Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2011

Matti Krouvila

INTERNETIN MERKITYS JA ELEKTRONISEN VALVONNAN TULEVAISUUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Tietoliikenne

Syyskuu 2011 | 38 sivua

Esko Vainikka

Matti Krouvila

INTERNETIN MERKITYS JA ELEKTRONISEN VALVONNAN TULEVAISUUS

Tämän opinnäytetyön tavoitteena oli tuoda esille tietoyhteiskuntien epäkohtia, ongelmia ja haavoittuvuuksia sekä pohtia elektronisen vallankumouksen vaikutusta ihmisten päivittäiseen elämään – Internetin merkitystä unohtamatta. Työssä käsitellään niitä tapahtumia ja asioita, jotka vaikuttavat, tavalla tai toisella, jokaisen tietoyhteiskunnassa elävän ihmisen arkeen. Muun muassa tietoturva, televalvonta, yksityisyyden suoja sekä tietoverkkojen kehitys ovat sellaisia asioita, jotka muodostuivat tämän opinnäytetyön ytimeksi.

Aihealueen ollessa näin laaja, jätettiin tekniset yksityiskohdat tarkentamatta keskittyen antamaan asioista ennemmin mahdollisimman kattava kokonaiskuva. Menetelminä käytettiin omakohtaista pohdintaa ja järkeilyä, tehden päättelyjä asioiden kyseenalaistamisen kautta. Lehtileikkeet ja uutiset yms. materiaali antoivat vahvistuksen esitetyille väitteille ja pohdinnoille. Teksti on luonteeltaan tutkivaa ja se pyrkii herättämään lukijan uteliaisuuden käsiteltäviä asioita kohtaan sekä valottamaan tietoyhteiskunnan varjopuolia.

Asioiden kriittisen pohdiskelun jälkeen tultiin siihen lopputulokseen, ettei ole järkevää luoda yhteiskuntaa pelkästään sähköisten toimintojen varaan. Tulevaisuudessa tekniikan kehitys tekee ihmisistä entistä riippuvaisempia teknologiasta ja Internetin olemassaolosta, eikä tiedettä aina sovelleta ihmiskunnan eduksi. Teknologian kehitys vie kohti nopeaa ja vaivatonta yhteiskuntaa, mutta samalla tulemme kohtaamaan uusia ongelmia ja ennennäkemättömiä uhkakuvia.

Työn tuloksia arvioidessa johtopäätös oli, että teknologian kehittyessä tullaan luomaan yhä uusia elämää helpottavia tekijöitä, mutta mikäli ihmisten perusoikeuksista ei pidetä huolta, vaarannetaan samalla oikeus yksityisyyteen. Käsiteltävä aihe pysyi suhteellisen hyvin raameissaan, tosin näkökulma muodostui melko kriittiseksi. Tämän opinnäytetyön tärkein päämäärä kuitenkin tavoitettiin, ja se oli yksinkertaisesti ottaa sellaisia asioita esille, joista yleensä mediassa vaietaan tai keskustellaan kovin vähän.

ASIASANAT: Internet, nanotekniikka, televalvonta, teknologia, tietoturva, tietoverkot, tietoyhteiskunta.

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

September 2011 | 38 pages

Esko Vainikka

Matti Krouvila

THE IMPORTANCE OF THE INTERNET AND THE FUTURE OF ELECTRONIC SURVEILLANCE

The goal of this study was to examine the shortcomings, problems and vulnerabilities of information societies as well as to consider the impact of the electronic revolution in people's daily lives – not forgetting the importance of the Internet. The work deals with the events and issues that affect, in one way or another, everyone's daily life in the information society. Among other things, security, electronic surveillance, privacy, and information networks formed to provide the core of this thesis.

As this topic is so broad, the technical details were left undetailed focusing to view things rather as a complete overview. The methods used were personal reflection and reasoning, making concludes by questioning. Clippings, news and other material gave a confirmation of the claims and reflections. The text is exploratory and seeks to arouse the reader's curiosity about the issues dealt with, to shed light on the shadowy side of the information society.

After the critical pondering of the issues, the conclusion was that it is not wise to create a society based on electronic functions only. In the future, technological developments will make people more dependent on technology and the existence of the Internet and science is not always applied for the benefit of mankind. Technological advances will lead towards a fast and easy society, but at the same time we are confronted with new problems and unprecedented threats.

Assessing the results of the work, the conclusion was that technological advances will create more and more new features that makes life easier, but if the basic human rights are not considered to be of concern, at the same time the right to privacy is jeopardized. The subject at hand kept relatively well its frames, however, the perspective formed to be quite critical. However, the main goal of this thesis was reached, and it was simply to bring out things, which usually remain silent in the media or reach very little discussion.

KEYWORDS: Internet, nanotechnology, electronic surveillance, technology, information security, data networks, information society.

SISÄLTÖ

KÄYTETYT LYHENTEET

ARPANET	Advanced Research Projects Agency Network, TCP/IP-protokollaa käyttänyt tietoverkko, josta kehittyi Internet (ARPANET, 2011.)
CIA	Central Intelligence Agency, Yhdysvaltain keskustiedustelupalvelu
CERN	Conseil Européen pour la Recherche Nucléaire, hiukkasfysiikan tutkimuskeskus Euroopassa
Cookie	Keksi eli eväste, www-palvelimelta käyttäjän tietokoneelle tallentuva tekstitiedosto.
DDR	Deutsche Demokratische Republik, Saksan demokraattinen tasavalta vuosina 1945 - 1990
DoS	Denial of Service, palvelunestohyökkäys
ECHELON	Maailman suurin sähköinen valvontajärjestelmä (ECHELON, 2011.)
EFF	The Electronic Frontier Foundation, tietoyhteiskunnan kansalaisoikeuksia puolustava organisaatio
EMP	Electromagnetic pulse eli elektromagneettinen pulssi
FRA	Förvarets radioanstalt, Ruotsin puolustusvoimien alainen tiedusteluorganisaatio
HAARP	High Frequency Active Auroral Research Program, ionosfääriä tutkiva projekti
HTML	Hypertext Markup Language, hypertekstin merkintäkieli
HTTP	Hypertext Transfer Protocol, Internetissä käytetty hypertekstin siirtoprotokolla
KGB	Neuvostoliiton turvallisuuspoliisi vuosina 1954 - 1991
Lex Nokia	Nimitys 2009 kesäkuussa voimaan tulleelle laille, joka sallii sähköpostiviestinnän tunnistetietojen seuraamisen
NFC	Near Field Communication, radiotaajuuksia käyttävä etätunnistustekniikka
NSA	National Security Agency, Yhdysvaltain kansallinen turvallisuusvirasto (NSA, 2011.)
P2P	Peer to peer, vertaisverkko

RFID	Radio Frequency IDentification, radiotaajuuksia käyttävä etätunnistustekniikka
Stasi	kansankielinen lyhennys sanasta Ministerium für Staatssicherheit, DDR:n salainen poliisi
SDI	Strategic Defence Iniative, Yhdysvaltain ohjuspuolustusohjelma 1980-luvulla, kutsuttu myös Tähtien Sota -ohjelmaksi.
SWIFT	Society for Worldwide Interbank Financial Telecommunication, standardi pankkiosoitteille
Telecoms Package	lainsäädäntöpaketti, jonka tarkoitus on EU:n televiestintämarkkinoita koskevien säännösten uusiminen (Apajalahti, 2009.)
URL	Uniform Resource Identifier, osoite, joka viittaa Internetissä olevaan kohteeseen
WELL	Whole Earth 'Lectronic Link, 1985 perustettu virtuaaliyhteisö

1 JOHDANTO

Valitsin tämän opinnäytetyön aiheen osittain mielenkiinnosta aihepiiriä kohtaan ja osittain sen vuoksi, että Internetin tarjoamat vaihtoehtoiset tietolähteet saivat minut epäilemään sen tiedon aitoutta, jota ihmiset päivittäin saavat perinteisistä valtamedioista, kuten TV:stä, radiosta ja sanomalehdistä. Tämän työn siemenet alkoivat itää jo vuosia sitten, kun aloin seurata tarkemmin maailman tapahtumia, katsoa silmiäavaavia dokumentteja sekä keräillä uutisia talteen Internetistä. Toisinaan ajatukseni olivat mustia kuin yö ja halusin jättää koko projektin kesken sekä etsiä jonkin muun käytännönläheisemmän aiheen, josta kirjoittaa. Minusta tuntui siltä, että olin avannut mieleeni Pandoran lippaan, jota en voinut enää sulkea.

Kuitenkin päätin jatkaa valitsemallani tiellä ja kirjoittaa täysin teoriapohjaisen opinnäytetyön. Tähän työhön ei sisälly varsinaista käytännön kokeellisuutta lainkaan, mutta omat tuntemukset, mielipiteet ja päätelmät pyrkivät korvaamaan sen puuttumisen. Työn tavoitteena ei ole liiemmin perehtyä tietoteknisiin yksityiskohtiin, vaan hahmottaa enemmänkin kokonaisuutta tietoliikenteen jatkuvasti uudistuvalla pelikentällä. Tarkoituksena on tarjota vaihtoehtoisia näkemyksiä asioista, joista puhutaan ja kirjoitetaan usein kovin ylistävään sävyyn, hyötyjä korostaen. Kolikolla on aina kaksi puolta ja itse pyrin tasapainoilemaan niiden välissä, joskin asiaan perehtymättömälle jotkin työssä esitettävät faktat saattavat vaikuttaa liian epäileviltä, jopa negatiivisilta.

Tämän työn tarkoitus on siis lyhyesti sanottuna valottaa vähemmälle huomiolle jääneitä totuuksia tietoyhteiskunnan varjopuolista. Toisena tavoitteena on saada lukija pohtimaan ja kyseenalaistamaan valtamedioista tulvivan tiedon alkuperää, aitoutta ja sen mahdollista rajoittuneisuutta. Internet ja tietoliikenteen kapasiteetin kasvu lisäävät käytettävissä olevan tiedon määrää sekä vaikeuttavat oikean ja väärän tiedon erottamista toisistaan.

2 MENNEISYYDESTÄ NYKYAIKAAN

Teknologian kehitys on tuonut mukanaan lukuisia mullistuksia ja keksintöjä tietoliikenteen alati muuttuvaan maailmaan. Aikanaan suurten innovaatioiden, radion ja television, rinnalle noussut uusi tiedotusväline Internet on tehnyt maailmasta pienen maailmankylän, jossa tiedon määrällä ja saatavuudella ei ole rajoja. Tämä rajaton tietopankki on tuonut mukanaan myös lukuisia ongelmia, jotka koskettavat jokaista maailman asukasta. Internetin nousu mediavaltiaan asemaan on mahdollistanut sen, että tiedon välittämisestä ja luomisesta on tullut osa jokamiehen oikeuksia. Nykyään kuka tahansa voi luoda mitä tahansa tietoa ja välittää sen minne tahansa alueelle, jossa on toimivat tietoliikenneyhteydet. Tämä tiedon rajaton vapaus on saanut kuitenkin valtaa pitävät tahot huolestumaan ja ryhtymään toimenpiteisiin, jotka pyrkivät rajoittamaan ihmisten sananvapautta ja kansalaisoikeuksia. Burman kyberkaupunkimalli ja Kiinan sensuurikoneiston asettamat Internet-rajoitukset antavat viitteitä siitä, mihin myös länsimaissa on mahdollista ajautua. Lisääntynyt elektroninen valvonta pyritään implementoimaan verkkojen verkkoon Internetiin, sillä rajattoman tiedon saatavuus ei palvele kaikkien etuja – etenkään vallankahvassa olevien tahojen.

Kun tarkastellaan teknologian kehitystä viimeisten 200 vuoden ajalta ja etenkin 1950-luvulta eteenpäin, on kehitys ollut päätähuimaavaa. Aina ensimmäisistä lennättimistä lähtien ihmiset ovat kiihtyvällä vauhdilla kehittäneet toinen toistaan nopeampia sähköisiä tiedonsiirtomenetelmiä. Hyvin lyhyessä ajassa on kehitytty huimiin nopeuksiin tiedonsiirtokapasiteettien suhteen muun muassa satelliittien ansiosta. Jos asiaa verrataan vanhaan postilaitokseen, jossa käytettiin hevosia ja lähettejä tiedon välittämiseen, on Internet tuonut valtavan muutoksen maailmaan, jossa elämme. Tieto, jonka ennen kesti jopa vuosia saapua perille toiselle puolelle maailmaa, tavoittaa vastaanottajansa nyt millisekunneissa. Nykyisten yhteyksien tuottamalla kapasiteetillä ei ole mitään vaikeuksia vastaanottaa videokuvaa reaaliajassa toiselta puolelta maailmaa – muista lukemattomista mahdollisuuksista puhumattakaan.

Missä mahdammekaan olla 10 vuoden päästä? Entä 50 vuoden? Teknologian kehityksellä ei näytä olevan mitään hahmotettavaa horisonttia, joten voimme vain arvailla, miltä esimerkiksi tulevaisuuden koti näyttää vuonna 2061. Elektronisen valvonnan näkökulmasta ajatellen ihmisten seuraaminen päivittäisellä tasolla tulee olemaan mielettömän helppoa, ja se on teknisesti täysin mahdollista jo nyt. Mihin olemassa olevaa tietoa voidaan käyttää ja miten sitä kerätään, on toistaiseksi vielä melkoinen mysteeri. Lakien muuttuessa tekniikan kehityksen ehdoilla myös yksityisyyden suojan määrittely tulee muuttumaan. Kenellä on oikeus mihinkin tietoon? Tällä hetkellä vaikuttaa siltä, että hallituksella, oli se sitten miten korruptoitunut tahansa, on oikeus tietää mitä sen johtaman valtion kansalaiset kullakin hetkellä tekevät, missä liikkuvat ja mitä tietoja Internetistä hakevat. Ymmärrettävää sinänsä, onhan terrorismi valtava uhka nykyään, mutta miten tulevaisuudessa määritellään terroristi? Onko se jonkin ääriliikkeen edustaja, kuten media antaa ymmärtää, vai voiko se olla henkilö, joka haluaa tietää kulissien takaisista asioista enemmän ja syvällisemmin – toisin sanoen, kuka tahansa meistä?

Kyseenalaisten tietojen hakeminen Internetistä on saanut tietyt tahot huolestumaan Internetin kehityksestä. Tavallisten kansalaisten kirjoittamat blogit nauttivat miljoonien lukijoiden huomiosta ja Facebookin kaltaiset verkostoitumispalvelut yhdistävät ihmisiä ympäri maailmaa. Jos kehityksessä ei siis voida ainakaan mennä takapakkia, onko mahdollista jotenkin seurata asioiden kehittymistä ja vaikuttaa kehitykseen sitä kautta? Ihmisten tiedonsaantimahdollisuuksia on aina pyritty ylemmiltä tahoilta rajoittamaan, ja näin pyritään tekemään tässäkin asiassa, ja tehdään – tälläkin hetkellä. Moni varmasti tietää miten kommunistidiktatuuri Kiina rajoittaa kansalaistensa Internetin käyttöä, tai miten Egypti pyrki sulkemaan osia Internetistä hiljattain tapahtuneen kansannousun aikaan. Se ei ole kovin kaukana siitä, mihin tietyt tahot esimerkiksi Yhdysvalloissa tällä hetkellä pyrkivät. Voidaan sanoa, että diktatuurissa se on mahdollista, mutta ei vapaassa demokraattisessa yhteiskunnassa. Teknisesti tämänkaltainen sensuuri on länsimaissakin täysin toteutettavissa, esteenä ovat ainoastaan lait, jotka eivät saa olla ristiriidassa

kansalaisvapauksien ja -oikeuksien kanssa. Jotta valvontaa toteuttavien viranomaisten on mahdollista valvoa kansalaisiaan, tarvitaan jokin hyvä syy, kuten terrorismi, jonka varjolla voidaan rajoittaa myös tavallisten kansalaisten perusoikeuksia. Esimerkiksi Yhdysvaltojen kansallisella turvallisuusvirasto NSA:lla on oikeus valvoa kansalaisten verkkoliikennettä (Ruotsi aloitti verkkoliikenteen salakuuntelun: mitä pitää tehdä ja tietää?, 2011). Tämän lisäksi sanottakoon, että suuri osa Suomen Internetliikenteestä kulkee Ruotsin kautta, jonka tiedusteluorganisaatio FRA:lla on oikeus salakuunnella Ruotsin rajat ylittävää liikennettä (Mäntylä, 2011). Tällä tavoin pystytään kiertämään myös esim. Suomen lainsäädäntöä, koska Internetiin mennyt tieto ei ole enää Suomen palvelimilla eikä Suomen lainsäädännön vaikutuspiirissä.

On siis päädytty tilanteeseen, jossa vapaa tiedon saatavuus on kääntymässä niitä vastaan, joilla on jotakin salattavaa. Yksittäisellä terroristilla on varmasti paljonkin salattavaa, mutta entä valtioilla? Hallituksilla? Suuryrityksillä? Kuka valvoo heitä? Mitä salattavaa heillä on? Jos poliisiviranomainen valvoo meitä, eikö meillä ole oikeutta valvoa, että he hoitavat työnsä samojen lakipykälien mukaan, joita me noudatamme? Meitä vartenhan he ovat yhteiskunnassa olemassa, meidän etujamme valvomassa.

Yhdysvalloissa nykyään käsitettä ”kansallinen turvallisuus” hyödynnetään niin, että säädetään uusia lakeja, jotka antavat valtuudet tehdä lähes mitä tahansa yhteiskuntajärjestyksen ylläpitämiseksi. Yhteiskunnan turvallisuus pyritään turvaamaan keinolla millä hyvänsä, vaikka se tarkoittaisi maan omien kansalaisten viemistä Quantanamo Bayn kaltaisiin terroristivankiloihin, joilla ei ole kansainvälisen yhteisön hyväksyntää. On aika herätä huomaamaan, että nykyisillä teknologian tuomilla positiivisilla eduilla on myös karu kääntöpuolensa, jota ei kansalaisille yleisesti mainosteta. Lait säädetään suljettujen ovien takana ja äänestäminen on joidenkin mielestä vain näennäistä demokratiaa. Saatamme pian herätä yhteiskunnassa, jossa jokainen liike on seurattavissa, jokainen maksutapahtuma rekisteröity ja jokainen vaihtoehtoinen tieto sensuroitu tai asetettu pannaan.

3 TEKNOLOGIAN LUOMAT UHAT JA MAHDOLLISUUDET

3.1 Sähköistetty maailma

Elämme sähköistetyssä maailmassa. Lähes kaikki tieto, mitä ihmisistä on olemassa, tulee tulevaisuudessa olemaan myös sähköisessä muodossa. Mitä tämä käytännössä tarkoittaa? Käytännössä elämme pian maailmassa, jossa kaikki tieto, mitä meistä on olemassa, tulee olemaan myös muiden saatavilla – tietoliikennelinjoja pitkin. Meidän tulee siis varoa ja pelätä sitä mitä teemme tietokoneillamme? Ei suinkaan. Pitää olla mahdollisimman rehellinen itselleen, voidakseen tehdä koneellaan, mitä ikinä haluaakin. Sillä lähes kaikki tieto, mitä sinusta on, tulee olemaan myös muiden saatavilla – osaavien käsien ulottuvilla. Huomionarvoista on, että nämä maagiset ”osaavat kädet” voivat yhtä hyvin olla rikollisia, kansalaishakkereita tai viranomaisia. Tämä asetelma luo lähtökohdat sille ajatukselle, mitä tulee tapahtumaan, jos kaikki tieto tulee olemaan sähköisessä muodossa.

Ajatuksesi ovat sähköä. Sähkö on siis ajatusta, ajatus sähköä aivojesi hermosolujen välillä. Tietoliikenteestä puhuttaessa sähkö on dataa ja data sähköä. Dataa voidaan liikuttaa erilaisina signaaleina esim. sähkön siivittämänä parikaapelissa, ääniaaltoina ilmassa sekä valokaapelin sisällä, valon nopeudella. Tietoliikenne on siksi myös valoa ja ääntä. Esimerkiksi ääniaallot voidaan dekoodata eli kääntää tietokoneen ymmärtämään muotoon ja toisin päin yksinkertaisen modeemin avulla. Tietokoneen näytöltä silmiisi tuleva valo ja kaiuttimista kuuluva ääni korvissasi on kuitenkin keinotekoista, palasista kasattua. Mikäli laatu on kohdallaan, silmä ja korva eivät aisti sitä. Ääni on saatettu esim. nauhoittaa mikrofonilla, kuljetettu valona ja ääniaaltoina jossakin väliaineessa ja lopuksi muunnettu sähköiseen muotoon, signaalin arvoiksi 0 ja 1 (aallon pohja ja huippu). Kaiuttimista ulos tullessaan kerran digitaaliseksi muutettu signaali on muuttunut takaisin analogiseksi, jotta korvasi voi poimia

sen. Täten tietoliikenne käsittää signaalin koko matkan äänen tuottajan suusta kuulijan korvaan. Siirtomedia on vain muuttunut matkalla.

Mitä tämä merkitsee laajemmasta näkökulmasta katsottuna? Ensinnäkin se tarkoittaa sitä, että lähes kaikki tieto, mitä sinusta on olemassa, voidaan kääntää sähköiseen muotoon: kirjoittamasi tekstit, mielipiteet, tiedot ystäväpiiristä, läheisistä ja itsestäsi sekä kuvasi, liikkeesi ja sijaintisi tarkkoja yksityiskohtia myöten. Listaa voisi jatkaa loputtomiin. Mitä merkitystä tällä on? Voit dekoodata itsesi sähköiseen muotoon. Kun Internet on saavuttanut jokaisen maailmankolkan, voimme kaikki elää oman itsemme heijastuksena lähes ikuisesti bittiavaruudessa.

3.2 Maailman, tietoverkkojen ja ihmisten yhdistyminen

Elämme yhteiskunnassa, joka pienenee jatkuvasti. Ei fyysisesti, mutta käytännössä kyllä. Maailmassa on käynnissä suuri tietoinen sekä tiedostamaton yhteenliittymä ihmisten, tietoliikenneverkkojen sekä kansainvälisen yhteistyön välillä. Internet leviää koko maailmaan, pankit yhtenäistävät rahajärjestelmiään, suuryritykset fuusioituvat, ihmiset luovat verkkoyhteisöjä ja eri maiden hallitukset tekevät tiivistä yhteistyötä mm. terrorismin torjumiseksi. Suuri osa tätä yhdistymistä koskevista päätöksistä tehdään suljettujen ovien takana, tavallisten ihmisten ulottumattomissa, kaukana kansalaisten vaikutuspiiristä. Kyse on kuitenkin elintärkeistä ja tulevaisuudessa jokaista ihmistä koskettavista asioista, kuten rahasta, tiedotusvälineistä, tiedonsiirrosta, kansalaisoikeuksista, sananvapaudesta, ihmisten ja eläinten hyvinvoinnista, elämästä ylipäänsä.

Mitä tämä kaikki tarkoittaa tietoliikenteen näkökulmasta katsottuna? Ainakin sitä, että lukuisat eri tahot kuten virastot, yritykset, hallitukset ja poliisi keräävät tälläkin hetkellä miljoonia tiedonpalasia yhteen käyttäen viimeisintä teknologiaa profiloidakseen ihmisiä ja asettaakseen heidät tiettyihin lokeroihin erilaisten asioiden perusteella. Tämä tapahtuu muun muassa hakusanasuodatuksen avulla ja näitä tietoja tullaan käyttämään viimeistään lähitulevaisuudessa sinun eduksesi ja sinua vastaan. Mainosten kohdentaminen on vain yksi esimerkki

siitä, miten näitä tietoja voidaan hyödyntää. Tietoja kerätään ja taltioidaan eri tarkoituksiin kulloinkin voimassa olevan lainsäädännön mukaisesti. Osansa näistä tiedon palasista saavat niin mainostoimistot, tiedustelupalvelut kuin rikollisorganisaatiotkin hyödyntäessään yksityisiä tai julkisia tietopankkeja eli palvelimia.

Esimerkiksi kiistelty ECHELON on ympäri maailmaa hajautettu valvontajärjestelmä, joka pystyy käsittelemään ja yhdistelemään valtavia tietomääriä millisekunneissa mm. avainsanalistojen avulla (Euroopan parlamentin loppuraportti ECHELONista, 2001). Näiden poimittujen tietojen avulla voidaan luoda profiili jokaisesta tietokoneesta, joka on kytketty Internetiin. Käyttäjän yhdistäminen esimerkiksi tietokoneelta tehtyihin hakuihin onkin jo hieman hankalampaa, muttei mahdotonta. Kysyä sopii, että mitä merkitystä tällä on ihmiselle, joka on täysin rehellinen ja lainkuuliainen kansalainen, kuten moni meistä on? Ei välttämättä mitään, mutta entä jos jonain päivänä tulee aika, jolloin tietoja aletaan käyttää tavallisia ihmisiä vastaan, tavalla tai toisella? Massiivisiin tietokantoihin varastoituja tietoja käytettäessä viattomia vastaan historia vain toistaisi itseään. Tieto on valtaa, sanotaan. Jos tämä ajatusleikki viedään hieman pidemmälle tulevaisuuteen, todellisuus saattaa muistuttaa scifi-elokuvaa: et voi olla enää missään yksin, joka puolella on kameroita, jotka seuraavat liikkeitäsi ja satelliitit paikantavat sinut mikrosirujen avulla. Muun muassa elokuva Enemy of the State ei ideoineen ole kovinkaan kaukana totuudesta, mikäli siinä esitettyihin ”faktoihin” on uskomista.

Yritysten ja virastojen välinen kansainvälinen yhteistyö on tiivistynyt siten, että tarvittaessa sinunkin tietosi voidaan luovuttaa eteenpäin esim. Facebookin palvelimilta mm. Yhdysvaltojen turvallisuusviranomaisille. Terroristit saadaan tällä tavoin kyllä varmemmin napattua, mutta tilanteen vaatiessa voidaan ketä tahansa syyttää ties mistä. Kehittyvä yhteistyö nanoteknologian parissa tutkimusta tekevien, ja uusia sovelluksia kehittävien lääkefirmojen, tietoliikenneyritysten ja aseteollisuuden välillä luo uusia uhkakuvia maailmaamme. Tämä kompleksi on pian levittänyt verkkonsa meidän ympärillemme niin tiiviisti, ettei siitä pysty enää irrottautumaan, vaikka

haluaisikin. Nykyään 1 % Suomen väestöstä tulee toimeen ilman kännyköitä (Lähes kaikilla alle viisikymppisillä on internet, 2011). Paljonko tämä prosentuaalinen osuus oli n. 15 vuotta sitten kun kännykät alkoivat vasta yleistyä? Jotkin kaupan alan yritykset haluaisivat jo siirtyä uuteen NFC-teknologiaa hyödyntävään maksutapaan, jossa kännykällä voitaisiin maksaa esimerkiksi päivittäiset ruokaostokset. Vaikka käteismaksu on edelleenkin nopein ja varmin tapa maksaa ostokset, halutaan siitä päästä eroon kustannussyistä. (Teppo, 2011). Jos teknologian evoluutio johtaa siihen, että ihmiset ottavat ihonsa alle mikrosirun, jolla hoidetaan tulevaisuudessa esimerkiksi päivittäinen kaupankäynti, miten tulet toimeen ilman sitä?

Yhdysvalloissa markkinoilla on jo jonkin aikaa ollut ihon alle asetettava RFID-siru. Tämä siru voi nykyään olla nanoteknologian ansiosta jopa niin pieni, ettei sitä välttämättä edes paljaalla silmällä erota. Kyseistä sirua markkinoidaan mm. lääkinnällisiin etuihin vedoten, ja mainittakoon, että eräs barcelonalainen yökerho tarjoaa VIP-asiakkailleen sellaista maksuvälineeksi. Skeptisimmät nettikirjoittajat ovat jo ehtineet arvailla sirun myöhempää käyttötarkoitusta tulevaisuudessa. Voiko käydä niin, että muutaman vuosikymmenen kuluttua kaikki raha on elektronisessa muodossa, eikä ilman tätä sirua voi ostaa eikä myydä mitään?

Yritysmainonta on mennyt mielestäni jo kauan sitten yli siedettävien rajojen. Internetmainokset, bannerit, hyppivät sanamukaisesti silmille ja nekin on profiloitu juuri sinua varten, esimerkiksi tekemiesi Google-hakujen perusteella (Tarvainen, 2011). Ihmiset tarvitsevat jatkuvasti nopeamman Internet-yhteyden, jotta kaikki sivuilla olevat mainokset latautuvat. Usein ne ovat vielä priorisoitu niin, että mainokset latautuvat ennen varsinaista verkkosivua. Jotta saat tietyn tarjouksen tiettyyn tuotteeseen, tulee sinun antaa matkapuhelinnumerosi sekä sähköpostiosoitteesi yrityksille mainontaa varten. Miltei jokainen tekemäsi ostos ja joissain tapauksissa pelkkä sivuston käyttö vaatii nykyään rekisteröitymisen. Taannoin voimaan tulleen EU-direktiivin valtuutuksella jokainen liikkeesi Internetissä tallennetaan operaattorisi palvelimille teletunnisteiden avulla vähintään vuodeksi. Suuryritysten yhdistyessä (mm. Nokia - Microsoft) tietosi

saattavat vaihtaa sekä omistajaa että maata. Näistä lisää myöhemmissä luvuissa.

Kaiken sähköistyminen ei ole hyvä asia. Mitä jos tietoliikennejärjestelmät kaatuvat maailmanlaajuisesti? Aseteknologian kehittyessä ja kilpavarustelun levitessä lähi- ja cyberavaruuteen koko maailma saadaan mahtumaan tähtäimeen. Internet on avannut osaltaan ihmisten silmiä ja mahdollistanut myös ennennäkemättömien virtuaalisten rintamalinjojen synnyn.

3.3 Teknologisen kehityksen horisontti

Kuten jokainen on varmasti todennut, teknologia kehittyy huimaa vauhtia. Tavallisen kuluttajan on vaikea pysyä jo esimerkiksi pelkän televisiotekniikan kehityksen perässä. Alkuun kuvaputkitelevisio säilytti pitkään asemansa, kunnes 2000-luvulla markkinat valtasivat LCD- ja plasmanäytöt. Nopeasti näiden jälkeen tulivatkin jo led- ja 3D-televisio, eikä kehitys suinkaan lopu tähän. Kehitys on kiihtyvää ja uudet laitteet ovat vanhentuneita jo kaupasta ulos kannettaessa. Ennen yksi kuvaputkitelevisio saattoi olla yhden perheen ikkuna maailmaan toista vuosikymmentä. Nykyään elektroniikka myös vikaantuu paljon nopeammin, eikä pitkäkestoiseen laatuun yritysten kannata edes panostaa, koska viimeistään kahden vuoden päästä saadaan myytyä uusi, parempi ja kehittyneempi laite ”vanhentuneen” laitteen tilalle. Sinällään täysin toimivat laitteet pyritään uusimaan mahdollisimman usein, jotta jatkuvaan kasvuun (myynnin lisäämiseen) perustuva markkinatalous voisi jatkaa voittokulkuaan. Minne vanha, käytetty elektroniikka päätyy, onkin jo täysin oma tarinansa.

Aseteknologia on kehittynyt vähintään siinä missä kuluttajaelektroniikkakin eli jatkuvasti kiihtyvällä vauhdilla. Ei ole varmaan kovin väärin väittää, että se teknologia ja osaaminen mitä nyt hyödynnetään televisioissa, kännyköissä, kameroissa jne., on ollut aseiden kehittäjillä jo vuosikymmeniä sitten. Karkeasti voisi sanoa, että nykyään tekniikka kehitetään tieteen nimissä, mutta mm. aseteollisuus seuraa kehitystä kuin hai laivaa, ja uusien teknisten läpimurtojen hyödyntäminen alkaa heti kun sille on keksitty käyttötarkoitus esim. apuvälineenä sodankäynnissä. Tämän lisäksi tieteen läpimurtoja hyödyntävät

nykyään kaikki suuryritykset – tavalla tai toisella. Aina automaatiotekniikan käytöstä tehtaissa kuluttajille päätyviin hyödykkeisiin asti kaikki mahdollinen teknologia pyritään valjastamaan, kuten aikoinaan hevoset maanviljelyn avuksi. Kuluttajille päätyessään tämä kyseinen teknologia on ollut olemassa jo vuosia, ellei jopa vuosikymmeniä. Eikä kyseisen tekniikoiden sovellukset siihen pääty. Joku taitava yksityishenkilö saattaa jalostaa keksintöä vielä pidemmälle antaen sille jonkin täysin uudenlaisen merkityksen. Voimme vain villeimmissä ajatuksissamme kuvitella mihin esim. 10 vuotta sitten keksittyä teknologiaa käyttää ja kehittää tänä päivänä edellä mainittu aseteollisuus.

Otetaanpa esimerkki avaruustutkimuksesta. Lyhyesti tiivistettynä Yhdysvallat kehitti 80-luvulla Tähtien Sota -ohjelmaksikin nimetyn SDI (Strategic Defense Initiative) -ohjuspuolustusjärjestelmän (Crowley, 2011). Tämä kyseinen järjestelmä suunniteltiin vastaamaan Kylmän sodan haasteisiin ja se käytti hyväksi jo kiertoradalla olevia satelliitteja sekä maassa olevia ohjuskilpiä. Sillä voitaisiin tarpeen vaatiessa tuhota esim. vihollisvaltion laukaisema ydinohjus jo heti laukaisunsa jälkeen. ”Tähtien Sota” -ohjelma lopetettiin aikanaan, mutta todellisuudessa ohjelma vain aikojen saatossa muutti nimeään ja teknologian kehittyessä sekin muuntui ja kehittyi. Kehitys on ollut tietoista, mutta salassa pidettyä, ja todisteet ovat harvassa siitä, että SDI-ohjuspuolustusjärjestelmän siemenistä on kehittynyt nykypäivän tabu HAARP. Tämä laitos on virallisesti olemassa ja sillä tutkitaan mm. ionosfääriä, mutta sen todellisista salatuista käyttötarkoituksista ei valtamediasta juuri mainintoja löydy. Joidenkin lähteiden mukaan asejärjestelmästä on jo olemassa toimiva prototyyppi (Manning & Begich, 2004). Mikäli tällaista teknologiaa on jo käytössä, niin se osuus teknologiasta mitä tavalliset ihmiset, kuluttajat näkevät ostamissaan hyödykkeissä on siis marginaalista – vain jäävuoren huipun huippu. Teknologia kehittyy siis ensin aseteollisuuden ehdoilla, ja vasta sen jälkeen sen sovellukset kehitetään tutkimuslaitoksissa ja yrityksissä, jotka markkinoivat ne lopuksi kuluttajille. Kantaessamme siis kotiin upouutta 3D-televisiota, käsissämme on vain mitättömät rippeet teknologian todellisten saavutusten ihmeistä.

Miten tämä kaikki vaikuttaa ihmisiin ja ympäröivään maailmaan? Kuten sanottu, elämme nykyään pienessä maailmankylässä, jossa melkein ketä tahansa voi olla suorassa yhteydessä keneen tahansa, missä päin maapalloa tahansa - Internetin välityksellä. Kaikki teknisesti kehittyneet nyky-yhteiskunnat nojaavat tietoyhteiskunnan varaan, jossa kaikki tieto tulee ennen pitkää olemaan sähköisessä muodossa. Yhteiskunnan toiminnot on rakennettu tietojärjestelmien varaan, joiden ei pitäisi missään olosuhteissa olla mahdollista kaatua kokonaan, edes sodan tai jonkin muun suurkatastrofin aikana. Kuitenkin mikäli edellä mainitun kaltaiset avaruusaseet ovat tulevaisuudessa arkipäivää, on mahdollista että sodan syttyessä kaikki maan tietoliikenne voidaan lamauttaa esim. EMP-pulsseilla. Tämä tarkoittaa käytännössä sitä, että päivittäin käytetyt nyky-ajan itsestäänselvyydet kuten kännykkä, nettiyhteys ja rahaliikenne lakkaavat toimimasta, ja esim. ruoka-, bensiini-, yms. ostokset jäävät tekemättä. Dokumentti Taistelu Avaruudesta (Pax Americana: The Weaponization of Space) tarjoaa syväluotaavan näkökulman aiheesta enemmän kiinnostuneille. Mielestäni ei ole hyvä asia, että kaikki ihmisen perustoimeentulon (elämisen) kannalta ratkaisevat asiat nojaavat tietoliikenneverkkoihin. Niiden kaatuessa vaikeutuu myös meidän elämämme huomattavasti.

Mihin olemme menossa? Ihmiskunta on menossa kohti uudenlaisia haasteita. Teknologian kehitys vie meitä huimaa vauhtia kohti vaivattomuutta sekä toisaalta kohti täydellistä katastrofia. Näinä aikoina teknologia voisi olla ihmiskunnan pelastus, mutta tällä hetkellä siitä hyötyvät eniten aseteollisuus sekä ylikansalliset suuryritykset. Tavalliselle kuluttajalle kehittyneestä tekniikasta on vain näennäistä hyötyä ja erityisesti vanhemmalle ikäpolvelle uusi teknologia tuo taas mukanaan yhden opeteltavan asian lisää – mikäli haluaa tekniikan kehityksen perässä pysyä.

4 INTERNETIN MERKITYS NYT JA TULEVAISUUDESSA

Internetistä kirjoitettaessa on kielellisesti kaksi vaihtoehtoa. Kirjoittaa sana joko isolla tai pienellä alkukirjaimella: internet tai Internet. Mielestäni sana kuuluu ehdottomasti kirjoittaa isolla alkukirjaimella sen tärkeyden korostamiseksi. Internetiä käyttää päivittäin yli 2 miljardia ihmistä, joten jos se olisi valtio, olisi se maailman suurin valtio (Tiededokumentti: Virtuaalivallankumous 4/4, 2010). Valtioiden nimet kirjoitetaan isolla alkukirjaimella, joten Internetin merkityksen korostamiseksi kirjoitan sen isolla alkukirjaimella. Onneksi se ei kuitenkaan ole valtio, koska siinä tapauksessa sen alkuperäinen idea katoaisi, ylhäältä johdetun hierarkiansa vuoksi. Internet on täysin vapaa tiedon avaruus ja sellaisena se tulee säilyttääkin. Sen käyttäjillä on kuitenkin aina viime kädessä vastuu omista tekemisistään.

4.1 Internetin merkitys käyttäjille

Tavalliset kansalaiset käyttävät Internetiä monenlaisten päivittäisten asioiden hoitamiseen. Ihmiset hoitavat raha-asioitaan verkkopankeissa, tukiasioita virastojen sivuilla, tilaavat verokorttinsa netistä ja ostavat sitä kautta muuan muassa lomamatkoja, vaatteita, pelejä, yms. Tietoa ja tiedostoja siirretään Internetin yli sähköpostitse, P2P-ohjelmilla sekä kuulumisia vaihdetaan Facebookin ja Twitterin kaltaisten yhteisöpalvelujen avulla. Tietoa haetaan verkkouutisista ja vaihtoehtoisista medioista, blogeja luetaan ja kirjoitetaan sekä mielipiteitä vaihdetaan avoimesti keskustelupalstoilla. Yrittäjät ja yksityishenkilöt ylläpitävät omia verkkosivujaan ja tekevät rahaa Internetissä. Raha vaihtaa omistajaansa nopeammin kuin käteinen kaupan kassalla. Edistyneemmät käyttäjät saattavat hakkeroida tietyille palvelimille ja tehdä kiusaa esim. julkisille palveluille. Pian ehkä äänestäminenkin tapahtuu sähköisesti. Listaa käyttömahdollisuuksista voisi jatkaa loputtomiin.

Radio ja televisio ovat myös älynneet alkaa hyödyntää Internetin tarjoamia mahdollisuuksia, koska suuri osa lukijoista/kuuntelijoista tavoitetaan sieltä. Radiolähetyksiä voi kuunnella podcasteina ja televisio-ohjelmia katsoa jälkikäteen netti-TV:stä. Uutiset ja säätiedot päivittyvät verkkosivuille reaaliajassa, kuten myös juorulehtien uusimmat ja kuumimmat tapahtumat. Mainonta on seurannut perässä ja hivuttautuu jokaiselle vähänkin tunnetummalle sivustolle. Pakoon ei pääse. Mainokset ovat tarkasti suunniteltuja liikkuvine kuvineen (jotta silmä kiinnittää huomion) ja upotettuja pop-up-ikkunoita ei voi olla huomaamatta. Cookiet eli keksit keräävät tietoa kuluttajista. Kaikenlaiset julkiset tiedotteet ovat nopeasti luettavissa verkkosivuilta. Lukijoiden huomion ohjaaminen ei kuitenkaan ole yhtä helppoa kuin mitä tavallisiin paperilehtiin tulee, koska vaihtoehtoja on paljon enemmän tarjolla. Tässäkin tapauksessa lukija valitsee yleensä kiinnostavimman jutun. Suomalaiset media-alan yritykset hankkivat pääasiassa tietonsa suurilta lehtitaloilta, kuten Suomen Tietotoimistolta (STT) ja Reutersilta, joten perinteisistä medioista saatu tieto saattaa ajoittain olla yksipuolista tai sen määrä rajallista.

Erinäiset virastot ja julkisen hallinnon toimijat jakavat tietoa palveluista verkkosivuillaan, mahdollistavat sähköisen asioinnin sekä ylläpitävät erilaisia rekistereitä käyttäjistään. Kela huolehtii tukiasioista, verovirasto veroasioista ja poliisi kansalaisten oikeuksista ja turvallisuudesta. Muuttoilmoituksen maistraattiin voi tehdä kätevästi Postin sivuilla. Eri virastojen välinen yhteydenpito on nykyään suunnattoman helppoa – tai ainakin pitäisi olla. Voiko byrokratia olla koskaan helppoa? Maiden rajat ylittävä tiedonvaihto on täten myös erittäin nopeaa. Eri maiden poliisit voivat toimittaa reaaliajassa etsintäkuulutuksen kaikkien EU-maiden viranomaisille, ja rikollinen voidaan napata jo tullissa ennen kuin henkilö ehtii poistua maasta. Biopassien ja kasvontunnistuslaitteiden avulla rikoksentekijä saadaan lähitulevaisuudessa kiinni vaikka toisesta maasta Euromaiden yhteisten rekisterien avulla. Rikollisilla on siis suurempi todennäköisyys jäädä kiinni EU:n alueella, Yhdysvaltoja unohtamatta. Tästä tiedonsiirtomahdollisuudesta johtuen myös tavallisten ihmisten tai rikosepäiltyjen seuraaminen on helpottunut ja nopeutunut.

Maailman vaikutusvaltaisimpiin kuuluvalla tiedusteluvirasto NSA:lla on valmiudet tehdä yhteistyötä Europolin kanssa, joten tiedot on mahdollista välittää valokaapeleita tai satelliitteja pitkin Atlantin taakse sekunneissa.

Hallitus toimii luonnollisesti yhteistyössä poliisin ja etenkin suojelupoliisin kanssa. Tiedonvaihto on lähinnä poliittisia asioita koskevaa ja maan turvallisuutta ylläpitävää toimintaa. Supolla on oikeus rajoittaa tietyille listatuille nettisivuille pääsyä sekä salakuunnella rikoksesta epäiltyjen henkilöiden puhelin- ja dataliikennettä. Sensurointi on aiheellista tiettyjen asioiden kohdalla kuten lapsipornon ja terrorismin estämiseksi ja ennaltaehkäisemiseksi. Kyseinen ”musta lista” on salattu, ja vain tietyillä tahoilla on oikeus lisätä sivustoja listalle. Nämä listat lähetetään operaattoreille, jotka noudattavat luonnollisesti lain kirjainta. Hallitusten välinen tiedonvaihto on olennaista esim. terrorismin torjunnassa, mutta muutakin arkaluontoista tietoa vaihdetaan, kuten suurta mediahuomiota saaneet Wikileaks-vuodot ovat paljastaneet.

Terrorismin torjunnassa näyttävät kaikki keinot olevan sallittuja. Kriisitilanteissa myös Suomessa saatetaan Egyptin tapaan Internet-yhteydet katkaista, ja tähän tähtää myös uusi pakkokeinolaki (Mäntylä, 2011). Keskustelupalstojen rehottavia keskusteluja saatetaan sensuroida uusien lakien linjauksilla sekä bannien avulla. Itsesensuuriin ajaminen on tässä tilanteessa erittäin tehokas sensuurimenetelmä. Hallitus voi näin poliittisesti linjata, mistä on sallittavaa keskustella, ja mistä ei sovi puhua tai kirjoittaa. Mihin kerättyjä tietoja voidaan tulevaisuudessa käyttää, on vielä mysteeri. Mikäli merkit pitävät paikkansa, profiileja ihmisistä luodaan jo nyt. Teletunnistetietojen tallentaminen ja muut Lex Nokian kaltaiset lakimuutokset tähtäävät valvonnan lisäämiseen. Voidaanko näitä kerättyjä tietoja käyttää tulevaisuuden kriisitilanteissa samalla tavalla hyödyksi kuten esimerkiksi Stasi teki DDR:ssä? Sinä päivänä kun näin tehdään, voimme sanoa elävämme poliisivaltiossa.

Valitettavasti myös todelliset terroristit ovat tajunneet Internetin potentiaalin ja ryhtyneet hyödyntämään sitä. Uusien solujen syntyminen ja kapinallisten ”rekrytointi” on helppoa maailmanlaajuisen verkon välityksellä.

Propagandavideoiden levitys ja solujen johtaminen ”etänä” salatusta paikasta on tuonut terrorismin uudelle tasolle. Tähän on syytäkin puuttua. Ääri-ideologiat leviävät siinä missä Youtuben hauskat videotkin, ja mustekalan lonkerot levittäytyvät kaikkialle Internetiin, hyvässä ja pahassa.

4.2 Internetin evoluutio

Internetin merkitys on kasvanut ja tulee kasvamaan tulevaisuudessa huippuunsa ja sitten vähitellen menettämään asemaansa samoin kuten kävi esimerkiksi hehkulampulle. Internet on vertauskuvallisesti vain valon välähdys tässä maailmankaikkeudessa, mutta erittäin kirkas sellainen. Sen vuoksi sitä pyritään rajoittamaan ja paljon. Erilaiset toimenpiteet pyrkivät rajoittamaan sen valtaa, koska Internetin kehittäjätkään eivät tienneet 70-luvulla, millaisen lumivyöryn he sysäsivät liikkeelle. Tämä verkkojen verkko on maailman mullistavin keksintö sitten kivestä muovatun kuparin. Ihmiset ympäri maailmaa voivat verkostoitua, jopa liittoutua keskenään. Sillä on sekä maailmaa yhdistävä että erottava vaikutus.

Internet on syntynyt periaatteeltaan anarkistisista lähtökohdista. Sen luominen oli vallankumouksellista ja kehitys kapinaa hierarkioita vastaan. Sen tekniset ominaisuudet muovautuivat jo olemassa olevien tietokoneiden ja tiedonsiirtoyhteyksien varaan, joskin niitä ei ollut vielä kehitelty Internetin alkutaipaleella. ARPANET-tietoverkko loi pohjan esimerkiksi WELL-virtuaaliyhteisölle. Tämä oli ensimmäinen yhteisö verkossa, johon kuka tahansa tietokoneen käyttäjä saattoi kirjoittaa mitä tahansa virtuaaliyhteisön luettavaksi. Internetin kehittyessä ja uusien käyttömahdollisuuksien laajentuessa Tim Berners-Lee ja Robert Cailliau kehittivät CERNissä työskennellessään uuden tavan ja protokollan, jolla internetiä voitiin hyödyntää. Oli syntynyt World Wide Web. WWW mahdollisti käyttäjien tiedonhaun ja tiedon jakamisen siihen aikaan innovatiivisen linkitysmetodin avulla. Uusia sivuja, jotka olivat kenen tahansa käytettävissä, voitiin luoda ja linkittää keskenään tiettyjä yhteyskäytäntöjä ja kieltä hyödyntäen (URL, HTTP, HTML). (Tiededokumentti: Virtuaalivallankumous ¼, 2010). Mihin mittoihin tämä tiedon valtateiden

yhteenliittymä kasvaisi, oli varmasti tässä vaiheessa vielä vain arvailua ja utopiaa.

Nykyään Internetin merkitystä ei enää sellaisenaan innovaationa korosteta, vaan siitä on tullut ikään kuin itsestäänselvyys – jopa välttämättömyys. Uusia sovelluksia nousee Internetin ”päälle” kuin sieniä sateella ja mitä enemmän ja laajemmalle tämä verkko levittäytyy, sitä riippuvaisempia siitä meistä tulee. Pankkiasiat hoidetaan luonnollisesti netissä, tapaamiset ystävien kanssa sovitaan yhteisöpalveluissa jne. Internetistä on tullut toinen maailma, toinen todellisuus, jossa elämme – virtuaalitodellisuus. Internetin ajatus ja sen takana piilevä ideologia on suunnaton voimavara ja sampo niille, jotka jotenkin hyötyvät sen olemassa olosta, taloudellisesti tai muissa arvoissa mitattuna. Vapaille markkinoille luonnollisesti siirtyy aina myös liiketoiminta, ja tässä tapauksessa se lähti aikoinaan liikkeelle Microsoftin perustajan Bill Gatesin aloitteesta. Hän esitti tuolloin kysymyksen: Miksei tietokoneohjelmien tekemisellä voisi myös rikastua? Miehen menestystarina kertookin loput. Vastavallankumouksena tälle ajatukselle syntyi myöhemmin muun muassa Napster, vertaisverkkojen esi-isä, joka mullisti tiedostojen, kuten musiikin, jakamisen ja vaihtamisen verkon käyttäjien kesken – ilmaiseksi. Tämä puolestaan herätti suurta keskustelua tekijänoikeusrikkomuksista, jotka puhuttavat vielä tänäkin päivänä ajankohtaisuudellaan (vrt. Pirate Bay).

Tulevaisuudessa Internetin merkitys tulee vielä kasvamaan suuresti, ja vaikka jokin vielä mullistavampi keksintö tulisi syrjäyttämään koko internetin, tulee se jäämään koko tietoliikenteen yhdeksi kivijalaksi. Siirtomediat, kuten puhelinlinjat ja matkapuhelinverkot, tulevat muuttumaan, mutta tietoliikenteen puhelinkeskus Internet tulee uskoakseni pysymään periaatteiltaan muuttumattomana. Käyttäjien valtaa tämän massiivisen verkkosuman sisällä pyritään jo nyt rajoittamaan, joten internetin käyttö kansalaisoikeutena tulee vaarantumaan. Siksi kansalaisten sekä kansanedustajien pitää olla erittäin tarkkana, kun säädetään lakeja, jotka saattavat rajoittaa ihmisten oikeutta päästä avoimen, jokaisen saatavilla olevan, vapaastimuokattavan tiedon äärelle. Rajoituksia tulee satelemaan sekä huolestuneiden yhteisöjen ja yksilöiden aloitteesta

lähtien aina EU:n huipulta tuleviin direktiiveihin ja lakeihin asti. Tästä lisää luvussa Elektonisen valvonnan suuntaviivat.

Internetin syövereistä löytyy myös paljon kyseenalaista materiaalia, mikä pitääkin sensuroida, esimerkiksi lapsipornoa. Kaikki tämän kaltainen aineisto, mitä henkisesti sairaat ihmiset nettiin välittävät, pitää kitkeä pois, koska ne ovat sekä lainvastaisia että sotivat yhteisön asettamia perusarvoja vastaan. Internet on kuitenkin maiden rajat ylittävä verkko, ja koska eri maissa on toisistaan poikkeavat lait, varsinaisen sensuurikoneiston olemassaolo on perusteltua.

Internet on paljon enemmän kuin pelkkä interaktiivinen televisio. Käyttäjät saavat itse täysin vapaasti valita katsomansa sivut ja ohjelmat miltei loputtomasta tarjonnasta sekä itse vaikuttaa tarjottavaan sisältöön. Tämän lisäksi se on nykyisen tietoyhteiskunnan perusta. Kukaan ei voi sanoa omistavansa Internetiä, joskin suuryritykset pyrkivät voimakkaasti monopolisoimaan käytettäviä palvelukanavia. Jää nähtäväksi mitä Internetillä on vielä tarjottavanaan sen käyttäjille ja mihin suuntaan sen alkuperäistä ideaa yritetään muuntaa. Tulevaisuudessa kvantti-internetin mukanaan tuomat mahdollisuudet saattavat muuttaa koko tietoteknisen pelikentän totaalisesti (Wallenius, 2011).

5 ELEKTRONISEN VALVONNAN TULEVAISUUS

5.1 Yksityisyyden suoja ja kansalaisoikeudet

Yksityisyyden suoja on yksi tärkeimpiä oikeuksia nykypäivänä. Jokaisella ihmisellä on oikeus yksityisyyteen. Tämä tarkoittaa sitä, että ihmisen henkilökohtaisten tietojen tulee olla vain niiden tahojen tiedossa, kenellä niitä on oikeus lain mukaan tarkastella, sekä niillä kenelle henkilö on antanut luvan niitä tarkastella. Internet-aikakaudella nämä tiedot ovat vaarantuneet pahemman kerran. Internet on mahdollistanut näiden tietojen varastamisen ja väärinkäytön ennennäkemättömällä tavalla. Identiteetti- ja henkilötieto- yms. varkaudet ovat helpompia kuin koskaan. Salasanavarkaudet ovat yleistyneet. Väärennettyjen biopassien tekeminen osaavalle ei ole kovinkaan vaikeaa, eivätkä tietomurrot vahvasti suojattuihin kohteisiin ole mahdottomia. Kolmannet osapuolet pääsevät hyödyntämään tietojamme uskomattoman helposti.

Nykyään jokaiseen asennettavaan ohjelmaan, jota käytät, vaaditaan yleensä käyttöoikeus, jossa määritellään tarkasti mitä tietoja kerätään ja mihin niitä käytetään. Kansankielellä tätä voisi kutsua ”pienellä präntätyksi” ja tämän käyttösopimuksen säännöt on hyväksyttävä, jotta voit käyttää ohjelmaa. Oli ohjelma sitten mikä tahansa, kunka moni oikeasti edes lukee tätä pienellä präntättyä? Itse luen tekstit hyvin harvoin jo pelkästään ajan puutteen vuoksi. Mihin ihmiset näissä sopimuksissa yleensä suostuvat, saattaa olla mitä tahansa maan ja taivaan väliltä. Rekisteröintien yhteydessä sinulta saatetaan kysyä esim. nimesi, syntymäaikasi ja osoitteesi. Tähdellä merkityt kentät ovat yleensä pakollisia ja niiden määrä vaihtelee sivuston käyttötarkoituksesta riippuen. Esimerkiksi pelataksesi jotain verkkopeliä sinulta saatetaan kysyä nimi- ja osoitetietoja sekä sähköpostiosoitetta. Sinun tulee myös keksiä salasana kyseiselle sivustolle kirjautumista varten. Rekisteröitymisen vaativat sivustot ovat lisääntyneet eksponentiaalisesti ja moni käyttäjä ei varmaankaan jaksa keksiä joka sivustolle erikseen omaa salasanaa. Siispä vanhoja, jo kertaalleen jossain muualla käytettyjä salasanoja ja käyttäjätunnuksia kierrätetään. Tämä heikentää käyttäjän tietosuojaa tietomurtojen yhteydessä, kuten kävi esimerkiksi

viimeaikaisen Playstation-tietomurron yhteydessä, jossa miljoonien ihmisten henkilötietoja varastettiin. Varkaita kiinnostavat lähinnä luottokorttitiedot, joilla voidaan saada suoraa rahallista hyötyä, mutta muustakin tiedosta voi olla osaaville rikollisille hyötyä. Muistettavia salasanoja saattaa olla niin paljon, ettei niitä millään muista elleivät ne ole mustaa valkoisella. Itse ainakin tunnustan, että jouduin vaihtamaan useaan eri paikkaan salasanan tämän kyseisen tietomurron yhteydessä.

Verkkopankitkaan eivät ole turvassa näiltä hyökkäyksiltä, eikä mikään järjestelmä ole täysin murtamaton. Osaavat hakkerit ja ammattirikolliset, tiedustelupalveluista puhumattakaan, pystyvät murtamaan minkä tahansa suojauksen, kun käytössä on tarvittavat laitteet sekä riittävästi aikaa. Siksi on erittäin kyseenalaista esimerkiksi suhteellisen tuore lakiehdotus, jossa poliisille annettaisiin oikeus luoda seurattavan henkilön koneelle ns. takaportti, jonka avulla on mahdollista asentaa käyttäjän koneelle vakoilu- ja seurantaohjelmia. Tällaista takaporttia pystyvät hyödyntämään myös mm. hakkerit.

> Lakiesityksen ongelmaan on kiinnittänyt huomiota muun muassa Piraattipuolue. Sen puheenjohtajan Pasi Palmulehdon mukaan salaa asennetut ohjelmistot voivat haitata tietojärjestelmien toimintaa. - Vakoilumetodit ohittavat useimmat tietoliikenteen salaustavat ja jättävät luettavaksi kaiken koneen käyttäjän viestinnän, pankkitunnukset ja lähes kaiken verkon käytön. (Uusi pakkokeinolaki uhkaa heikentää tietoturvaa, 2011)

Facebookissa on useita kyseenalaisia tietoturvaongelmia, jotka liittyvät yksityisyyden suojaan. Yksi näistä ongelmista liittyy esim. sähköpostiosoitteen ja salasanan kyselyyn kaverihaun yhteydessä.

> Kaverihaku ilmeisesti tarkastaa sähköpostin osoitetiedoista, kenen kanssa on pidetty yhteyttä, ja ehdottaa kaveruussuhdetta Facebookista löytyvien henkilöiden kanssa. Viestintäviraston CERT-FI-tietoturvayksikön päällikkö Erka Koivunen pitää toimintaa tietoturvan kannalta pöyristyttävänä. Tunnusten kysyminen on kuitenkin hänen mukaansa laillista. Koivusen mielestä sähköpostin salasanaa ei kannata antaa Facebookille. Hän kuitenkin korostaa, ettei usko Facebookin syyllistyvän yksittäisten käyttäjien sähköpostiviestinnän seuraamiseen. (Facebook urkkii salasanoja, 2010)

Kansalaisten oikeuksia tietoyhteiskunnassa puolustavan The Electronic Frontier -järjestön (EFF) mukaan yhdysvaltalaisia rikostutkijoita koulutetaan käyttämään hyväkseen Facebookia ja muita vastaavia yhteisöpalveluja. Järjestön julkaisemien dokumenttien mukaan esimerkiksi liittovaltion poliisin FBI:n agentit liittyvät yhteisöpalveluihin tekaistuilla henkilöllisyyksillä ja pyrkivät pääsemään epäiltyjen ihmisten kaveripiiriin. (Varo: Facebook-kaverisi voikin olla agentti, 2010.) Googlen yksityisyyden kunnioittamisesta löytyy lukemattomia eri epäkohtia, joista on myös uutisoitu suhteellisen paljon. Yksi esimerkki liittyy Suomessa kesällä 2010 julkitulleeseen urkintatapaukseen, jossa Google keräsi tietoja yksityisten ihmisten langattomista verkoista Google Streetview -palvelun kehittämistarkoituksessa Suomessa ja muualla maailmassa. Asia on viety oikeuteen Yhdysvalloissa ja myös Suomen viranomaiset ovat pyytäneet Googlelta selvitystä asiaan. Google ei myönnä rikkoneensa lakia, vaan yhtiön mukaan tietoa kerättiin ohjelmointivirheen vuoksi. (Yhdysvallat tutkii Googlen kotiverkkojen urkintaa, 2010). Jälkeenpäin Internetyhtiö kuitenkin myönsi, että osa katunäkymäpalvelua varten kerätystä tiedosta sisälsi sähköpostiosoitteita, verkko-osoitteita ja tunnuksia. Yhtiö pahoitteli tietojen urkkimista ja lupasi hävittää kerätyt tiedot. Googlen mukaan ihmisten yksityisyydestä pidetään jatkossa parempaa huolta. (Googlen katunäkymäpalvelu keräsi nettiosoitteita ja tunnuksia, 2010).

Asiaa sivuten edellä mainittu yritysjätti rakentaa parhaillaan Suomeen massiivista datacenteriä eli palvelinkeskusta Haminaan Stora Ensolta ostamaansa paperikeskukseen. Investoinnin arvo on n. 200 miljoonaa euroa. Hankkeen sijoittaminen maantieteellisesti lähelle Venäjää ei Googlen mukaan vaikuttanut päätökseen rakentaa datacenter juuri Suomeen. (Tamminen, 2010.)

Yksityisyyden suojaa uhkaavat myös monet muut viimeaikaiset tapahtumat. Yksi tekijä aiheeseen liittyen on EU:sta säädettävät lakiehdotukset, jotka koskettavat koko Eurooppaa jokaista suomalaista myöten. Muun muassa pankkijärjestelmien yhtenäistäminen Euroopassa sekä tietojen luovuttaminen Yhdysvaltoihin uuden SWIFT-sopimuksen myötä on herättänyt laajaa spekulaatiota tietosuojasta.

> Suomalaismeppi Carl Haglundin (r.) mukaan neuvosto ei ole antanut parlamentaarikoille riittävästi tietoa esimerkiksi siitä, mihin tarkoituksiin kansalaisten pankkitietoja tultaisiin käyttämään ja mihin tarkoitukseen niitä kerätään. Yhdysvallat on halunnut pankkitietoja EU:lta osana terrorismin vastaista taistelua. Tietojen kerääminen on herättänyt voimakasta vastustusta.
>
> Yhdysvaltain keskustiedustelupalvelu CIA on seurannut jo vuosia eurooppalaista rahaliikennettä kansainvälisen Swift-pankkitunnuksen avulla. Eurooppalaiset viranomaiset eivät valvoneet toimintaa eikä asiasta ollut sopimusta EU:n ja Yhdysvaltain välillä. Muun muassa Euroopan keskuspankki tiesi toiminnasta, mutta sanoo olleensa voimaton puuttumaan asiaan. (EU-parlamentti ei halua luovuttaa kansalaisten pankkitietoja Yhdysvaltoihin, 2010.)

Yhdysvalloilla on ilmeisesti oikeus tehdä mitä tahansa terrorismin vastainen toiminta -leimasimen varjolla. Mikäli asia tulee julki, sitä puolustellaan juuri tällä päättymättömällä terrorisodalla, tai sitten asiasta tehdään lakiehdotus EU:ssa, jonka hallintoelimet myötäilevät useissa eri asioissa Yhdysvaltoja ja ylikansallisia suuryhtiöitä. Lain voimaantulon jälkeen ennen paheksuttu tietosuojaloukkaus on hyväksyttävä osana terrorismin vastaista sotaa. Karkeasti kärjistettynä se, mikä on nyt arkipäivää Yhdysvalloissa, pyritään muodossa tai toisessa implementoimaan myös Euroopan Unioniin. Suomi on ollut monien käskyjen ja direktiivien noudattajana mallioppilas, mutta toisin kävi esimerkiksi Saksassa, jossa teletunnistetietolaki todettiin perustuslain vastaiseksi (Effi: teletunnistetietojen pakkoluovutus Saksassa perustuslain vastainen, 2010).

Yksi mietityttävä askel valvontayhteiskunnan kehittymistä kohti poliisivaltiota on sormenjälkirekisterin luominen biometripassien haun yhteydessä. Tämä johtaa lähes välttämättömästi ”olen rikollinen kunnes toisin todistetaan” -ajatteluun, mikä on tyypillistä esim. Yhdysvalloissa. Tästä tulee väkisinkin mieleen elokuva Minority Report, jossa tulevaisuuden rikokset estetään jo ennen kuin ne on ehditty toteuttaa – ennustajien ja superälykkään tietokoneohjelmiston avulla. Koska mikään järjestelmä ei ole koskaan virheetön, elokuvan päähenkilö lavastetaan syylliseksi rikoksesta, jota hän ei ole vielä edes tehnyt. Aiheeseen liittyen hollantilaisen Radbound Universiteit Nijmegen –yliopiston tutkimusryhmä SoS on tutkimuksissaan todentanut mahdollisuudet salakuunnella

biometripassien ja lukulaitteiden välistä tietoliikennettä. Passeista pystytään valmistamaan kopioita sekä etälukemaan tietoja haltijan tietämättä. EFFI ry:n mukaan kuitenkin suomalaisten passien tietoturva on ainakin tällä hetkellä kunnossa. (Biopassi, 2011). Tämän tekniikan käyttöönotto tapahtui 9/11 -tragedian seurauksena, mikä selittää jo yksistään miksi tällaista teknologiaa kuitenkin tarvitaan. Terrorismin vastainen sota on siis aina myös sotaa ihmisten yksityisyyttä vastaan. Tämä jakaa ihmisten mielipiteet asiasta ainakin kolmeen osaan: niihin jotka ovat huolissaan yksityisyydestään, niihin jotka kannattavat terrorismin vastaista sotaa mihin hintaan hyvänsä, ja niihin joita asia ei juuri liikuta. Useimmat löytävät oman ajattelumallinsa varmasti jostakin näiden kolmen välimaastosta.

EU:n yksi pääperiaatteista alkujaan oli kansalaisten vapaa liikkuvuus EU-maasta toiseen ilman sen suurempia tarkastuksia. Nykyään terrorismin vastainen sota pakottaa rajoittamaan näitä oikeuksia esim. henkilöskannereiden muodossa sekä sisäisten rajatarkastusten lisäämisellä. Voisi sanoa, että kaksipäinen lohikäärme kuolee, jos siltä leikkaa toisen pään irti. Vaikea asia oikeanlaisen välimalliratkaisun löytämisen kannalta, mutta varmaa on että tekniikan kehittyessä elektroninen valvonta tulee lisääntymään terrorismin vastaisen sodan seurauksena. Esimerkiksi Osama Bin Ladenin ruumis tunnistettiin osittain kasvontunnistusteknologiaa hyväksikäyttäen (Alhopuro, 2011). Melko realistinen visio tulevaisuuden yhteiskunnasta on nähtävissä esimerkiksi BBC:n sarjassa Viimeinen vihollinen. Siinä jokaisen viraston ovessa on viivakoodilukija ja jokaisen julkisen liikenteen sisäänkäyntiä valvotaan elektronisesti. Lentokentillä on silmäskannerit ja jokaisessa kadun kulmassa on kamera, joka pystyy tunnistamaan henkilön esim. kasvojen perusteella. Sarjassa mennään hieman scifin puolelle käsiteltäessä nanorokotteita ja seurantasiruja, mutta jos asiaa lähtee tarkemmin tutkimaan, vihjailussa on kyllä tiettyä totuuspohjaa. Nanoteknologia käsittelee silminnäkemättömän pientä tekniikkaa (Yksi nanometri on miljoonasosa millimetristä), joten jää vain arvailujen varaan mihin tarkoitukseen esim. aseteollisuus tätä jo hyödyntää. Täysin varmaa on, että muun muassa em. taho on enemmän kuin kiinnostunut asiasta.

5.2 Elektronisen valvonnan suuntaviivat

Elektronisen valvonnan toteuttaminen on nykyään helpompaa kuin koskaan ja teknologian kehitys vain vauhdittaa tätä kehitystä. Internetin anarkistinen luonne luo valtaa pitäville hallituksille ja muille yhteiskuntajärjestystä valvoville tahoille jatkuvaa päänsärkyä. Uusia huolia tarjoaa muun muassa yhteisöpalvelut kuten Twitter ja Facebook, joista on tullut todellinen piikki auktoriteettien lihaan. Esimerkiksi Iranissa mielenosoittajiin kohdistunut väkivalta paljastui Twitterin ansiosta, kun videot väkivalloin tukahdetuista mielenilmauksista levisivät nettiin (Tiededokumentti: Virtuaalivallankumous 2/4, 2010). Sama ilmiö on tällä hetkellä käynnissä arabikevään johdosta monissa Pohjois-Afrikan ja Lähi-idän valtioissa. Egyptin kansannousun aikaan maan hallitus yritti estää levottomuudet sulkemalla verkkoa sen jälkeen, kun yli 500 000 ihmistä oli verkostoitunut Facebookissa. Valtion televisiokanava sen sijaan toimi ja välitti propagandaa Maan asukkaille. Tällä hetkellä esim. viimeaikaisten uutisten mukaan Syyriaan ei päästetä lainkaan ulkomaalaisia toimittajia, joten Youtuben kaltaiset videopalvelut ovat ainoa keino välittää kuvaa maan todellisista tapahtumista. Tällaiset palvelut saattavat jossain vaiheessa syrjäyttää koko valtamedian monopolin ainoana luotettavana tiedonlähteenä. Muutamia mainitakseni mm. Iran, Burma, Kiina ja jopa EU-jäsenyyttä hakeva Turkki sensuroivat ja valvovat laajasti kansalaistensa internetin käyttöä. Tietyille ulkomaisille sivuostoille ei ole pääsyä ja mm. Googlen hakutuloksia sensuroidaan ahkerasti. Lisäksi esimerkiksi Kiinassa toimii niin kutsuttuja 50 sentin kommentoijia, jotka kirjoittavat hallitusmyönteisiä kommentteja esimerkiksi keskustelupalstoilla (Tiededokumentti: Virtuaalivallankumous 2/4, 2010).

Kommunistidiktatuureissa tällainen sensuuri on jotenkin ymmärrettävissä, mutta ei kuitenkaan hyväksyttävissä. Kuitenkin maailmanpolitiikkaa seuranneena voin varovaisesti väittää, että kaikki mikä havaitaan diktatuureissa toimivaksi, tullaan tavalla tai toisella, jossakin muodossa ujuttamaan myös länsimaalaiseen lainsäädäntöön. Tällä toiminnalla pyritään ylläpitämään valtiovallan asema ja estämään hienovaraisesti esim. kansalaislevottomuutta ja tyytymättömyyden

leviämistä netin välityksellä. Ei ole kovinkaan kauaa aikaa siitä, kun DDR:n salainen poliisi Stasi valvoi myöhään yöllä seuraten sekä terroristeja että tavallisia kansalaisia, jotka kirjoittivat havaintoja uudesta maailmanjärjestyksestä, tekivät kriittisiä elokuvia tai puhuivat julkisesti asioista, joista ei sopinut puhua. Stasilla oli käytössään siihen aikaan uudenlaista pientekniikkaa kuten puhelimiin ja seiniin asetettavia salakuuntelulaitteita, jotka KGB oli todennäköisesti valmistanut Saksan demokraattisen tasavallan hallintokoneistolle. Tähän väliin mainitakseni elokuviin ja sarjoihin (etenkin Hollywoodissa tuotettuihin) on kautta aikojen piilotettu sekä suoria että epäsuoria vihjeitä asioista, jotka ovat monelle silkkaa fiktiota. Esim. James Bond -elokuvista voi poimia viitteitä asiaa koskien, mikäli mielikuvitus janoaa lisätietoa salaisen ase- ja vakoiluteknologian olemassaolosta. Jossain pisteessä tullaan varmasti siihen, että eri maiden tiedustelupalvelut seuraavat ihmisiä ja vallankumouksellisten aatteiden leviämistä Internetin kautta, ja pyrkivät vaikuttamaan toiminnallaan maailman tapahtumiin. Mahdollisten uusterroristien päistä kilpailisivat monet valtiot ja liittoutumat. Muistaa sopii, että joillekin terroristi on toisille vapaustaistelija, kuten tapaus Bin Laden taas kerran todisti. Kuitenkaan tässä terrorismin aikakaudessa eläessämme, ei ole niinkään tärkeää kenen puolella olet tai ketä edustat, vaan sillä tehdäänkö päätökset oikeudenmukaisesti järjellä ja tunteella, eikä vain omia etuja ajaen. Tällä hetkellä Euroopan Unionin jäsenenä Suomenkin elektronisen valvonnan suuntaviivat määräytyvät pitkälti EU:n yhteisten päätösten ja niistä luotujen säädösten pohjalta.

Lähitulevaisuudessa ketä tahansa on mahdollista syyttää terroristiksi vain siksi, että haluaa tietää lisää asioista. Otat esimerkiksi selvää maailman tapahtumista ja uppoudut syvemmälle kanin koloon. Kun huomaat tutkivasi erilaisia asioita Internetissä, saatat poiketa välillä niin kutsutuilla sivuteillä. Jos olet kiinnostunut maailman politiikasta ja päädyt esimerkiksi islamistien blogeille tutkimaan heidän näkökulmaansa asioista, sinusta saattaa jäädä jälki johonkin rekisteriin, jonnekin palvelimelle jossakin päin maailmaa. Lisäksi, jos oletetaan, että olet Facebookissa jonkun ulkomaalaisen ystävän kaveri, jonka ystävä onkin terroristi, saatat joutua seurattavien listalle, jos Suomessa tapahtuu jotakin.

Suomessa tapahtui juuri äskettäin jotakin ja se oli jääkiekon maailmanmestaruuden voitto. Siksi siis Suomessa voi tapahtua myös jotakin suurta. Historiaa tarkasteltaessa olimme olleet pitkään melko takapajuinen valtio Euroopan reunalla, sivistyneen yhteiskunnan ulkolaidoilla. Teknologisen vallankumouksen ansiosta Suomi on siirtynyt periferiasta tapahtumien keskipisteeseen. Tällä hetkellä on suurta merkitystä sillä, mitä ennen niin pieni ja sivistymätön valtio haluaa sanoa esim. Kreikan uudesta tukipaketista. Siksi ulko- ja sisäpolitiikalla on erittäin suuri merkitys myös siihen kohdistuuko Suomeen tulevaisuudessa terroriuhkaa, ja millä keinoilla se pyritään estämään. Jää nähtäväksi tapahtuuko ennaltaehkäisy elektronisen valvonnan lisäämisellä vai provosoimattomalla ulkopolitiikalla. Tässä yhteydessä voisi vertauskuvallisesti sanoa, että jos sohaiset kepillä muurahaispesään, on varmaa että osa muurahaisista yrittää kiivetä keppiä pitkin puremaan sinua.

Mitä tämä kaikki oikein tarkoittaa käytännössä elektronisen valvonnan näkökulmasta? Internetiä käyttää nykyään yksi neljäsosa maailman ihmisistä. Maailma, jossa elämme, on ajautunut pisteeseen, jossa jokaisella uutisella ja asialla on mahdollisuus saavuttaa huomattava julkisuusarvo. Siten tiedolla kuin tiedolla on teoriassa mahdollisuus tavoittaa miltei kaksi miljardia maailman kansalaisista, lähes välittömästi. Samalla jokaisella ihmisellä on multiploitunut mahdollisuus saada juuri oma asiansa kuuluville. Internet on avain valtaan. Vähintään se on viides valtiomahti. Juuri tämän vuoksi se on valtavan suuri huoli eliitille, joka on saanut pitää valta-asemansa kautta ihmiskunnan historian. Virtuaalisen maailman hallittavuus ei ole kenenkään kontrollissa. Internetiin rakennettavat muurit ja esteet eivät tule koskaan olemaan läpäisemättömiä. Tästä huolimatta esteitä tullaan rakentamaan ja tiedon levitystä rajoittamaan. Tämä yritys tapahtuu lakimuutoksilla, sensuurilla ja itsesensuurilla teknologisen kehityksen varjolla. Esim. Yhdysvalloissa on tehty lakialoitteita Internetin rajoittamisesta ja jopa ”sulkemisesta”. Tämän lain voimaantulo antaisi presidentille valtuudet lamauttaa yksityiskäytössä olevat koneet esim. laajamittaisen cyberhyökkäyksen yhteydessä. (Crowley, 2009) Viimeaikaisten uutisten mukaan tämä voisi tapahtua jopa ohjusiskuilla! (Leppänen, 2011).

Toinen esimerkki on EU:n käsittelyssäkin jo ollut kyseenalainen lakipaketti Telecoms Package, josta mm. Piraattipuolueen varapuheenjohtaja Ahto Apajalahti on kirjoittanut mielestäni hyvin ja puolueettomasti blogissaan (Apajalahti, 2009). Netin saisi poikki kokonaan tai osittain Suomessakin tarpeen vaatiessa, sillä Suomen koko verkkoliikenne kulkee käytännössä kolmen ethernet-kytkimen kautta. Laitteita hallinnoi Ficix ry, eikä niiden tarkkoja sijainteja turvallisuussyistä paljasteta. Esim. yksittäisten operaattoreiden poissulkeminen on mahdollista poikkeustilanteissa valmiuslain valtuutuksella. (Mäntylä, 2011.)

Vastavoimana näille aikeille ovat internetin vapautta puolustavat yksittäiset tai verkostoituneet hakkerit, jotka pystyvät halutessaan lamauttamaan kokonaisia verkkosivustoja esim. DoS-hyökkäyksillä ja siten häiritsemään mm. pankkiliikennettä. Esimerkkinä tästä voisi mainita Virossa kohun nostattanut patsaan siirto-operaatio, joka herätti voimakasta vastustusta maan venäläisväestössä. Tämän mielenosoituksen tueksi eräs venäläinen hakkeri toteutti hyökkäyksen Viron valtion virastojen ja pankin verkkosivuja vastaan, tehden ne käytännössä toimintakyvyttömiksi. Toinen vastavoimaa edustava huomattavaa julkisuutta saanut taho on Wikileaks-sivusto. Salaisia asiakirjoja julkaisevalla sivuston perustajalla on paljon sanottavaa muun muassa yksityisyyden suojasta esim. Facebookissa:

> Julian Assangen mukaan Facebook on vaarallinen, "tyrmistyttävä vakoilukone". Assangen mukaan Facebookissa on maailman kattavin tietokanta ihmisistä, heidän osoitteistaan, sijainnistaan ja viestinnästään muiden kanssa. Assangen mukaan kaikki Facebookin, kuten myös Googlen ja Yahoon organisaatiot on rakennettu niin, että niistä saatu tieto on Yhdysvaltain tiedustelupalvelun käytettävissä, Assange sanoo venäläisen Russia Todayn haastattelussa. (Wikileaksin Assange: Facebook on tyrmistyttävä vakoilukone, 2011.)

Facebook Places on suhteellisen uusi Facebook-palvelu, jossa muut käyttäjät voivat seurata missä joku toinen palvelun käyttäjä liikkuu.

> Matkapuhelinversion käyttäjä voi ilmoittaa palvelun avulla oman olinpaikkansa ja tarkistaa kavereidensa olinpaikat. Puutteellisesta tietoturvasta kritisoidun

> Facebookin johto painottaa, että palvelunkäyttäjien yksityisyys on suojattu. Heidän mukaansa käyttäjä voi itse kontrolloida, miten paikkatiedot jaetaan muille. (Uusi Facebook-palvelu kertoo käyttäjän olinpaikan, 2010.)

Samankaltaista teknologiaa käyttää hyödykseen myös esim. Fambit Oy:n tarjoama olinpaikan seurantapalvelu, jonka avulla vanhemmat voivat tarkkailla lastensa liikkeitä Googlen tarjoaman karttapohjan avulla. Tietosuojavaltuutetun, Reija Aarnion mukaan kännyköiden sijaintitietoja hyödyntävä palvelu sisältää riskin tietojen päätymisestä kolmannelle osapuolelle. Fambit Oy:n toimitusjohtaja Pertti Kasanen kuitenkin vakuuttaa, ettei vaaraa ole (Vanhemmat kyttäävät nyt lastensa liikkeitä netistä, 2010). Aiheeseen liittyen ainakin Applen puhelimista on löydetty ongelmallinen tietoturvariski.

> Turvallisuustutkijat ovat saaneet selville, että iPhone tallentaa sekunnin tarkkuudella käyttäjänsä kaikki liikkeet. Tiedot tallentuvat salaiseen tiedostoon käyttäjän puhelimeen sekä tietokoneelle. Tallentamiseen ei erikseen kysytä käyttäjän lupaa. Tallennetut tiedot voivat aiheuttaa turvallisuusriskin, mikäli puhelin tai tietokone joutuvat varkaiden käsiin. Ulkopuolinen voi selvittää omistajan kaikki liikkeet yksinkertaisen ohjelman avulla. Turvallisuustutkijoiden mukaan salainen tieto voidaan siirtää myös uusiin laitteisiin, kun ne synkronoidaan puhelimen kanssa. Tutkijoiden mukaan Apple ei kuitenkaan kerää käyttäjien tietoja tällä hetkellä itselleen. He ovat kuitenkin sitä mieltä, että Apple ei ole ottanut käyttäjien yksityisyyttä vakavasti. (Iphone tallentaa käyttäjän jokaisen liikkeen – toimintoa mahdoton poistaa, 2011.)

Edellä mainitut artikkelit valottavat vain pientä murto-osaa teknologian kehityksen toisesta puolesta ja mahdollisista yksityisyyden suojan loukkauksista, joista puhutaan vasta sitten kun ne paljastuvat. Tällaiset tiedot pyritään yleensä pitämään totaalisessa pimennossa, koska ne todella ovat kyseenalaisia ihmisten yksityisyyden kannalta.

Kuka omistaa yksityisyytesi? Yle Teemalla viime aikoina näytetty Tiededokumentti: Virtuaalivallankumous 3/4 valottaa erittäin hyvin omistamisen käsitteen muutosta. Yksityisyys on tuotteistettu ja sitä voidaan kaupata erilaisin keinoin ilman, että kaupattava henkilö edes tietää antaneensa jotain itsestään. Maailmassa tehdään n. 2 miljardia Google-hakua 40 miljoonalta eri hakijalta

päivittäin (Tiededokumentti: Virtuaalivallankumous 4/4, 2010). On olemassa monia muitakin hakukoneita, mutta tällä hetkellä juuri Google on kasvanut nettimainonnan monopoliksi. Googlen idea pähkinänkuoressa nykyään on antaa ihmisille mahdollisimman räätälöity hakutulos, jotta hakija saisi parhaan mahdollisen vastaavuuden hakemalleen tiedolle. Tämä edellyttää kuitenkin, että annat tiedostaen tai tietämättä valtavan paljon tietoa itsestäsi yritykselle, johon sinun vain on luotettava. Googlea käyttäessä ihmiset luovuttavat käytännössä oman vapaan ajattelunsa pois lahjoittaen sen jollekin muulle, joka tietää paremmin mitä etsivä itse haluaa löytää. Tällä periaatteella, tosin paljon kaunopuheisemmin muotoiltuna, Google markkinoi palvelujaan. Googlen sähköpostiohjelma Google Mail analysoi jokaisen viestin, jonka kirjoitat, ja muuttaa reaaliajassa vaihtuvat mainokset viestissä käytettävien sanojen mukaan. Esimerkiksi jos kirjoitat ”tänään maistuisi yksi olut”, saattaa näkemäsi mainokset ja linkit muokkautua avainsanan ”olut” perusteella, ja siten näet ruudullasi esim. Sinebrychoffin mainoslinkin. Jos tämän käytännössä ajattelee loppuun asti (tai ainakin lähelle sitä), tulevaisuudessa kuinka suuri osa hakukoneeseen syöttämistäsi sanoista on sinun itse keksimiäsi ja kuinka moni on ujutettu päähäsi tällaisella piilomainonnalla? Google on maailmanluokan mainostoimisto, ja sinun henkilökohtaiset tietosi ovat kaupan.

Kenen käsiin nämä kerätyt tiedot päätyvät ja kauanko ne säilyvät tietokannoissa? Yritysten omistajanvaihdosten yhteydessä tiedot yrityksen omistamana vaihtavat omistajaansa. Kenen käsissä nämä tiedot ovat poikkeustilanteissa, jotka erikseen lakeihin säädetään? Poikkeus vahvistaa säännön, sanotaan. Eli poikkeus ei ole säännönmukainen, se vain korostaa sääntöä. Poikkeustilanteissa mitkään normaalioloissa pätevät säännöt eivät päde, ja täten edellä mainittuun tietoon on oikeus sääntöjen keksijällä eli lakeja säätävällä taholla. Myös kansalaisilla pitäisi olla oikeus tähän tietoon, ovathan he itse johtajansa valinneetkin. Kuitenkin tänä päivänä tuntuu siltä, että kaikki kriittinen tieto on niin kovin salaista. Tai sitten ihmisistä on vain tullut uteliaampia, käytettävän koneiston, Internetin siivittämänä.

Kun ajat ovat vaikeita, mikä voi olla hallituksille vaarallisempaa kuin yhdistyneet kansalaiset? Lakiuudistukset ja nykypolitiikka suosivat suuryritysfuusioita, Internetsensuuria, eliitin valtaa, kansalaisoikeuksien kutistamista, köyhyyttä ja eriarvoisuutta. Kun tähän päälle lasketaan vielä elektronisen valvonnan verkko, on asetelmana valvontakoneisto vastaan kansalaiset. Kun kansa harjoittaa sananvapautta, sitä rajoitetaan. Kun ihmiset haluavat vapautta, rakennetaan vankila ilman fyysisiä rajoja, ilman ”kuolleita kulmia”. Kävi tulevaisuudessa miten tahansa, varmaa on, että yhtä ainoaa oikeaa vaihtoehtoa, keskitietä tai totuutta ei tulla löytämään. Sillä totuus on tuolla jossakin – maailman kanin koloissa, tiedon valtateiden katveissa ja sivuteillä. Paikoissa, joista ei puhuta, koska niitä ei ole olemassakaan.

6 POHDINTA

Tämän opinnäytetyön tekemiseen käytetty aika ylitti hieman alkuperäisen suunnitelman mukaiset kehykset ja – johtuen omasta mielenkiinnosta aihepiiriä kohtaan – tiedon kerääminen sekä työn laajuuden hahmottaminen teettivät runsaasti töitä. Olen enemmän kuin tyytyväinen saadessani työni päätökseen ja uskon, että käsiteltävä aihe tulee kiinnostamaan yhä useampia ihmisiä lähitulevaisuudessa. Kuitenkin toivon, että suuri osa työssä esitellyistä uhkakuvista voitaisiin välttää, vaikka ne olisivatkin teknisesti toteutettavissa. Tämä vaatii yhteiskunnan päättäjiltä ja kansalaisilta jatkuvaa tarkkaavaisuutta, jotta voidaan puuttua kyseenalaisiin lakiehdotuksiin ja direktiiveihin ajoissa sekä tuoda esille epäkohtia, joita jo olemassa olevat lait ja asetukset sisältävät.

Työn ehkä merkittävin saavutus itselleni on rohkeus tarttua aiheeseen, josta ei tietääkseni ammattikorkeakoulutasolla ole kovinkaan paljoa käsitelty. Toivottavasti työ herättää lukijoissaan edes jonkin asteista ajattelun muutosta positiivisessa mielessä. Oma tapani lähestyä tietoteknisen kehityksen tulevaisuutta saattaa olla melko skeptinen, jopa synkistelevä, mutta tarkoitukseni on kuitenkin vain valottaa tietoyhteiskunnan pimeimpiä nurkkia, jotta asioista voitaisiin puhua leimaamatta ketään mihinkään ”lokeroon”.

Internetin merkitystä ei tässäkään kohtaa voi olla mainitsematta, sillä tällä hetkellä vain virtuaalitodellisuudessa eri puolilla maailmaa asuvien ihmisten on mahdollista verkostoitua ja vaihtaa mielipiteitään reaaliajassa. Vaikka Internet onkin vain heijastus todellisesta maailmasta, ovat siellä esitetyt asiat ja ajatukset aina todellisia. Yhtä ainoaa totuutta ei ole olemassa, sillä ihmisten maailmankuvat eroavat yhteisöjenkin sisällä huomattavasti. Internetin positiivinen vaikutus piilee mielestäni sen foorumimaisuudessa, sillä avoimella keskustelulla on mahdollista ratkoa pahimmatkin ristiriidat.

Aika näyttää mihin suuntaan tulevaisuuden tietoyhteiskunnat kehittyvät. Jää siis nähtäväksi tulevatko tekniikan sovellukset synnyttämään lisää uusia epäkohtia ja ongelmia, vai pystyvätkö ihmiset muodostamaan järkeviä kompromisseja yhteisten sääntöjen luomiseksi, ihmisten elämänlaadun parantamiseksi.

LÄHTEET

Alhopuro, S. 2011. Osama bin Ladenin kasvot tunnistanutta teknologiaa kehitetään ympäri maailman. Turun Sanomat. 7.5.2011. vko 18.

Apajalahti, A. 2009. Telecoms package – mitä, missä, milloin?. Piraattipuolueen blogi. Viitattu 13.6.2011. http://blog.piraattipuolue.fi/2009/04/telecoms-package-mita-missa-milloin/.

ARPANET. 2011. Wikipedia. Viitattu 13.6.2011. http://fi.wikipedia.org/wiki/ARPANET.

Biopassi. 2011. Wikipedia. Viitattu 13.5. http://fi.wikipedia.org/wiki/Biopassi.

Crowley, K. 2009. The Strategic Defense Initiative (SDI): Star Wars. The Cold War Museum. Viitattu 11.4. http://www.coldwar.org/articles/80s/SDI-StarWars.asp.

Effi: teletunnistetietojen pakkoluovutus Saksassa perustuslain vastainen. 2010. Electronic Frontier Finland. Lehdistötiedote. Viitattu 4.3.2010. http://www.effi.org/uutiset/100304-effi-teletunnistetietojen.html.

Euroopan parlamentin loppuraportti ECHELONista. 2001. Viitattu 13.6.2011. http://cryptome.org/echelon-ep-fin.htm.

EU-parlamentti ei halua luovuttaa kansalaisten pankkitietoja Yhdysvaltoihin. 2010. Helsingin Sanomat. Viitattu 15.9.2011. http://www.hs.fi/ulkomaat/artikkeli/EU-parlamentti+ei+halua+luovuttaa+kansalaisten+pankkitietoja+Yhdysvaltoihin/1135252654997.

Facebook urkkii salasanoja. 2010. Satakunnan Kansa. Viitattu 18.12.2010. http://www.satakunnankansa.fi/cs/Satellite/Kotimaa/1194659168956/artikkeli/keskisuomalainen+facebook+urkkii+salasanoja.html.

Googlen katunäkymäpalvelu keräsi nettiosoitteita ja tunnuksia. 2010. Ilta-Sanomat. Viitattu 23.10.2010. http://www.iltasanomat.fi/ulkomaat/googlen-katunakymapalvelu-kerasi-nettiosoitteita-ja-tunnuksia/art-1288350528504.html.

Iphone tallentaa käyttäjän jokaisen liikkeen – toimintoa mahdoton poistaa. 2011. MTV3. Viitattu 20.04.2011. http://www.mtv3.fi/uutiset/ulkomaat.shtml/2011/04/1316580/iphone-tallentaa-kayttajan-jokaisen-liikkeen---toimintoa-mahdoton-poistaa.

Leppänen, H. 2011. Kybervarustelu käy täysillä. Turun Sanomat. 3.6.2011. vko 22.

Lähes kaikilla alle viisikymppisillä on internet. 2011. Kaleva. Viitattu 18.2.2011. http://www.kaleva.fi/uutiset/lahes-kaikilla-alle-viisikymppisilla-on-internet/889441.

Manning, J & Begich, N. 2004. Angels Don't Play This Haarp, Advances in Tesla Technology. Suomentanut Toivonen, P. Viitattu 25.8. http://www.heinola.org/~patato/HAARP_E3.html.

McCullagh, D. 2009. Bill would give president emergency control of Internet. CNET News. Viitattu 28.3.2011. http://news.cnet.com/8301-13578_3-10320096-38.html.

Mäntylä, J. 2011. Netin saisi poikki Suomessakin. Voima 2/2011, 8.

NSA. 2011. Wikipedia. Viitattu 21.1.2011. http://fi.wikipedia.org/wiki/NSA.

Ruotsi aloitti verkkoliikenteen salakuuntelun: mitä pitää tehdä ja tietää?. 2011. Suomen Kuvalehti. Viitattu 25.8.2011. http://suomenkuvalehti.fi/jutut/talous/ruotsi-aloitti-verkkoliikenteen-salakuuntelun-mita-pitaa-tehda-ja-tietaa.

Tamminen, J. 2010. Googlen Suomi-projekti: ”Iso ja uniikki” – katso kuvat. Uusi Suomi. Viitattu 14.1.2010. http://www.uusisuomi.fi/raha/82276-googlen-suomi-projekti-%E2%80%9Diso-ja-uniikki%E2%80%9D-%E2%80%93-katso-kuvat

Tarvainen, T. 2009. Google näyttää sinulle eri asiat kuin kaverillesi. Electronic Frontier Finland. Viitattu 8.12.2011. http://www.effi.org/blog/2009-12-08-Tapani-Tarvainen.html.

Teppo, A. 2011. Kauppiaat epäilevät vielä kännykkämaksamisen turvallisuutta. Turun Sanomat. 14.5.2011. vko 19.

Tiededokumentti: Virtuaalivallankumous 1/4. 2010. Esitetty 7.5.2011 Yle Teema.

Tiededokumentti: Virtuaalivallankumous 2/4. 2010. Esitetty 14.5.2011 Yle Teema.

Tiededokumentti: Virtuaalivallakumous 4/4. 2010. Esitetty 26.5.2011 Yle Teema.

Uusi Facebook-palvelu kertoo käyttäjän olinpaikan. 2010. Turun Sanomat. Viitattu 19.8.2010. http://www.ts.fi/online/talous/154130.html.

Uusi pakkokeinolaki uhkaa heikentää tietoturvaa. 2011. Helsingin Sanomat. Viitattu 25.2.2011. http://www.hs.fi/politiikka/artikkeli/Uusi+pakkokeinolaki+uhkaa+heikent%C3%A4%C3%A4+tietoturvaa/1135264077147.

Wallenius, J. 2011. Valon kvanttien ja hiukkasten yhteispeli mahdollistaa kvanttitietokoneen. Turun Sanomat. 31.5.2011. vko 22.

Vanhemmat kyttäävät nyt lastensa liikkeitä netistä. 2010. Kaleva. Viitattu 2.6.2010. http://www.kaleva.fi/uutiset/Vanhemmat-kyttaavat-nyt-lastensa-liikkeita-netista/857094.

Varo: Facebook-kaverisi voikin olla agentti. 2010. Etelä-Suomen Sanomat. Viitattu 17.3.2010. http://www.ess.fi/?article=275064.

Wikileaksin Assange: Facebook on tyrmistyttävä vakoilukone. 2011. Helsingin Sanomat. Viitattu 3.5.2011. http://uutiset.msn.hs.fi/ulkomaat/artikkeli/Wikileaksin+Assange+Facebook+on+tyrmistytt%C3%A4v%C3%A4+vakoilukone/1135265847758.

Yhdysvallat tutkii Googlen kotiverkkojen urkintaa. 2010. Aamulehti. Viitattu 22.6.2010. http://www2.aamulehti.fi/uutiset/ulkomaat/yhdysvallat-tutkii-googlen-kotiverkkojen-urkintaa/182353.

.