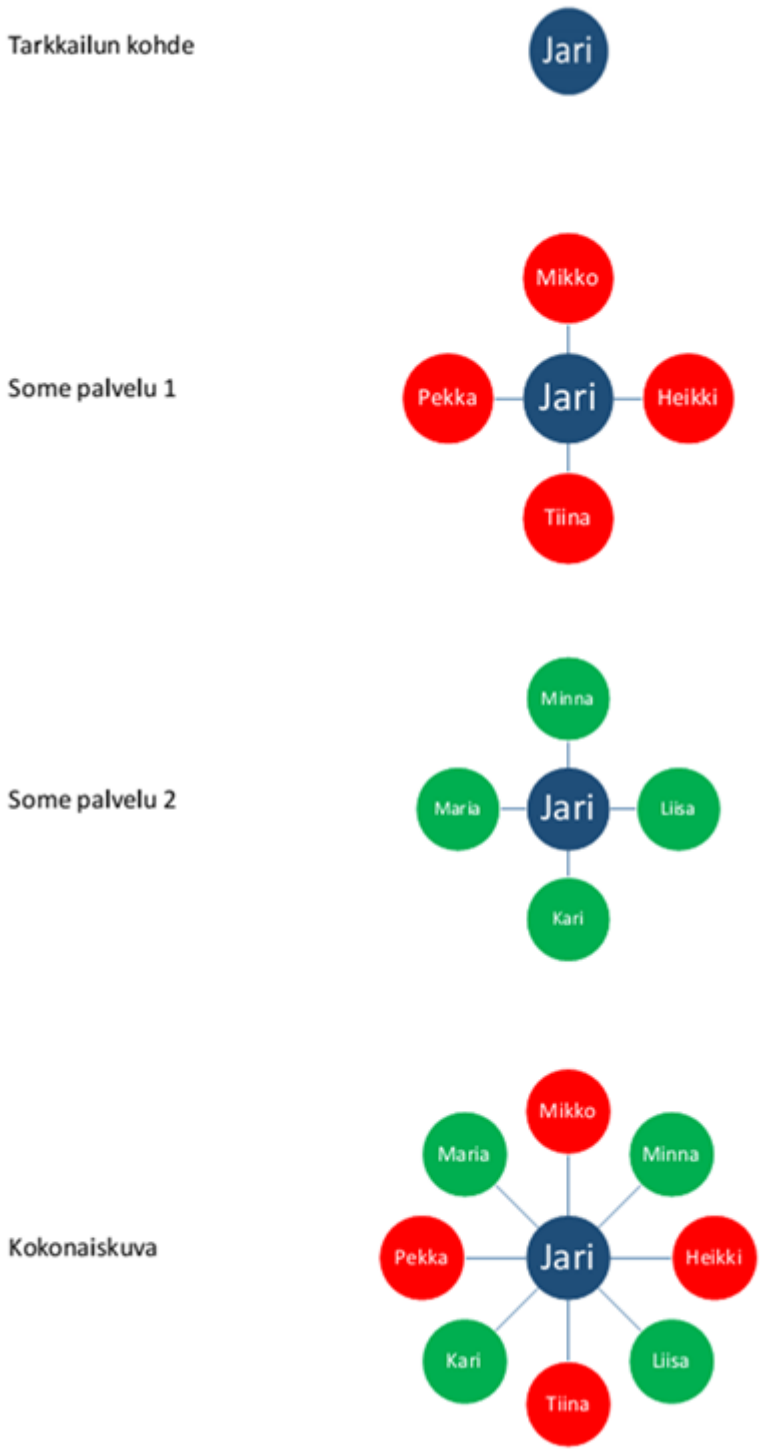
Viimeistään Iso-Britannian ulkomaantiedusteluun MI6 kohdistunut tietovuoto sosiaalisen median kautta osoitti aiheeseen liittyvät riskit sekä tietovuotojen vaarallisuuden (Sophos 2010, 6). Kyseisessä tapauksessa ulkomaantiedusteluyksikön päällikön vaimo julkaisi omassa Facebook –profiilissaan hyvin yksityiskohtaisia tietoja perheen elämästä, asuinpaikasta, ystävistä ja lomanviettopaikoista. Samalla profiilin tietosuoja-asetukset olivat käytännössä avoimet. Profiilin kautta oli mahdollista saada esimerkiksi kuvat koko yksikön päällikön perheestä. Profiilin kautta saatavilla ollut informaatio aiheutti suoranaisen hengenvaaran, ei pelkästään yksikön päällikölle, vaan koko perheelle. Lisäksi tietovuoto vaaransi myös perheen lähipiirin, jossa oli henkilöitä, jotka työskentelivät salaisessa palvelussa. (Lewis 2009.)

Edellä kuvatussa tapauksessa korostuu hyvin kappaleessa kuusi (sosiaalisen median riskien taustalla vaikuttavat tekijät) käsiteltyjä aiheita. Lisäksi se osoittaa sen, että sosiaalisen median teho tiedustelukanavana perustuu siihen, että sen käyttäjät jakavat itsestään ja toisista mahdollisimman paljon informaatiota.

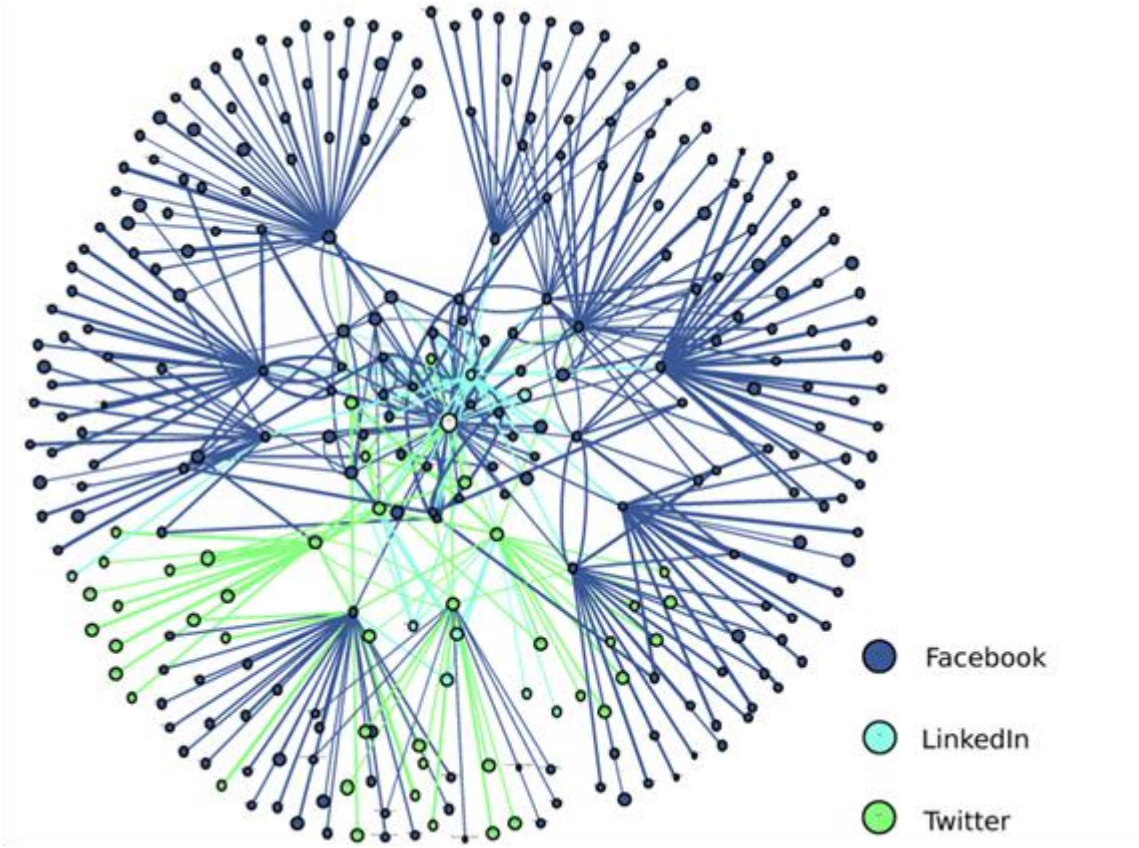
Ennen ihmisten sosiaalinen verkosto määriteltiin pitkälti maantieteellisesti. Tänä päivänä se voidaan määritellä yhtä hyvin myös sähköisten kontaktien kautta. (Appel 2010, 9.) Yhdestä sosiaalisen median profiilista on mahdollista saada hyvin kattava kuva profiilin omistajasta, mutta se kertoo myös erittäin paljon profiiliin liitetyistä toisista käyttäjistä. Käyttäjän tekemät statuspäivitykset, tykkäykset, ladatut valokuvat, mutta myös toisten käyttäjien statuspäivitysten kommentointi luo hyvän henkilökuvan profiilin omistajasta. (Appel 2010, 13.)

Kokonaiskuva esimerkiksi tarkkailun kohteena olevasta henkilöstä muodostuu yhdistämällä eri sosiaalisen median palveluiden kautta saatava tieto. Yhdistämällä esimerkiksi Facebook, Twitter, Linkedin ja Flickr –palveluiden tiedot voidaan luoda erittäin tarkka kuva kohteesta. Lisäksi mahdolliset tietopuutteet yhdessä palvelussa voidaan korvata toisen palvelun tiedoilla. (Varangot 2010.) Lyhyesti sanottuna kontaktisi eri palveluissa kertovat kuka sinä olet.

Sosiaalisen median rooli tiedonhankintakanavana tulee kasvamaan ja siitä onkin tulosssa merkittävä tiedustelun alalaji nimeltä SOCMINT (Social Media Intelligence). Iso-Britannian tiedustelukeskuksen entinen päällikkö Sir David Omand on vaatinutkin, että viranomaisilla tulisi olla turvallisuuden nimissä pääsy Facebookin ja Twitterin kaltaisiin palveluihin. Samaan aikaan Iso-Britannian hallitus suunnittelee esitystä, jossa tiedusteluviranomaisilla olisi reaaliaikainen pääsy esimerkiksi sähköpostiin ja Messenger -viesteihin. (Clare & Sir Omand 2012.)




Kuvio 4: Kokonaiskuvan muodostaminen tarkkailtavasta kohteesta (mukaillen Core-labs.coresecurity.com 2008).




Kuva 7: Esimerkki Exomind ohjelmalla luotu kokonaiskuva kohteesta yhdistämällä Facebookin, Linkedinin ja Twitterin tiedot (Orlicki 2008).

Seuraavissa kappaleissa on kuvattu tiedonhankintaa kahdesta tunnetusta sosiaalisen median palvelusta. Käytetyt esimerkit ovat yksinkertaisia, mutta niiden periaatteita voidaan soveltaa monimutkaisemmissa tiedonhakuskenaarioissa. Kyseiset esimerkit eivät ole ainoita tapoja hakea tietoa sosiaalisesta mediasta, vaan eri toimintaperiaatteisiin perustuvia menetelmiä on niin paljon, ettei niiden tyhjentävä esittely ole mahdollista. Lisäksi työhön liittyvät eettiset kysymykset sekä lainsäädäntö rajoittavat eri menetelmien esittelyjä.

## 7.1 Case: Facebook ja tiedonhalu Facebook GraphAPI:n avulla

Facebook GraphAPI on osa Facebookin sovelluskehittäjille tarkoitettua ohjelmaa, jonka tarkoituksena on tarjota yhteinen rajapinta kaikille, jotka haluavat käyttää Facebookin tarjoamia palveluita omilla verkkosivuillaan tai haluavat luoda omia sovelluksia Facebookin sisälle (Facebook Developers 2012). Kaiken ytimenä toimii Facebookin Social Graph, joka yhdistää kaikki Facebookin elementit toisiinsa. Elementit voivat olla esimerkiksi ihmisiä, palveluita, ohjelmia, tykkäyksiä tai valokuvia. (Facebook Developers 2012.)

GraphAPi mahdollistaa tiedon hakemisen Facebookista ja haetun tiedon esittämisen esimerkiksi omilla verkkosivuilla. GraphAPI perustuu siihen, että kaikilla Facebookissa olevilla objekteilla (henkilöt, kuvat, statukset) on oma yksilöllinen tunnus eli ID. Jos tietää objektin ID -tunnuksen, sen tiedot on mahdollista hakea kirjoittamalla selaimen osoitekenttään:

`https://graph.facebook.com/<OBJECT_ID>`
(mukaillen Facebook Developers 2012.)

Esimerkiksi Helsingin kaupungista on olemassa oma julkinen Facebook profiili, jonka ID on 278073387879. Kirjoittamalla selaimen osoitekenttään:

`https:graph.facebook.com/278073387879`

Antaa seuraavanlaisen JSON vastauksen:


```
{
              "name": "Helsinki",
              "is_published": true,
              "website": "http://en.wikipedia.org/wiki/Helsinki
              http://fi.wikipedia.org/wiki/Helsinki",
              "username": "helsinki.finland",
              "founded": "1550",
              "description": "Helsinki is the capital city of Finland. Helsinki is the
              largest city in Finland, approx. 600,000 people live in Helsinki, and over
              1,300,000 live in the Helsinki metropolitan area.",
              "about": "This page is for people to share stories, secrets or anything
              they want about the amazing city that is Helsinki. Get involved - spread
              the word - Helsinki is the place to be! (Please, Respect the page. No unso-
              licited advertisement or spam.)",

              "talking_about_count": 93,
              "category": "Public places",
              "id": "278073387879",
              "link": "http://www.facebook.com/helsinki.finland",
              "likes": 10504,
              "cover": {
                            "cover_id": "10150904501912880",
                            "source": "http://sphotos-d.ak.fbcdn.net/hphotos-ak-
                            snc7/s720x720/392462_10150904501912880_1758858646_n.jpg",
                            "offset_y": 0
              }
}
```

GraphAPI mahdollistaa myös tiedon hakemisen suoraan Facebookin sisältämästä julkisesta tiedosta (Facebook Developers 2012). Haku tapahtuu komennolla:

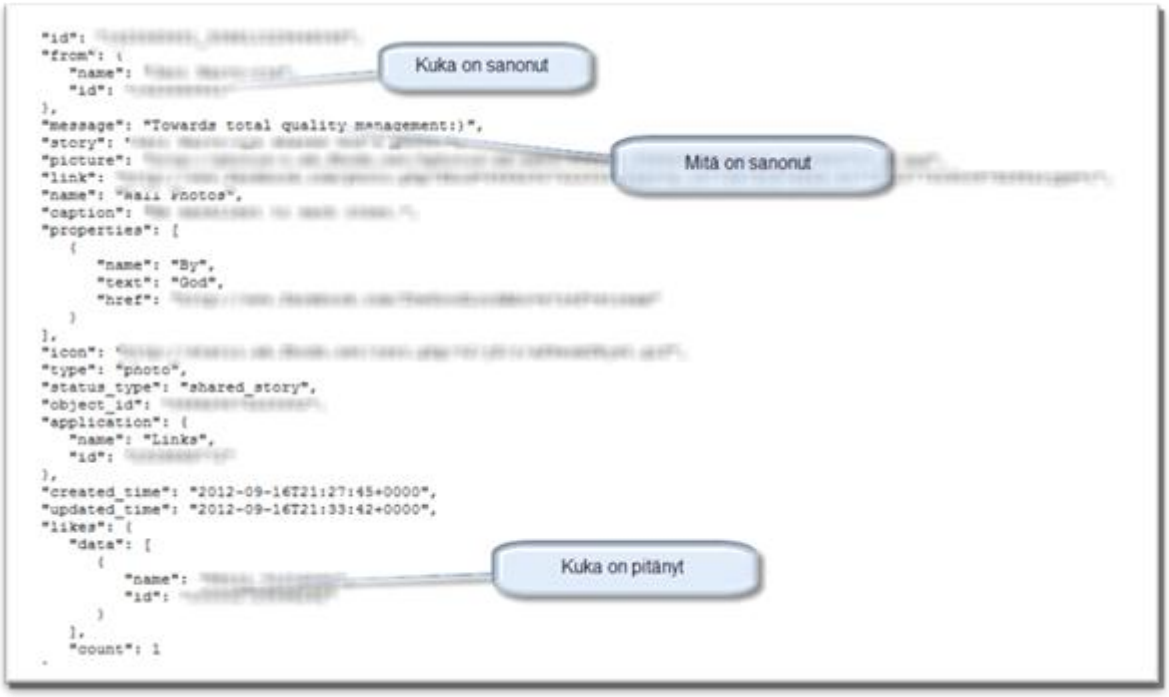
```
https://graph.facebook.com/search?q=<QUERY>&type=<OBJECT_TYPE>
```

Esimerkiksi, jos halutaan hakea Facebookista riskienhallintaan liittyviä julkisia tietoja, haku voisi tapahtua sanoilla *risk* ja *management*. Silloin komento olisi:

```
https://graph.facebook.com/search?q=Risk&q=Management
```

Tuloksena on pitkä JSON –listaus hakua vastaavista tuloksista. Ohessa lyhyt osa:


Kuva 8: Otanta JSON vastauksesta hakusanoille risk management.




Kuva 9: JSON vastauksen tulkinta.

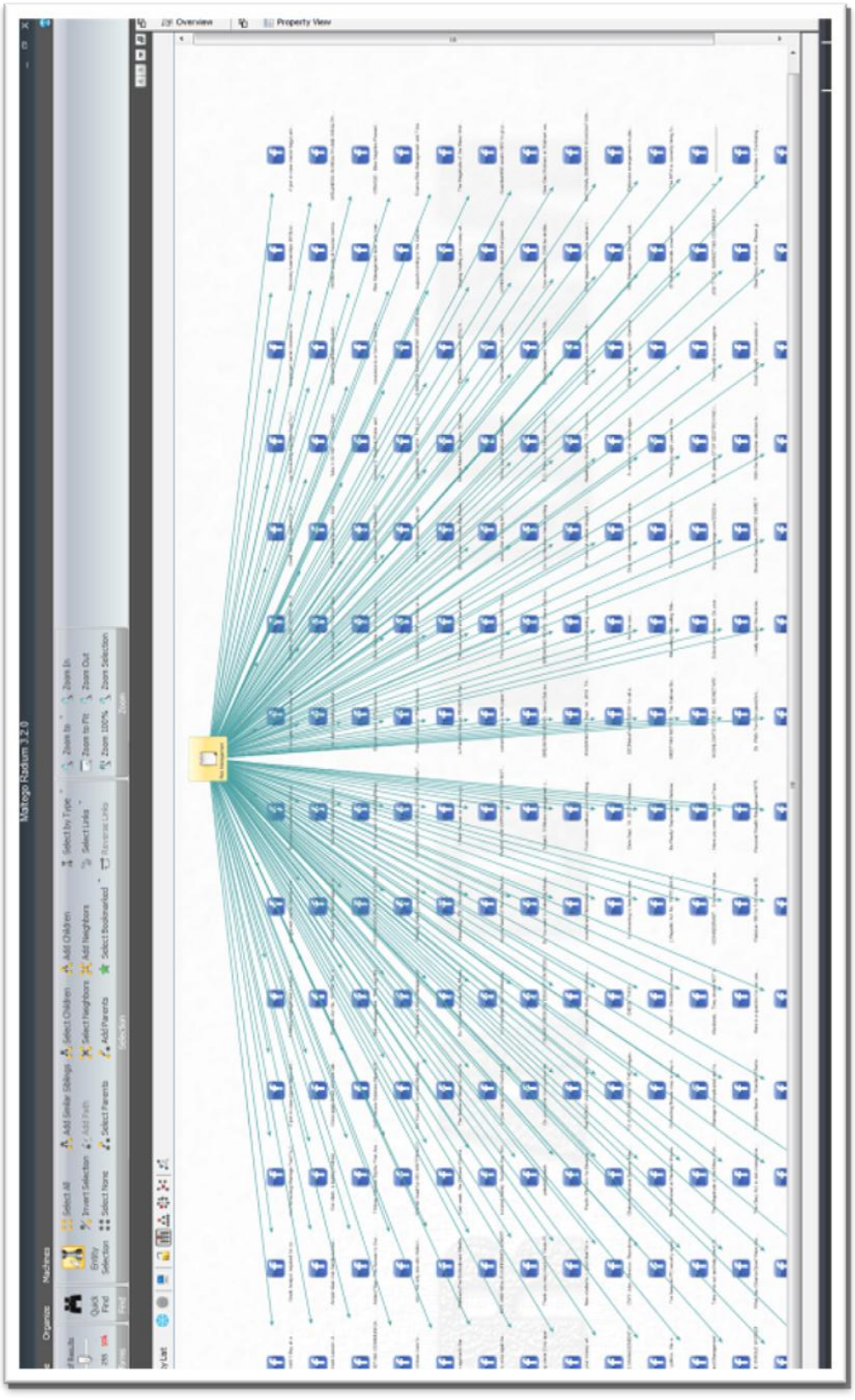
Tiedustelun kannalta mielenkiintoista on se, että haku näyttää myös käyttäjien tiedot. Kuva 8 todistaa, että hakutuloksissa on myös käyttäjän nimi ja yksilöllinen ID. Hakutuloksista näkyy sen lisäksi mitä on sanottu, kuka on sanonut ja kuka on pitänyt sanomisesta (kuva 9). (Adrew-Nohawk.com 2012.)

### 7.1.1 Esimerkki tiedon hakemisesta ja käsittelystä julkisista profiileista

Käyttämällä edellä kuvattua GraphAPI:n hakuominaisuutta kuka tahansa voi hakea informaatiota Facebookin julkisista profiileista. Ketjuttamalla hakuja, käyttämällä vaihtelevia hakusanoja ja keskittämällä hakuja esimerkiksi tietylle maantieteelliselle alueelle organisaatiot voisivat edelleen tehostaa informaation keräämistä. On hyvä muistaa, että tällä tavalla kerätty informaatio on vielä raakadatana ja se vaatisi vielä paljon jatkokäsittelyä. Tässä esimerkissä raakadata olisi taulukoitava, jäsenneltävä ja analysoitava, jolloin prosessi voi muodostua liian raskaaksi ja aikaa vieväksi. (AdrewNohawk.com 2012.)

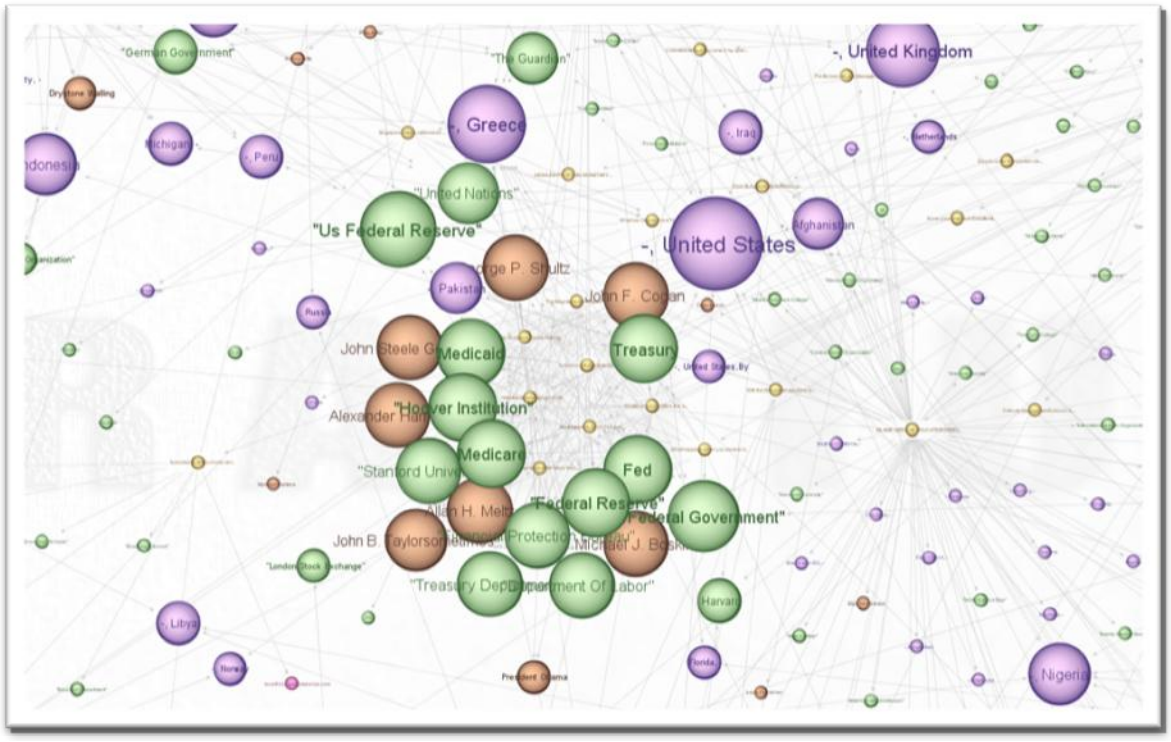
Yksi mahdollisuus prosessin nopeuttamiseksi on sen automatisointi. Tässä työssä prosessin nopeuttamista testattiin Maltego -ohjelmalla. Maltego on Eteläafrikkalaisen Paterva nimisen yrityksen kehittämä ohjelmisto, joka keskittyy tiedon hankintaan avoimista lähteistä. Sen avulla on mahdollista hakea tietoa useista eri lähteistä, louhia haettua tietoa sekä esittää tietoa visuaalisesti. (Paterva 2012.) Maltegossa on graafinen käyttöliittymä, jonka ansiosta ohjelman käytön aloittaminen on helppoa. Lisäksi ohjelma on joustava ja helposti laajennettavissa. Se sallii myös oman ohjelmakoodin ajamisen, joten käytännössä sen käyttöä rajoittaa ainoastaan mielikuvitus ja ohjelmointitaidot. Ohjelmasta on saatavissa ilmainen ja kaupallinen versio. (Paterva 2012.)

Tiedon hakeminen tapahtui ohjelmoimalla Maltego hakemaan tietoa Facebookin GraphAPI:n hakutoiminnolla. Hakusanoina käytettiin sanoja risk ja management. Kuva 10 esittää kuvankaappauksen haun tuloksista. Kuvassa näkyy kaikki avoimista profiileista löytyvät lauseet tai kommentit, joissa käytetään sanoja Risk Management yhdessä tai erikseen. Tämän jälkeen aineistoa olisi mahdollista käsitellä eteenpäin esimerkiksi hakemalla aineistosta henkilöt lauseiden taustalla. Kuvassa 11 on kuvankaappaus pienestä osasta aineistoa, jossa on tehty juuri näin.



Kuva 10: GraphAPI haku Maltegon avulla.

Kuva 11: Aineistosta eritelty henkilöiden nimet ja profiilikuvat.




Kuva 12: Painotettu näkymä aineistosta.

Aineistoa voidaan käsitellä edelleen esimerkiksi painottamalla haluttuja kriteereitä. Kuvassa 12 on kuvankaappaus aineistosta. Aineistossa on käytetty sellaista painotusta, jossa korostuu se, miten tiivisti hakutulokset linkittyvät toisiinsa. Periaate on, että mitä suurempi pallo, sitä mielenkiintoisempi kohde on.

### 7.1.2 Esimerkki tiedon hakemisesta suljetuista profiileista

Edellisen kappaleen esimerkistä on huomioitava, että haku tapahtui ainoastaan julkisista tiedoista. Jos käyttäjä on ollut tietoinen Facebookin yksityisyysasetuksista, informaation kerääminen kyseisellä tavalla ei olisi mahdollista. Lisäksi Facebook on rajoittanut GraphAPI:n hakuominaisuuksia siten, että haku valtaosasta profiilin tiedoista vaatii erillisen valtuutuksen (Authorization). Hyväksytystä valtuutuksesta käytetään termiä Access Token, jota eri ohjelmat ja palvelut käyttävät Facebookin sisällä osoittaakseen pääsyluvan valtuutuksen vaativaan tietoon. Käytännössä tämä tarkoittaa sitä, että kaikkea Facebook –profiilissa näkyvää informaatiota, ei voi hakea GraphAPI:n avulla ilman erillistä valtuutusta. (Facebook Developers 2012.)

| | |
|---|---|
| Friends | Permissions |
| News feed | Photo Tags |
| Profile feed | Photo Albums |
| Likes | Video Tags |
| Movies | Video Uploads |
| Music | Events |
| Books | Groups |
| Notes | Checkins |

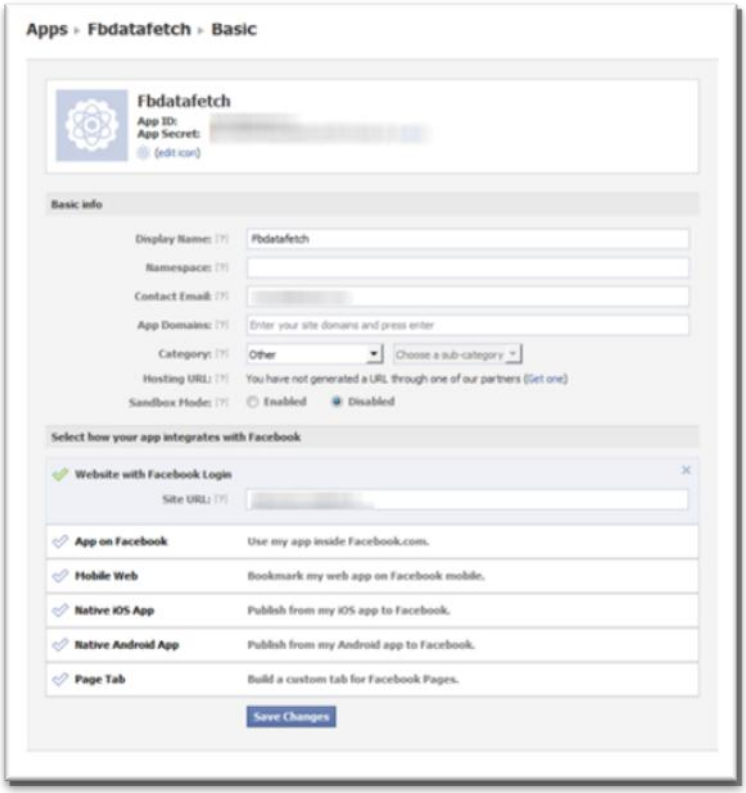
Taulukko 8: Mitkä tiedot vaativat erillisen hyväksynnän (mukaillen Facebook Developers 2012).

Esimerkkinä käytetään kuvitteellista yritystä, jota vastaan verkkorikollisten ryhmittämä suunnittelee kohdistettua hyökkäystä yrityksen tuotekehitystietojen varastamiseksi. Yksi mahdollinen hyökkäysreitti on sosiaalisen median avulla tapahtuva tunkeutuminen. Verkkorikolliset ovat kartoittaneet Facebookista yrityksen palveluksessa olevia henkilöitä, mutta kyseisten henkilöiden Facebook -profiilin asetukset ovat sellaiset, että profiilin näkevät vain kaveripiiriin kuuluvat, jolloin rikolliset eivät näe henkilöiden sosiaalista verkostoa. Tämä vaikeuttaa sopivan hyökkäysreitin valintaa, joten heidän tulee keksiä keino kiertää Facebookin yksityisyysasetukset.

Toimiva vaihtoehto on hyödyntää se tosiseikka, että monet hyväksyvät kaveriksi henkilöitä, joita eivät todellisuudessa tunne. Jos tämä onnistuu, se ei poista sitä ongelmaa, että verkkorikollinen ei silti voi hakea automaattisesti kaikkea profiilissa olevaa informaatiota ilman erillistä hyväksyntää. Toinen tapa kiertää valtuutuksen ongelma on laatia ohjelma, jolla on jokin näennäinen viihteellinen tarkoitus, esimerkiksi viikkohoroskooppi. Sen jälkeen ohjelma yritetään ujuttaa kohteena olevalle henkilölle niin, että hän edes kokeilisi sitä ja antaisi näin oh-

jelmalle valtuutuksen käyttää kohteen profiilissa olevia tietoja. Tässä tapauksessa ohjelma toimii eräänlaisena troijalaisena, jolla kierretään Facebookin yksityisyysasetukset.

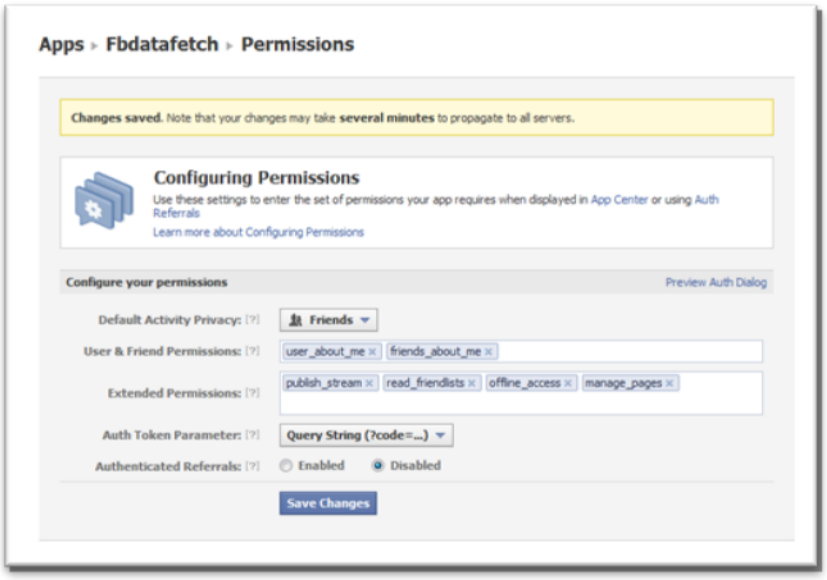
Esimerkin testaamista käytännössä, kokeiltiin luomalla yksinkertainen ohjelma nimeltä **FBdatafetch**. Sen tarkoituksena oli kuvata troijalaisena toimivaa ohjelmaa. Ensimmäiseksi luotiin ohjelma Facebookin kehittäjille tarkoitetun sivuston kautta (kuva 13).




Kuva 13: Troijalaisena käytettävä ohjelma.

Tämän jälkeen määriteltiin, mitä tietoja ohjelma tarvitsee käyttäjältä. Tavoitteena oli luoda graafinen kuva kohteena olevan Facebook profiilin sosiaalisesta verkostosta, joten ohjelman asetuksiin määriteltiin vaatimus profiilin kaveritietojen käytöstä (Kuva 14).

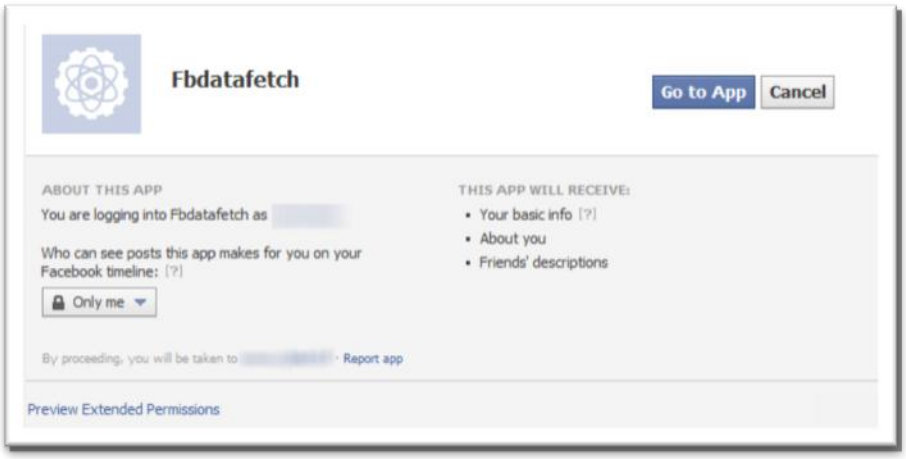
Seuraavaksi luotiin yksinkertainen WWW-sivu, joka vaatii kirjautumisen Facebookin avulla (kuva 15 ja kuva 16). Kirjautumisen jälkeen Fbdatafetch –ohjelma pyytää kirjautujalta lupaa käyttää profiilin tietoja (kuva 17). Käyttäjän suostuessa tähän, ohjelma saa valtuutuksen eli Access Tokenin. Tätä valtuutusta ohjelman laatija voi käyttää hyväksi hakiessaan tietoja kohteena olevasta käyttäjästä.




Kuva 14: Fbfatafetch sovelluksen oikeudet.

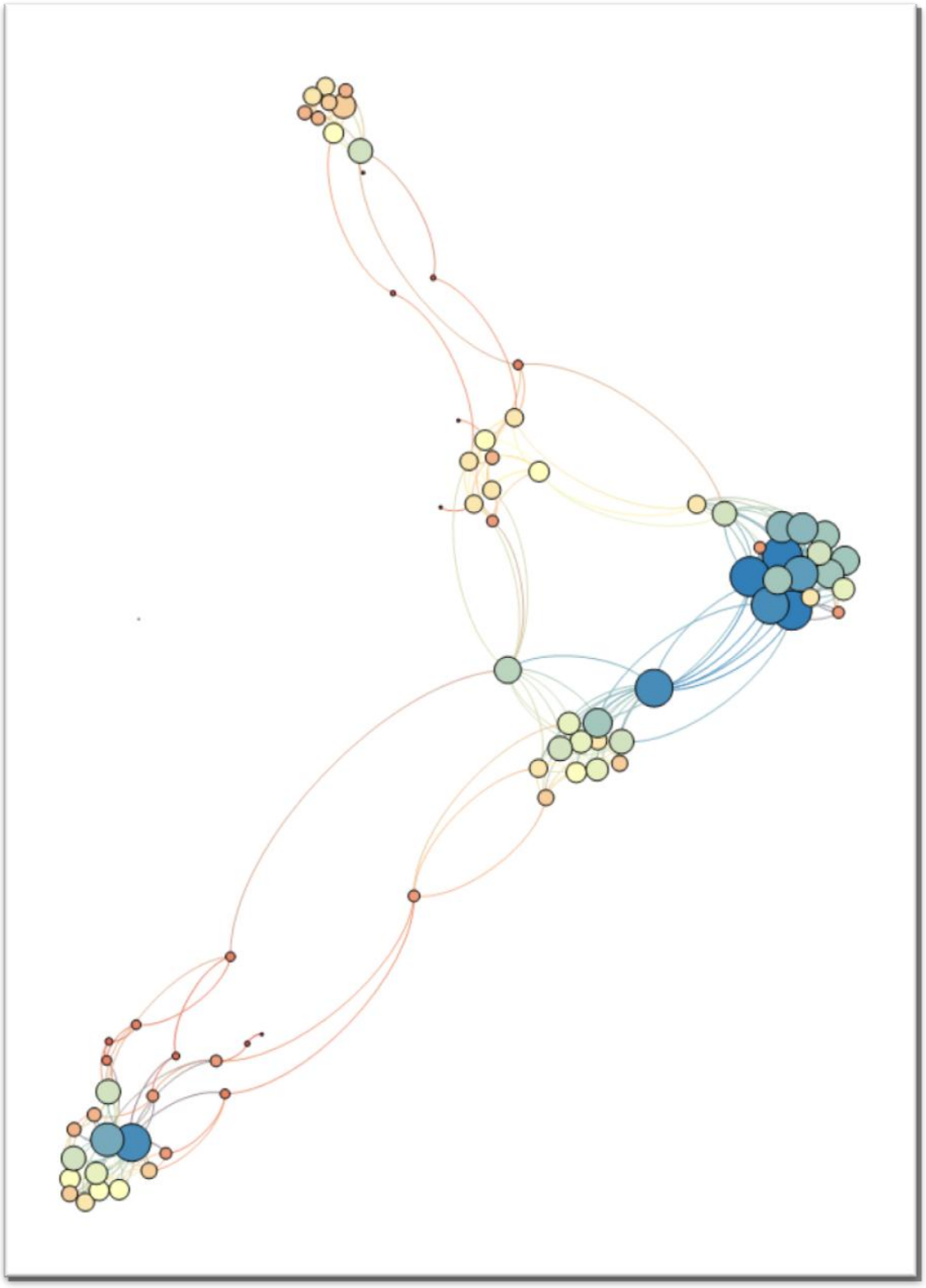

Kuva 15: Yksinkertainen WWW-sivu, johon kirjaudutaan Facebookin avulla.


Kuva 16: Kirjautumisnäkymä.




Kuva 17: Ohjelma pyytää lupaa käyttäjätietoihin.

Esimerkkiohjelman avulla haettiin raakadataa oikeasta Facebook -profiilista, profiilin omistajan suostumuksella. Tämän jälkeen saatua dataa käsiteltiin Gephillä, joka on avoimen lähdekoodin perustuva tiedon mallintamiseen ja käsittelyyn tarkoitettu ohjelmisto (Gephi.org 2012). Kohteena olleen Facebook –profiilin sosiaalisesta verkostosta (kaveriverkosto) luotiin malli, joka näkyy kuvassa 18.



Kuva 18: Facebook -profiilin sosiaalisesta verkostosta luotu kuva.

Kuvassa jokainen pallo edustaa yhtä henkilöä, ja kaarevat viivat kuvaavat sitä, miten henkilöt liittyvät toisiinsa. Pallon koko kertoo sen, miten verkostoitunut kyseinen henkilö on. Kappaleen alussa oli kuvitteellinen skenaario verkkorikollisten suunnittelemasta kohdistetusta hyökkäyksestä. Heille kuvassa 22 esiintyvä malli antaa mahdollisuuden kohdistaa hyökkäyksen seuraavat vaiheet sellaiseen verkoston kohtaan, jossa se tuottaa mahdollisimman hyvän lopputuloksen. Jos verkkorikollinen haluaa kohdistaa hyökkäyksen tiettyä henkilöä kohtaan, tämä ei välttämättä pyri kontaktiin suoraan kohteen kanssa. Hyökkäys voi tapahtua myös johonkin kohteen kaveripiiriin kuuluvaan, jolloin lähipiiri toimii siltana varsinaiseen kohteeseen.

## 7.2 Case: Twitter ja tiedonhaku Twitter API:n avulla

Twitterin käyttäjät julkaisevat päivittäin yli 200 miljoonaa tweettiä (blog.twitter.com 2011), joten yksi mielenkiintoisimmista syistä tiedonhakuun Twitteristä on saada selville mitä ihmiset puhuvat juuri tällä hetkellä (Russell 2011, 9). Saatua informaatiota voidaan käyttää hyväksi monella eri tavalla. Esimerkiksi yritys voi seurata uuden tuotteensa saamaansa vastaanottoa seulomalla twitteristä tuotetta käsitteleviä viestejä. Toisen ääripään esimerkkinä voidaan pitää Irania, joka käytti twitteriä tehokkaasti jäljittäessään Iranin opposition edustajia vuoden 2009 mellakoiden yhteydessä (Diamond 2010, Smythin 2011 mukaan).

Myös Twitterissä sisältää ohjelmistosuunnittelijoille suunnatun TwitterAPI:n, jonka avulla sovelluskehittäjä voivat käyttää hyväksi Twitterin sisältämää informaatiota (dev.twitter.com 2012). Twitter Api jakaantuu neljään osa-alueeseen, joista tiedonhaun kannalta mielenkiintoisimmat osa-alueet ovat **SearchAPI**, **RESTAPI** ja **StreamingAPI** (dev.twitter.com 2012).

**SearchAPI:n** avulla voidaan hakea Twitterin sisällöstä esimerkiksi tweettejä, jotka sisältävät valitut hakusanat. Tai sitten haku voi kohdistua tiettyyn käyttäjään tai jonkun käyttäjän tweetteihin (dev.twitter.com 2012). SearchAPI:n hakutoimintoja on rajoitettu niin, että se sisältää ainoastaan viimeisimmät tweetit 6-9 päivän ajalta. Lisäksi Twitter rajoittaa SearchAPI:n avulla tehtyjen hakujen monimutkaisuutta ja tiheyttä. Twitter suosittelee käyttämään hakutoiminnossa korkeintaan 10 sanaa ja useisiin peräkkäisiin hakuihin tulisi käyttää RESTAPI:a (dev.twitter.com 2012).

SearchAPI:n avulla voidaan tietoa hakea suoraan kirjoittamalla hakukomento suoraan selaimen osoitekenttään. Komento on:

```
http://search.twitter.com/search.json?q=%<Searchquery>
```

Esimerkiksi hakusanoilla risk management komento olisi:

```
http://search.twitter.com/search.json?q=%40riskmanagement
```

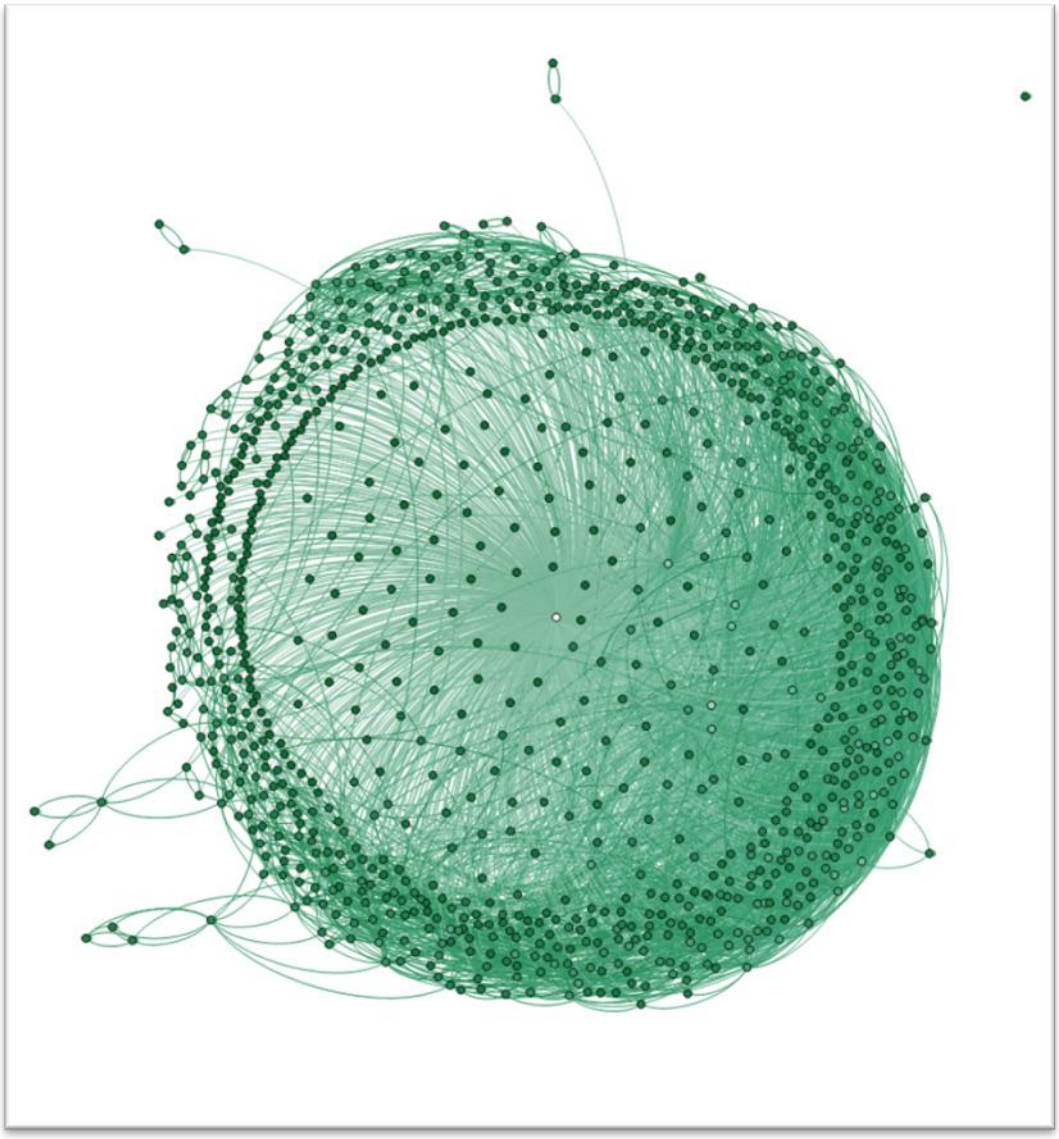
Tuloksena on JSON vastaus, joka näyttää haun tulokset.

**RESTAPI** mahdollistaa pääsyn joihinkin Twitterin ydintoimintoihin, kuten statuspäivityksiin ja käyttäjien tietoihin. RESTAPI:n avulla on mahdollista esimerkiksi muodostaa kuva jonkun Twitterin käyttäjän seuraajista. Lisäksi RESTAPI mahdollistaa suoran vuorovaikutuksen Twitterin kanssa. Sen avulla on mahdollista tweetata suoraan tai vastata toisten tweetteihin. (dev.twitter.com 2012.)

**StreamingAPI** on tarkoitettu Twitterin raskaaseen käyttöön. Jos tarkoituksena on tiedonlouhinta tai tutkimus, joka vaatii monimutkaisia hakutoimintoja kuten maantieteellisten sijaintien selvittäminen, se onnistuu parhaiten StreamingAPI:n avulla. (dev.twitter.com 2012.)

Facebookista poiketen Twitter ei rajoita hakutuloksia millään tavalla. Käytännössä tämä tarkoittaa, että kaikki informaatio, minkä näkee Twitterissä, on mahdollista hakea TwitterAPI:n avulla. Twitter suojautuu väärinkäytöksiltä rajoittamalla hakujen määrää. Esimerkiksi RESTAPI:ssa ohjelmat jaetaan tunnistettuihin (authenticated) ja tunnistamattomiin (unauthenticated). Tunnistamattomilla ohjelmilla voi suorittaa 150 hakutoimintoa tunnissa. Tunnistetuilla määrä on 350 hakutoimintoa tunnissa. (dev.twitter.com 2012.)

Tiedonhakuun twitteristä on kehitetty valmiita ohjelmia, jotka käyttävät hyväksi edellä kuvattuja käyttöliittymiä. Tässä työssä tiedonhakua Twitteristä kokeiltiin NodeXl -ohjelmalla. NodeXl on Excel 2007/2010 taulukkolaskentaohjelman lisäosa, jonka avulla on mahdollista kerätä, käsitellä ja julkaista dataa sosiaalisesta mediasta (Socialmedia Research Foundation 2012). NodeXl on tarkoitettu sosiaalisten verkostojen tutkimiseen, mutta sen ominaisuuksia on mahdollista käyttää hyväksi myös tiedonhankinnassa.



Kuva 19: Yhdestä Twitter -tilistä louhittua tietoa. Käsitelty NodeXl:llä ja Gephillä.

Kuvassa 19 on lopputulos esimerkistä, jossa NodeXl:n avulla haettiin raakadataa yhdestä erään maailmanlaajuisesti tunnetun henkilön Twitter tilistä. Haku rajattiin 1000 ihmiseen, jotka seuraavat kyseistä Twitter -tiliä ja mahdollisesti kommentoivat tweettauksia. Koska kyseessä oli tunnistamaton ohjelma, Twitterin säännöt rajoittivat datan keräämistä 150 hakuun tunnissa. Haun jälkeen aineiston käsittelyä jatkettiin Gephi -ohjelmalla ja siitä muodostettiin kuva, jossa näkyy kaikki 1000 henkilöä ja heidän suhde kohteena olleeseen Twitter -tiliin.

# 8 Suojautuminen sosiaalisen median kautta tapahtuvalta tiedonhankinnalta

Tiedonhankinnalta suojautuminen edellyttää organisaatiolta uudenlaista lähestymistapaa sosiaaliseen mediaan, tiedon hallintaan sekä tietoturvallisuuteen. Esimerkiksi malli, jossa yritykset estävät työntekijöiden pääsyn sosiaalisen mediaan saattaa osittain toimia, mutta kaiken taustalla vaikuttaa vanha ajatusmaailma, jonka mukaan tietoturva on staattinen tapahtuma (Kelly 2008; Sophos 2010; Ernst & Young 2011). Totaalisen kiellon ongelmana on se, että erilaiset kannettava laitteet, kuten älypuhelimet, ovat yleistyneet työntekijöillä ja he käyttävät niitä myös työaikana. Käytännössä työntekijöillä on vapaa pääsy sosiaalisen mediaan rajoituksista huolimatta. (Ernst & Young 2011.)

Sosiaalisen median käytön totaalinen kieltäminen voi itsessään aiheuttaa riskin ja vahinkoa organisaatiolle. Keväällä 2012 julkaistiin uutinen, jossa verkkorikolliset olivat luoneet Naton amiraali James Stavridista väärennetyn valeprofiilin Facebookin ja sen avulla saaneet tietoa Iso-Britannian sotilasviranomaisista ja puolustusministeriön virkamiehistä (Lewis 2012). Valeprofiilin avulla vakoojat pystyivät luomaan kuvan amiraali Stavridisin sosiaalisesta verkostosta. Vaikka mitään salaista sotilastietoa ei tiettävästi vuotanut, sosiaalisen verkoston avulla oli mahdollista luoda laajat profiilikuvaukset uusista vakoilun kohteista. Tapauksen tultua ilmi on Nato muuttanut käytäntöjään sellaisiksi, että nykyään sotilasliiton korkeimmilla upseereilla on omat sivut sosiaalisessa mediassa. (Lewis 2012.) Näin Nato voi kontrolloida, mitä tietoa sosiaalisessa mediassa liikkuu.

Tietoturvallisuus on perinteisesti koettu riittäväksi, jos organisaatioiden käytössä on palomuurit, pääsynhallinta ja kaikkea ohjaa organisaation tietoturvapolitiikka (mukaillen Kelly 2008). Kohdistetut hyökkäykset ovat viimeistään osoittaneet sen, että ajattelumalli, jossa tietoriskit estetään, ei enää toimi nykyaikaisessa tietoyhteiskunnassa (Alridge 2012). Suojautuminen tiedonhankinnalta alkaa siitä, että hyväksytään täydellisen estämisen mahdottomuus.

Tämä ei tarkoita, että esimerkiksi yritysten tulisi hyväksyä tilanne, jossa sen luottamuksellista tietoa vuodetaan Facebookin kautta. Suojautuminen alkaa siitä, että tapaukset pyritään ennaltaehkäisemään. Sen lisäksi organisaatio alkaa seurata aktiivisesti siitä liikkuvaa informaatiota ja mahdollinen tietovuoto pyritään havaitsemaan mahdollisimman aikaisessa vaiheessa. (mukaillen Kelly 2008, Alridge 2012.)

Ennaltaehkäisy lähtee liikkeelle riskienhallinnan kautta. Sosiaalisen median palveluiden käyttöä arvioidaan siihen liittyvien riskien ja palveluiden kautta saatava hyödyn välisenä suhteena (Vahti 4/2010, 25). Riskienhallinnassa on hyvä tiedostaa se, että tietoturvallisuuteen liittyy haavoittuvuuden käsite. Haavoittuvuuksia on lukemattomia ja niitä havaitaan koko ajan. Mi-

käli organisaatio keskittyy haavoittuvuuksiin ja niiden paikkaamiseen, syö se organisaation resurssit kaikelta muulta. (mukaillen Kelly 2008.)

Organisaatioiden on keskityttävä sellaisiin haavoittuvuuksin, jotka muodostavat sille uhkan. Uhkakuvat vaihtelevat, ja siksi organisaatioiden tulee huomioida aina oman toimialana erityispiirteet (mukaillen Kelly 2008; Aldridge 2011). Painopisteen tulisi olla sellaisissa tekijöissä, jotka aiheuttavat organisaatiolle todellisen riskin. Riskienarvioinnin kautta organisaatio tekee päätöksen, miten se osallistuu sosiaaliseen mediaan vai estääkö se sosiaaliseen mediaan pääsyn työaikana. Päätöksen jälkeen organisaation tulee luoda politiikka, jossa määritellään pelisäännöt sosiaalisen median käytöstä. Politiikan tulee olla linjassa tietoturvapolitiikan kanssa. (Vahti 4/2010, 25–27.)

Tietoturvaohjeiden ja -politiikan suurin haaste on siinä, kuinka saada henkilöstö ymmärtämään ja omaksumaan niihin liittyvät asiat. Henkilöstön on noudatettava useita erilaisia ohjeita, politiikoita ja määräyksiä. Näiden kaikkien muistaminen saati noudattaminen on mahdotonta. Usein myös itse ohjeet ovat sellaisia, että ne eivät vastaa sitä realiteettia missä henkilöstö työtään tekee. (Herley 2009.) Esimerkkinä voidaan mainita verkkosivujen SSL-sertifikaattien virheilmoitukset, kuten varmenteiden vanhentumiset tai todentamisongelmat. Jos virheilmoitukset ovat 100 % vääriä, mikä merkitys on ohjeella, jossa kielletään sellaiselle sivustolle menemisen, joka antaa varmenteen virheilmoituksen? (Herley 2009.)

Henkilöstön tietoisuuden lisääminen ja turvallisuuskoulutus ovat avaintekijöitä sosiaalisen median käytössä ja siihen liittyvien uhkatekijöiden hallinnassa. Koulutusta on annettava koko henkilöstölle ja siinä on käsiteltävä ne periaatteet, missä määrin organisaation tietoa saa kertoa sosiaalisessa mediassa ja missä roolissa henkilöstö esiintyy sosiaalisessa mediassa. (Vahti 4/2010, 28.) Koulutukseen liittyy omat haasteensa. Karjalaisen (2011, 9) mukaan perinteinen henkilöstön koulutus ei toimi tietoturvallisuuden kohdalla. Tietoturva-koulutuksen vaikuttavuuden saaminen halutulle tasolle edellyttää, että koulutuksessa huomioidaan ne syyt, jonka takia henkilöstö noudattaa tai jättää noudattamatta annettuja tietoturvaohjeita. Sen jälkeen koulutusmenetelmiä on muokattava syytä vastaavaksi. (Karjalainen 2011, 10.)

Osa toimivaa sosiaalisen median käyttöpolitiikkaa on sen seuraaminen, mitä organisaatiosta puhutaan sosiaalisessa mediassa. Seurannan järjestäminen ei ole riippuvaista siitä, millä tavoin organisaatio on päättänyt osallistua sosiaalisen mediaan. Se ei voi estää siitä Internetissä käytävää keskustelua. (Scott & Jacka 2011, 23.) Aktiivisella tiedon seuraamisella organisaatio pyrkii muuttamaan asetelmaa, jossa organisaatio olisi passiivinen toimija. Organisaatio hakee itseään koskevaan sellaista informaatiota, joka voisi muodostaa sille uhan. Jos tällaista informaatiota löytyy, organisaation tulee arvioida ne keinot, miten informaatioon voidaan vaikuttaa.

Seurannan suunnittelu aloitetaan kertomalla siihen liittyvät periaatteet tietoturva- tai sosiaalisen median käyttöpolitiikassa (Appel 2011, 131). Politiikan avulla organisaatio tuo henkilöstölleen selkeästi esille sen, että organisaatioon liittyvää informaatiota seurataan Internetissä sekä millä periaatteilla seuranta tapahtuu. Laadukas seuranta ja tiedonhankinta on:

- suunnitelmallista, kattavaa ja asianmukaista,
- liittyy organisaation toimintaan,
- tulokset ovat käyttökelpoisia,
- tarkasti rajattua ja löydökset on todennettavissa,
- on varmistettu, että aineistossa ei ole virheitä (väärät hälytykset)
- tiedot ovat ajantasalla, aineisto on päivätty ja
- noudattaa voimassa olevaa lainsäädäntöä.
  (mukaillen Appel 2011, 149.)

Vaikka tässä työssä lainsäädäntö on rajattu käsiteltävien aiheiden ulkopuolelle, etenkin tiedon keräämisessä tulee huomioida, että se ei ole ristiriidassa henkilötietolain (523/1999), sähköisen viestinnän tietosuojalain (516/2004) ja lain yksityisyyden suojasta työelämästä (759/2004) kanssa. Henkilötietolain (523/199) 5 §:n, 6 §:n ja 9 §:n mukaan rekisterinpitäjän on meneteltävä huolellisesti, käytettäviä luotettavia tietolähteitä ja käsiteltävä vain tarpeellisia henkilötietoja. Lisäksi lain yksityisyyden suojasta työelämästä (759/2004) 4 §:n mukaan työnantajan tai tämän edustaja tulee kerätä henkilötietoja työntekijältä itseltään. Sähköisen viestinnän tietosuojalaki (516/2004) 4 § määrittelee verkkosivujen selailusta kertyvät tunnistamistiedot luottamuksellisiksi. Tietosuojavaltuutetun toimisto (2006) tarkentaa edellä olevia lain asettamia vaatimuksia seuraavasti:

> *”Jos työnantaja tai tämän edustaja ainoastaan etsii ja saattaa omaan tietoonsa tietoverkoissa olevaa tietoa ilman että työnantaja kerää, tallettaa tai muutoin käyttää näitä tietoverkosta hankkimiaan tietoja työntekijää tai työnhakijaa koskevassa päätöksenteossa, jää tällainen käsittely henkilötietolain ja työelämän tietosuojalain soveltamisen ulkopuolelle.”*
> (Tietosuojavaltuutetun toimisto 2006.)

# 9 Pohdintaa

Verkkotiedustelu on erittäin laaja kokonaisuus ja tämä työ edustaa siitä hyvin pientä ja tarkkaan rajattua osaa. Tiedonhankinnan kohteeksi valitsin sosiaalisen media sen ajankohtaisuuden vuoksi. Samalla periaatteella valitsin myös Facebookin ja Twitterin. On hyvä muistaa, että sosiaalinen media on paljon muutakin kuin pelkästään Facebook ja Twitter. Tarkastelun kohteena olisi voinut olla esimerkiksi joku toinen sosiaalisen median palvelutarjoaja, jolloin työn tuloksetkin olisivat olleet erilaiset.

Tutkimuksen alku noudatti hyvin laadullisen tutkimuksen kriteereitä sekä toimintatutkimuksen periaatteita. Alkuperäinen ajatus oli tutkia passiivista tiedonhankintaa sosiaalisessa mediassa. Työskentely tapahtui koko ajan oikeassa ympäristössä, jossa aineistoa arvioitiin ja testattiin käytännössä koko ajan. Tutkimuksen edetessä työ alkoi muotoutua työssä esitettävän kahden tutkimuskysymyksen ympärille. Kuten kappaleessa kolme mainitaan, tässä työssä toimintatutkimus tulee ymmärtää enemmän tutkimusstrategiana kuin itsenäisenä tutkimusmenetelmänä.

Lopullisessa työssä käytetty aineisto on vain murto-osa siitä kokonaisuudesta mitä tämän työn aikana on käsitelty. Ennen tätä työtä olen työskennellyt aiheen parissa jo parin vuoden ajan ja kehittänyt Internetin kautta tapahtuvaa tiedonhankintaprosessia. Kehitystyön aikana aineistoa on kertynyt todella paljon, joten sen hallinta muodostui työn haasteeksi.

Aineiston ja aiheen rajauksessa auttoi kaikkein eniten etukäteen tehdyt päätökset eettisistä periaatteista. Näin kaikki sellainen materiaali, joka voisi rikkoa lainsäädäntöä, suljettiin työn ulkopuolelle. Toisaalta samalla työn ulkopuolelle jäi useita mielenkiintoisia tiedonhankintaan liittyviä skenaarioita.

Kappaleessa 3.2 käsittelin toimintatutkimusta kohtaan esitettyä kritiikkiä. Jälkikäteen tarkasteltuna tätä työtä kohtaan voidaan esittää samaa kritiikkiä, kuin toimintatutkimusta kohtaan on yleisesti esitetty. Työ on tarkasti rajattu, joten voidaanko sitä pitää kattavana otantana? Myös käytettyjä metodeja voidaan kritisoida, kuten myös sitä, että onko teorian ja käytännön yhdistämisessä onnistuttu?

Yksikään tutkimusmenetelmä ei ole täydellinen ja tämä seikka tulee hyväksyä. Tämän työn muodostuminen toimintatutkimukseksi oli tietoinen valinta ja samalla hyväksyttiin siihen liittyvät mahdolliset puutteet. Tässä opinnäytetyössä esitellään oman tiedon mukaan ensimmäistä kertaa sosiaalisen median riskien taustalla vaikuttavia tekijöitä. Työn ei ole tarkoituskaan olla kattava, vaan se toimii lähtökohtana, jota aihepiiriä käsittelevät muut tutkimukset voivat jalostaa, tarkentaa tai kyseenalaistaa. Sama periaate koskee työssä esitettyjä käytännön esi-

merkkejä. Facebookin ja Twitterin kehitystyökalut ovat yleisesti tunnettuja, mutta tässä niitä sovelletaan tiedonhankintaan sekä niiden toimintaperiaatetta esitellään toimintatutkimuksen keinoin.

Facebookin ja Twitterin avulla kuvatut skenaariot ovat yksinkertaisia, mutta toimintaperiaate on sama myös monimutkaisemmissa skenaarioissa. Niin pitkään kun Facebook ei muuta GraphAPI:n toimintaperiaatetta, esimerkkien soveltamista rajoittaa ainoastaan oma mielikuvitus ja ohjelmointitaidot.

Sosiaalisen median ja tietoturvallisuuden suhteen haasteet ovat samat kuin yhteiskunnassa. Maailma muuttuu niin nopeasti, etteivät yritykset tai julkisyhteisöt pysty enää reagoimaan ympäristön tapahtumiin riittävän nopeasti. Tietotekniikan käyttö on muuttunut kulutuskäytöksi, jossa trendit vaihtuvat hyvin nopeasti. Samaan aikaan organisaatioiden tietoturvaorganisaatiot ovat vaikeuksissa resurssien riittävyyden ja sille asetettujen tulostavoitteiden kanssa. Tämä on johtanut siihen, että yritysten tietoturvaosastot ovat koko ajan askeleen jäljessä.

Myös tietoturvallisuuteen liittyvien asenteiden on muututtava. Tietoturvallisuus ei ole staattista toimintaa, joka perustuu virustorjuntaan ja palomuurin käyttöön. Tämä näkyy esimerkiksi siinä, että tietoturvasta vastaavien tulostavoitteita tarkastellaan sen mukaan, miten monta virusta on löydetty tai kuinka usein palomuuri estää laittoman yhteydenmuodostamisen. Lehtiartikkelissa Overcoming America's lost decade of IT security ongelma kiteytyy kaikkein parhaiten:

> *"The Compliance Hawk is that guy who secures his network by checkbox lists. It's the guy who believes that he's 80 percent secure when, in actuality, he's 80 percent patched. It's the guy who measures what percent he's compliant rather than on the percentage reduction in security incidents. It's the guy who thinks his job is done when he's hit all of his compliance metrics.*
> *Now in truth, it isn't entirely this guy's fault. He just fell victim to an industry that told him that if he follows the compliance regime, his job is safe."*
> (Ghosh 2011)

Työn aikana esille nousi vahvasti ajatus, että työntekijöihin ei luoteta, he vuotavat informaatiota tai he ovat laiskoja noudattamaan sääntöjä. Ehkä sosiaalisen median riskien yhteydessä pitäisi esittää myös kysymys mistä johtuu, tai mikä on syy, että työnantajat eivät luota työntekijöihinsä? Olisiko parempi, että sosiaalisen median politiikan yhtenä perusperiaatteena olisi yritysten luottamus omiin työntekijöihin?

# 10 Yhteenveto

Sosiaalinen media on merkittävä osa Internetin web 2.0 aikakautta. Siitä on tullut niin olennainen osa yhteiskuntaa ja ihmisten päivittäistä elämää, että elämä ilman osallistumista sosiaaliseen mediaan on vaikeaa tai peräti mahdotonta. Sosiaalisen median myötä ihmisten tapa käsitellä ja julkaista tietoa on muuttunut. Samalla se on luonut uusia ihmisten yksityisyyteen ja tiedon luottamuksellisuuteen liittyviä riskitekijöitä.

Ensimmäisenä tutkimuskysymyksenä oli, onko sosiaalisen median riskien taustalla sellaisia tekijöitä, jotka edesauttavat sosiaalisen median kautta tapahtuvaa tiedonhankintaa? Kysymyksen tarkastelu aloitettiin soveltamalla neutralisoimistekniikoita. Huomattiin, että neutralisoimistekniikoiden avulla voidaan hyvin selittää sosiaalisen median riskien taustalla vaikuttavia inhimillisiä tekijöitä. Jokaisella on tarve selitellä ja perustella itselleen normien vastainen toiminta. Lisäksi löydettiin kolme tekijää, jotka yhdistävät sosiaalisen mediaan liittyviä riskejä. Nämä tekijät ovat luottamuksen ilmapiiri, sosiaalisuuden tarve ja ”minulla ei ole mitään salattavaa."

Lähestymistapa sosiaalisen median riskeihin poikkeaa aikaisemmista tutkimuksista ja ilmeistesti kyseessä on ensimmäinen kerta, kun sosiaalisen median riskejä on käsitelty niiden taustalla vaikuttavien syiden kautta. Vaikka tämän aihepiirin käsittely edellyttää laajempaa ja syvällisempää tutkimusta, siitä huolimatta tässä työssä on onnistuttu tuottamaan uutta tietoa, jota voidaan soveltaa käytännössä. Esimerkiksi keskittymällä sosiaalisen media riskien taustalla vaikuttaviin tekijöihin on mahdollista päästä ennakoivaan riskienhallintaan, joka huomio nykyiset tunnistetut riskit kokonaisuutena, mutta myös tulevaisuudessa syntyvät uudet uhkatekijät. Lisäksi organisaatiot voivat kohdentaa omaa sosiaalisen median turvallisuuskoulutusta riskien taustalla vaikuttaviin tekijöihin.

Toisena tutkimuskysymyksenä oli se, miten sosiaalista mediaa voidaan käyttää tiedonhankintaan. Kysymykseen haettiin vastausta esittelemällä käytännössä kuinka tietoa voidaan hakea kahden sosiaalisen median palveluntarjoajan, Facebookin ja Twitterin, kehitystyökalujen avulla. Vaikka esimerkit olivat yksinkertaisia ja pelkistettyjä, ne osoittavat hyvin miten helppoa on rakentaa järjestelmä, jonka avulla on mahdollista kerätä, käsitellä ja julkaista informaatiota.

Nämä kaksi tutkimuskysymystä liittyvät toisiinsa siten, että sosiaalisen median käyttö tiedonhankinnassa ei ole mahdollista ilman ensimmäisen tutkimuskysymyksen periaatteita. Kuten aikaisemmin on käynyt ilmi, sosiaalisen median käyttö tiedonhankintaan perustuu siihen, että ihmiset ovat valmiita julkaisemaan itsestään tietoa.

Organisaatioiden keinot suojautua sosiaalisen median riskeiltä ja tiedonhankinnalta lähtevät sen myöntämisestä, että ajatus estämisestä on vanhentunut. Sen jälkeen on tunnistettava todelliset riskit omalle toiminnalleen ja mitoittaa toimet tunnistettujen riskien mukaisiksi. Tärkein keino on ennaltaehkäisy, kuten selkeä ohjeistus, henkilöstön koulutus ja turvallisuustietoisuuden lisääminen.

Tämä opinnäytetyö antaa useita vaihtoehtoja jatkotutkimuksille. Tässä työssä lähtökohtana oli sosiaalisen median kautta tapahtuva tiedonhankinta. Kuten on käynyt ilmi, sosiaalista mediaa voidaan käyttää myös hyökkäysreittinä tai kaapatun tiedon siirtoon hyökkääjälle. Molemmat kohdat ovat erittäin hyviä jatkotutkimuksen lähtökohtia. Myös tiedonhankinnan tarkastelu eri näkökulmasta tuottaisi uutta mielenkiintoista tietoa. Tässä työssä aihetta tarkasteltiin Facebookin ja Twitterin avulla. Jatkotutkimuksissa tarkastelun kohteena voisi olla esimerkiksi hakukoneet.

Kolmantena jatkotutkimuksen kohteena voisi tarkastella syvällisemmin tiedonhankinnalta suojautumista. Tässä työssä aihetta käsiteltiin lyhyesti ja käsittelyn tarkoituksena oli kyseenalaistaa vallitseva ajatus estävästä tietoturvasta ja herätellä organisaatioita tarkastelemaan omaa tietoturvapolitiikkaa ja sosiaalista mediaa uudesta näkökulmasta. Jatkotutkimuksena ennaltaehkäisevän prosessin luominen sekä aktiivisen valvontajärjestelmän rakentaminen konkreettiseen organisaatioon tuottaisi aihepiiriä syventävää tietoa.

Lähteet

Acquisiti, A., Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Viitattu 15.9.2012.
http://blues.ius.cs.cmu.edu/ralph/Publications/acquisti-gross-facebook-privacy-PET.pdf

Aldridge, J. 2012. Remediating Targeted-threat Intrusions. Viitattu 20.8.2012.
http://media.blackhat.com/bh-us-12/Briefings/Aldridge/BH_US_12_Aldridge_Targeted_Intrustion_WP.pdf

Anderson, N, 2006. Tim Berners-Lee on Web 2.0: "nobody even knows what it means". Viitattu 8.3.2012.
http://arstechnica.com/business/2006/09/7650/

Andress, J., Winterfeld, S. 2011. Cyber Warfare -Techniques, Tactics and Tools for Security Practitioners. USA: Syngress.

AndrewNohawk.com. 2012. Facebook GraphAPI and Maltego. Viitattu 15.9.2012.
http://andrewmohawk.com/2010/10/12/facebook-graphapi-and-maltego-or-you/

Appel, J.A. 2011. Internet Searches for Vetting, Investigations, and Open-Source Intelligence. USA: CRC Press.

AuroraWDC.com. 2012. What is Competitive Intelligence. Viitattu 6.10.2012.
http://www.aurorawdc.com/whatisci.htm

BBC News. 2012. Facebook has more than 83 million illegitimate accounts. Viitattu 1.9.2012.
http://www.bbc.com/news/technology-19093078

Bhatti, B. 2012. Cyber Security and Privacy in the Age of Social Networks. Teoksessa Zubairi, J.A., Mahboob, A. 2012. Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies. USA: IGI Global.

Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. 2009. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. Teoksessa Quemada, J., León, G., Maarek, Y., Nejdl, W. 2009.WWW '09 Proceedings of the 18th international conference on World wide web. New York. ACM.
http://www.sba-research.org/wp-content/uploads/publications/Bilge_AllYourContacts_2009.pdf

Blog.twitter.com. 2011. 200 million Tweets per day. Viitattu 4.10.2012.
http://blog.twitter.com/2011/06/200-million-tweets-per-day.html

Carr, J. 2011. Is The Advanced Persistent Threat A "Who" Or A "What"?. Viitattu 20.8.2012.
http://www.forbes.com/sites/jeffreycarr/2011/02/08/is-the-advanced-persistent-threat-a-who-or-a-what/

Cendrowski, H., Mair, W.C. 2009. Enterprise Risk Management and COSO. USA: John Wiley & Sons.

Cert.fi. 2010. Tietoturvakatsaus 2/2010. Viitattu 1.4.2012.
http://www.cert.fi/katsaukset/2010/tietoturvakatsaus_2_2010.html

Clare, S., Sir Omand, D. 2012. Social media snooping powers out of date. Viitattu 24.9.2012.
http://www.bbc.co.uk/news/uk-politics-17815202

Corelabs.coresecurity.com. 2008. What is Exomind. Viitattu 15.9.2012.
http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=Exomind

dev.twitter.com. Viitattu 15.9.2012.
https://dev.twitter.com/

Dey, R., Jelveh, Z., Ross, K. 2012. Facebook Users Have Become Much More Private: A Large-Scale Study. VIitattu 30.3.2012.
http://cis.poly.edu/~ratan/facebookusertrends.pdf

D'Monte, L. 2009. Swine flu's tweet tweet causes online flutter. Viitattu 4.10.2012.
http://www.business-standard.com/india/news/swine-flu%5Cs-tweet-tweet-causes-online-flutter/356604/

Dugan, L. 2012. Twitter To Surpass 500 Million Registered Users On Wednesday. Viitattu 1.10.2012.
http://www.mediabistro.com/alltwitter/500-million-registered-users_b18842.

Dwyer, C., Hiltz, S.R., Passerini, K. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Viitattu 15.9.2012.
http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

Edwards, L., Brown, I. 2009. Data Control and Social Networking: Irreconcilable Ideas? Viitattu 20.3.2012.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1148732&

Erkkola, J-P. 2008. Sosiaalisen median käsitteestä. Taideteollinen korkeakoulu. Medialaboratorio. Lopputyö. Viitattu 20.3.2012.
http://mlab.taik.fi/pdf/ma_final_thesis/2008_erkkola_jussi-pekka.pdf

Ernst & Young. 2011. Into the cloud, out of the fog: Ernst & Young's 2011 Global Information Security Survey. Viitattu 1.3.2012.
http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

Europe versus Facebook. 2012. Viitattu 5.9.2012.
http://europe-v-facebook.org/EN/en.html

Facebook.com. 2012a. Facebook Pages Terms. Viitattu 1.7.2012.
http://www.facebook.com/page_guidelines.php

Facebook.com. 2012b. Tietosuojakäytäntö. Viitattu 5.9.2012.
https://fi-fi.facebook.com/about/privacy/your-info

Facebook developers. 2012. Viitattu 5.9.2012.
http://developers.facebook.com/

Faircloth, J. 2011. Penetration Tester’s Open Source Toolkit. 3. Painos. USA: Syngress.

Gaudin, S. 2009. Execs worry that Facebook, Twitter use could lead to data leaks. Viitattu 15.9.2012.
http://www.computerworld.com/s/article/9136465/Execs_worry_that_Facebook_Twitter_use_could_lead_to_data_leaks

Gephi.org. 2012. The Open Graph Viz Platform. Viitattu 15.9.2012.
http://gephi.org/

Ghosh, A. 2011. Overcoming America's lost decade of IT security. Viitattu 20.9.2012. http://www.scmagazine.com/overcoming-americas-lost-decade-of-it-security/article/214023/

Graham, B. 2005. Hackers Attack Via Chinese Web Sites. Viitattu 20.8.2012. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html

Gragido, W., Pirc, J. 2011. Cybercrime and Espionage: An Analysis of Subversive Multivector Threats. USA: Syngress.

Gross, R., Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networks. (The Facebook Case). Viitattu 20.3.2012. http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Gundecha, P., Barbier, G., Liu, H. 2011. Exploiting Vulnerability to Secure User Privacy on a Social Networking Site. Viitattu 15.9.2012. http://engineering.asu.edu/sites/default/files/shared/ASUCIDSE-2011-001.pdf

Gunter, D., Sonya, S. 2012. The Danger of Data Exfiltration over Social Media Sites. Viitattu 10.10.2012. https://media.blackhat.com/bh-us-12/Briefings/Gunter/BH_US_12_Gunter_Sonya_SNSCat_WP.pdf

Hearn, M. 2012. Facebook's Q2 Report Reveals 955 Million Profiles, of Which 83 Million Are Fake. Viitattu 1.9.2012. http://www.technobuffalo.com/internet/social-networking/facebooks-q2-report-reveals-955-million-profiles-of-which-83-million-are-fake/

Henkilötietolaki 523/1999.

Helsingin Sanomat. 2012. Facebookin käyttäjämäärä ylitti miljardin. Viitattu 5.10.2012. http://www.hs.fi/msn/talous/Facebookin+k%C3%A4ytt%C3%A4j%C3%A4m%C3%A4%C3%A4r%C3%A4+ylitti+miljardin/a1305603461307

Heikkinen, H. 2010, Toimintatutkimus –Toiminnan ja ajattelun taitoa. Teoksessa Aaltola, J., Valli, Raine. 2010. Ikkunoita tutkimusmetodeihin I. 3. uudistettu ja täydennetty painos. Juva: WS Bookwell.

Herley, C. 2009. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. Viitattu 23.9.2012. http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf

Hirsjärvi, S., Remes, P., Sajavaara, P. 2006. Tutki ja kirjoita. 12. painos. Jyväskylä: Gummerus.

Häikiö, L., Niemenmaa, V. 2007. Valinnan paikat. Teoksessa Laine, M., Bamberg, J., Jokinen, P. 2007. Tapaustutkimuksen taito. Helsinki: Yliopistopaino.

Into, T. 2012. Sosiaalisten verkkosovellusten tietoturva. Jyväskylän yliopisto. Tietotekniikan laitos. Pro gradu –tutkielma. Viitattu 3.9.2012. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/26923/URN%3aNBN%3afi%3ajyu-2011050810765.pdf?sequence=1

Isokangas, A., Vassinen, R. 2011. Digitaalinen jalanjälki. Helsinki: Talentum.

Json.org. 2012. Introducing JSON. Viitattu 15.9.2012.
http://json.org/

Juutilainen, K. 2008. Julkisiin lähteisiin perustuva tiedustelu (Open Source Intelligence). Helsingin yliopisto. Yleisen valtio-opin laitos. Pro gradu -tutkielma.

Juvonen, M., Korhonen, H., Ojala, VM., Salonen, T., Vuori, H. 2008. Yrityksen riskienhallinta. Helsinki: Yliopistopaino.

Karjalainen, M. 2011. Improving Employees' Information systems (is) Security Behavior. Toward a meta-theory of is security training and a new framework for understanding employees' is security behavior. University of Oulu. Faculty of Science. Department of information processing science. Dissertion. Viitattu 5.8.2012.
http://herkules.oulu.fi/isbn9789514295676/isbn9789514295676.pdf

Kalliala, E., Toikkanen, T. 2012. Sosiaalinen media opetuksessa. 2. uudistettu painos. Helsinki: Finn Lectura.

Kelly, M. 2008. Defcon 18 – Perspectives on Cyber Security and Cyber Warfare (video). Viitattu 10.9.2012.
http://www.securitytube.net/video/3192

Kietzmann, J.H., Hermkens, K., McCarthy, I.P., Silvestre, B.S. 2011. Social media? Get serious! Understanding the functional building blocks of social media. Viitattu 1.10.2012.
http://beedie.sfu.ca/files/PDF/research/McCarthy_Papers/2011_Social_Media_BH.pdf

Korkeimman oikeuden ennakkopäätös. 2003:36. Vahingonkorvaus –korvauksen sovittelu. Viitattu 3.9.2012.
http://www.finlex.fi/fi/oikeus/kko/kko/2003/20030036?search[type]=pika&search[pika]=tietomurto

Laki yksityisyyden suojasta työelämässä 759/2004.

Laine, M., Bamberg, J., Jokinen, P. 2007. Tapaustutkimuksen taito. Helsinki: Yliopistopaino.

Laine, M. 2007. Kriminologia ja rankaisun sosiologia. Jyväskylä: Gummerus.

Lehtonen, P. 2007. Tapaus- ja toimintatutkimuksen yhdistäminen. Teoksessa Laine, M., Bamberg, J., Jokinen, P. 2007. Tapaustutkimuksen taito. Helsinki: Yliopistopaino.

Lewis, J. 2009. MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving. Viitattu 15.9.2012.
http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html

Lewis, J. 2012. How spies used Facebook to steal Nato chiefs' details. Viitattu 1.10.2012.
http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html

Lifehacker.com. 2012. The Problem with Your Google Search Result Feedback Loop (and What You Can Do About It). Viitattu 1.7.2012.
http://lifehacker.com/5814100/the-problem-with-your-google-search-results-and-what-you-can-do-about-it

Lyons. G. 2012. Facebook to Hit a Billion Users in the Summer. Viitattu 20.3.2012.
http://connect.icrossing.co.uk/facebook-hit-billion-users-summer_7709

Mahmood, S., Desmedt, Y. 2012. Your Facebook Deactivated Friend or a Cloaked Spy (Extended Abstract). Viitattu 10.8.2012.
http://arxiv.org/abs/1203.4043

Manjoo, F., Yoffe, E. 2012. Revenge of the Facebook Stalker. Viitattu 20.8.2012.
http://www.slate.com/articles/podcasts/manners_for_the_digital_age/2012/03/transcript_facebook_stalker_should_i_tell_a_cheating_guy_s_girlfriend_that_we_hooked_up_.single.html

Mcclure, S., Scambray, J., Kurtx, G. 2009. Hacking Exposed 6: Network Security Secrets & Solutions. 6. painos. USA: The McGraw-Hill Companies

Mcclure, S., Scambray, J., Kurtx, G. 2012. Hacking Exposed 7: Network Security Secrets & Solutions. 7. painos. USA: The McGraw-Hill Companies.

Moore, R., McMullan, E.C. 2009. Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students. Viitattu 8.10.2012.
http://www.cybercrimejournal.com/mooreijcc2009.pdf

Metsämuuronen, J. 2008. Laadullisen tutkimuksen perusteet. Metodologia sarja 4. 3. uudistettu painos. Jyväskylä: Gummerus.

Molok, N.N.A., Chang, S., Ahmad, A. 2010. Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. Viitattu 1.7.2012.
http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism

Molok, N.N.A., Chang, S., Ahmad, A. 2011. Exploring The Use Of Online Social Networking By Employees: Looking At The Potential For Information Leakage. Viitattu 1.9.2012.
http://aisel.aisnet.org/pacis2011/138/

Moyer, S., Hamiel, N. 2008. Satan is on my Friend List: Attacking Social Networks. BlackHat USA Briefings 2008. Viitattu 1.3.2012.
http://www.blackhat.com/presentations/bh-usa-08/Moyer_Hamiel/BH_US_08_Moyer_Hamiel_Satan_is_on_my_Friends_List_Whitepaper.pdf

New York Times. 2010. Facebook Privacy: A Bewildering Tangle of Options. Viittu 30.3.2012.
http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Oulun yliopisto. Luonnontieetellinen tiedekunta. Tietojenkäsittelytieteiden laitos. Väitöskirja. Viitattu 10.9.2012.
http://herkules.oulu.fi/isbn9789514295713/isbn9789514295713.pdf

Opsahl, K. 2009. Google Begins Behavioral Targeting Ad Program. Viitattu 1.7.2012.
https://www.eff.org/deeplinks/2009/03/google-begins-behavioral-targeting-ad-program

Orlicki, J.I. 2008. LeakedOut: The Social Networks You Get Caught In. Viitattu 15.9.2012.
http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=publication&name=LeakedOut%3A_the_Social_Networks_You_Get_Caught_In

Paterva.com. 2012. Viitattu 20.9.2012.
http://www.paterva.com/web6/

Perustuslaki 731/1999.

Puusa, A., Juuti, P. 2011. Tieteenfilosofisista kysymyksistä laadullisen tutkimuksen näkökulmasta. Teoksessa Puusa, A., Juuti, P. 2011. Menetelmäviidakon raivaajat. Perusteita laadullisen tutkimuslähestymistavan valintaan. Vantaa: Hansaprint.

Rikoslaki 39/1889.

Russel, M.A. 2011. Mining The Social Web. USA: O'Reilly Media.

Saarela-Kinnunen, M., Eskola, J. 2010. Tapaus ja tutkimus =tapaustutkimus. Teoksessa Aaltola, J., Valli, Raine. 2010. Ikkunoita tutkimusmetodeihin I. 3. uudistettu ja täydennetty painos. Juva: WS Bookwell.

Schulze, K. 2012. Machen sich Facebook-Verweigerer verdächtig. Viitattu 20.8.2012. http://www.tagesspiegel.de/weltspiegel/nach-dem-attentat-von-denver-kein-facebook-profil-kein-job-angebot/6911648-2.html

Scott, P.R., Jacka, J.M. 2011. Auditing Social Media. A Governance and Risk Guide. USA: John Wiley & Sons.

Smyth, S.M. 2011. The New Social Media Paradox: A Symbol of Self-Determination or a Boon for Big Brother. Viitattu 1.9.2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2122939

Socialmedia Research Foundation. Viitattu 15.9.2012. http://www.smrfoundation.org/

Sophos. 2010. Security Threat Report 2010. Viitattu 15.9.2012. http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

Sophos. 2012. Security Threat report. Viitattu 1.3.2012. http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Solove, D.J. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. Viitattu 15.9.2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

Sørensen, L. 2009. User Managed trust in social networking –Comparing Facebook, MySpace an Linkedin. Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. Viitattu 3.9.2012. ftp://lenst.det.unifi.it/pub/LenLar/proceedings/2009/wv09/WVITAE09/PDF/AUTHOR/WV092855.PDF

Street, J.E., Nabors, K. 2010. Dissecting the Hack: The F0rb1dd3n Network. USA: Syngress.

Sähköisen viestinnän tietosuojalaki 516/2004.

The Sociable. 2012. Facebook by the numbers: 845 million users sharing 100 billion friendships. Viitatu 20.3.2012. http://sociable.co/social-media/facebook-by-the-numbers-845-million-users-sharing-100-billion-friendships/

Thornburg, N. 2005. The Invasion of the Chinese Cyberspies. Viitattu 20.8.2012. http://www.time.com/time/magazine/article/0,9171,1098961-4,00.html

Tirronen, M. 2008. Web 2.0, verkon numerologia. Helsinki: BTJ kustannus.

Tietosuojavaltuutetun toimisto. 2006. 626/452/2006. Henkilötietojen kerääminen internetistä hakukoneen avulla ns. Googlaamalla työnantajan toimesta ja tietojen poistaminen google-hakukoneesta. Viitattu 10.9.2012. http://www.tietosuoja.fi/48526.htm

Tuunanen, V.P., Pitkänen, O., Hovi, M. 2009. Users' Awareness of Privacy on Online social Networking sites –Case Facebook. Viitattu 20.3.2012.
http://domino.fov.uni-mb.si/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf

US Army. 2001. FM 7-92 The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry). Viitattu 4.10.2012.
http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/fm7_92.pdf

Uusitalo, K., Kohtamäki, M. 2011. Konstruktiivisen tutkimusotteen rooli menetelmien kentässä. Teoksessa Puusa, A., Juuti, P. 2011. Menetelmäviidakon raivaajat. Perusteita laadullisen tutkimuslähestymistavan valintaan. Vantaa: Hansaprint.

Vance, A. 2010. Why do employees violate is security policies? Insights from multiple theoretical perspectives. University of Oulu. Faculty of Science. Department of information processing science. Dissertion. Viitattu 5.8.2012.
http://herkules.oulu.fi/isbn9789514262876/isbn9789514262876.pdf

Valtiovarainministeriö. 2010. Sosiaalisen median tietoturvaohje, Vahti 4/2010. Viitattu 1.8.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf

Valtiovarainministeriö. 2009. Kohdistetut hyökkäykset, Vahti 6/2009. Viitattu 1.8.2012.
https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091117Kohdis/kohdistetut_hyoekkaeykset_netti_kannet.pdf

Varangot, P.O. 2010. State of the Art Automation of Open Source Intelligence and Impersonation in Social Networks. Viitattu 15.9.2012.
http://corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=publication&page=State_of_the_Art_Automation_of_Open_Source_Intelligence_and_Impersonation_in_Social_Networks&file=RR-303_Varangot.pdf

Verizon. 2012 Data Breach Investigations Report. Viitattu 1.8.2012.
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Vercellis, C. 2009. Business Intelligence: Data Mining and Optimization for Decision Making. United Kingdom: John Wiley & Sons.

Wrenn, E. 2012a. Facebook 'five subtle tricks' to get users accepting app requests without thinking what info they are giving away. Viitattu 3.9.2012.
http://gibiru.com/index.php/uncensored-news/78-news/21460-security-adviser-accuses-facebook-of-playing-five-subtle-tricks-to-get-users-accepting-app-requests-without-thinking-what-info-they-are-giving-away

Wrenn, E. 2012b. Security adviser accuses Facebook of playing 'five subtle tricks' to confuse users over their privacy settings. Viitattu 4.10.2012.
http://www.dailymail.co.uk/sciencetech/article-2194834/Security-adviser-accuses-Facebook-playing-subtle-tricks-users-accepting-app-requests-thinking-info-giving-away.html?ITO=1490

Kuvat

Kuviot

Taulukot