Opinnäytetyö (YAMK)

Yrittäjyys ja liiketoimintaosaaminen

Tradenomi (YAMK)

2015

Senjariitta Auvinen

DIGITALISAATIO JA TIETOTURVA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Yrittäjyys ja liiketoimintaosaaminen

Opinnäytetyön valmistumisajankohta | Sivumäärä

Eija Koivisto

Senjariitta Auvinen

DIGITALISAATIO JA TIETOTURVA

Tämän opinnäytetyön tarkoituksena on pyrkiä nostamaan esille tietoturvaan liittyviä näkökulmia yhä kiihtyvällä vauhdilla digitalisoituvassa työelämässä. Työssä käydään läpi digitalisaation mukanaan tuomia ilmiöitä, ja pyritään selvittämään mitä pitää ottaa huomioon sähköisessä maailmassa jotta pienentäisimme riskiä joutua rikoksen uhriksi. Lainsäädännön tarkoitus on suojata oikeuden omistajaa, mutta sähköisen maailman lainalaisuudet eivät kuitenkaan toimi samoin kuin reaalimaailmassa, eikä rikosten selvittäminen ole helppoa.

Kyberturvallisuuden perusasiat on hyvä ymmärtää jokaisen yksittäisen käyttäjän, mutta tässä työssä näkökulma painottuu kuitenkin työpaikoille riippumatta siitä, ollaanko työntekijän tai -antajan ominaisuudessa. Heikoin lenkki on liian usein yksittäinen työntekijä, vaikka ei olisikaan kyse tahallisuudesta, vahinko voi tapahtua myös tietämättömyydestä, sillä liian usein ei tiedetä, miten uudessa ympäristössä pitää toimia.

Työntekijänä henkilöön voi kohdistua tiedustelu tai vakoiluyrityksiä, tavoitteena esimerkiksi varastaa yrityksen yrityssalaisuuksia kyseisen tuotteen valmistamiseksi ja tuottamiseksi ensimmäisenä markkinoille, tai viranomaisen salassa pidettäviä tietoja osana valtioiden välistä tiedustelua. Usein pyrkimyksenä on saada tietoja organisaation tietojärjestelmistä ja –verkoista, tavoitteena vaikuttaa organisaation toimintaan myöhemmin.

Vihamielisiä kyberhyökkäyksiä raportoidaan maailmanlaajuisesti päivittäin. Ne kohdistuvat niin yksilöihin, yrityksiin kuin valtioihinkin. Siksi on tärkeää että, jokainen ymmärtää kyberturvallisuuden perusperiaatteen samalla tavalla kuin esimerkiksi liikenneturvallisuuden.

ASIASANAT:

digitalisaatio, tietoturva, tietoturvastrategia, lainsäädäntö

MASTER´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Master's Degree Programme in Entrepreneurship and Business Competence

Completion year of the thesis | Total number of pages

Eija Koivisto

Senjariitta Auvinen

DIGITALIZATION AND SECURITY

The purpose of this study is to highlight aspects of information security at an accelerating pace digitalizing workplace specifically to ordinary workplace for operators. A standard operator shall mean those persons who do not have a background in cyber security or information security experts, but employees, regardless of their status in workplace, who use information technology to every day.

The thesis examines the phenomena brought about by digitalization with them and seeks to determine what needs to be taken into account in the electronic world in order to minimizing the risk of becoming a victim of crime. Purpose of the legislation is to protect the owner the right, but the electronic world laws do not work as well as in the real world and investigation of crimes is not easy.

Every individual user need to understand the cyber security basics but in this work perspective focuses on the workplace, regardless of whether you are in capacity as employee or owner. The weakest link is all too often an individual employee, even in the absence of intentional, damage may also occur because of ignorance. Too often it is not known how to act in the environment must.

An employee can be contacted for spying purposes, for example, to steal the company's corporate secrets in order to ensure access to the market first or to get confidential information of the Authorities as part of intelligence between countries. Often, the aim is to get information about the organization's information systems and networks aim of affect the operation of the organization later.

Hostile cyber-attacks are reported worldwide each day. They are aimed at both individuals as companies as well as the state, therefore, important that each one understands the basic principle of cyber security in the same way as, for example, road safety. Just being aware of the general risks and using common sense will help a long way and that is an aim of this work.

KEYWORDS:

digitalization, security

SISÄLTÖ

KUVAT

1 JOHDANTO

1.1 Työn taustaa

Melko lyhyessä ajassa on otettu käyttöön monia uusia teknologioita kiinnittämättä juuri lainkaan huomioita sen kaikkiin vaikutuksiin, niin yksittäisiin kansalaisiin kuin jopa kokonaisiin yhteiskuntiin. Digitaalinen maailma ei tunne rajoja, mikä edellyttäisi päättäjiltä mahdollisimman yhtenäistä kansainvälistä lainsäädäntöä ja pelisääntöjä. Meidän tulisi varautua niihin vaikutuksiin, joita digitalisaatio aiheuttaa joko suoraan tai välillisesti. Dekaani Pekka Neittaanmäen mukaan 80 prosenttia yritysten tuottavuuden kasvusta on tullut viimeisen kymmenen vuoden aikana, pääsääntöisesti tietoliikenneyhteyksien hyödyntämisestä. (Peltomäki-Norppa 2015, 16.)

Digitaalitekniikka on suuri mahdollisuus, mutta nostaa esiin myös uusia ongelmia, sillä digitaalista elämää on helppo seurata ja tallentaa sillä ne asiat, joita olemme tottuneet pitämään luottamuksellisina ja henkilökohtaisina, ovatkin hakkerien ja nettiyritysten helposti hankittavissa. Kuten Petteri Järvinen on todennut, yksityisyys rapautuu niin nopeasti, että ajatukset ovat pian ainoa pakopaikka, johon sähköinen valvonta ei yllä. (Järvinen 2014, 11.)

Viime aikoina julkisuudessa on paljon puhuttu kahdesta käsitteestä, jotka tavallaan ovat saman asian kääntöpuolet, nimittäin kyberturvallisuus ja kyberrikollisuus. Palvelunestohyökkäykset, urkinta, vakoilu, wikileaks, laiton lataaminen, phishing, kyberterrorismi ja –vandalismi sekä identiteettivarkaudet ovat joitakin niistä sanoista ja termeistä, joita kuulemme lähes päivittäin. Rikolliset ja muut netin väärinkäyttäjät löysivät nopeasti verkon ja sitä kautta ihan tavalliset kansalaiset ja yrittäjät. Suomessa useat yritykset ovat joutuneet muun muassa palvelunestohyökkäysten kohteeksi, ja haittaohjelmat ovat tulleet kansalaisten kasvavan päätelaitevalikoiman kautta arkeen mukaan. Esimerkiksi käyttäjätunnuksista ja salasanoista on tullut kauppatavaraa, ja kyberrikollisuus kasvaakin nopeasti, koska voitot ovat suuria, mutta toisaalta kiinnijäämisen riski usein pieni. On arvioitu, että vuonna 2014 kyberrikollisuuden aiheuttamat tappiot

maailmantaloudelle nousevat jo yli 400 miljardiin dollariin. (Peltomäki-Norppa 2015, 6.)

1.2 Työn tavoite ja tutkimusongelma

Tutkimusongelmasta määrittyvät tutkimusaiheen tarkoitus ja tavoitteet, ja tutkimuskysymyksillä saadaan ratkaisu tutkimusongelmaan. Tutkimusongelma voi löytyä käytännön työelämästä tai aihealueeseen perehtymällä. (Kananen 2008, 51.) Tämän työn tavoitteena on selvittää, miten tämän hetkinen lainsäädäntö on ottanut huomioon toimintaympäristömme muuttumisen sähköiseksi, ja mikä on yksittäisen käyttäjän vastuu tietoturvasta tässä ympäristössä. Sähköiselle maailmalle ei juuri enää ole vaihtoehtoja, ja yksityisyydestä on tullut ylellisyyttä, johon vain rikkailla tai taitavilla tietotekniikan taitajilla on mahdollisuus. Työssä keskitytään erityisesti yritysten tietoturvaan ja uhkiin, ja mitä niille voidaan tehdä. Tietoturvakonsultti llkka Demanderin mukaan on kahdenlaisia verkkorikoksen uhreja, niitä jotka ovat joutuneet hakkeroiduiksi ja niitä, jotka tulevat hakkeroiduiksi jossain vaiheessa. (Peltomäki-Norppa 2015, 14.)

1.3 Tutkimusmenetelmä

Tutkimusmenetelmänä on laadullinen eli kvalitatiivinen menetelmä, jossa pyritään ymmärtämään tutkittavaa ilmiötä. Kvalitatiivinen tutkimus tarkoittaa sellaista tutkimusta, joka ei perustu tilastollisiin tai määrällisiin menetelmiin. (Kananen 2008, 24.) Aineistona tutkimuksessa on käytetty valmista aineistoa. Tutkimusongelmaa pyritään ratkaisemaan käyttämällä lähteinä lainsäädäntöä, viranomaisohjeita, artikkeleita ja uusinta alan kirjallisuutta sekä työelämässä kertynyttä tietoa. Laadullisessa tutkimuksessa havainnointi on samalla tiedonkeruuta ja analyysia. (Kananen 2008, 86.) Tutkimuksen avulla pyritään ymmärtämään tutkimuksen kohteena olevaa ilmiötä sekä selittämään tähän ilmiöön liittyvien toimijoiden käyttäytymiseen ja päätöksiin liittyviä syitä.

Tämä opinnäytetyö on luonteeltaan kirjoituspöytätutkimus. Kirjoituspöytätutkimus on kirjallinen työ, jossa eri lähteitä hyväksikäyttäen selvitetään jotain kysymystä tai ongelmaa. Valmiita aineistoja hyödyntävää tutkimusta kutsutaan kirjoituspöytätutkimukseksi (Mäntyneva, Heinonen & Wrange 2008, 29). Kirjoituspöytätutkimuksessa yksi olennaisimmista seikoista on käyttää luotettavia ja ajantasaisia lähteitä. Mäntyneva ym. (2008) luokittelevat lähteet kahteen eri luokkaan, joita ovat organisaation sisäiset tai ulkoiset lähteet. Sisäisiä lähteitä ovat esimerkiksi koottu asiakaspalaute ja myynnin raportit. Erilaiset tilastot, ammattilehdet, alan kirjallisuus ja tutkimustulokset taas luokitellaan ulkoisiksi lähteiksi.

2 DIGITALISAATIO

2.1 Tietoyhteiskunnan kehitys

Ensimmäinen tietokoneen keksimisestä on eri tietolähteissä erilaisia näkemyksiä, mutta merkittävänä yleisesti pidetään vuotta 1946 kun USA:n armeijan ENIAC -tietokone julkaistiin. Tämän jälkeen tietotekniikan kehitys on ollut nopeaa mitä vielä vauhditti 1960 luvulla alkunsa saanut internet eli verkko johon tietokoneet liitettiin. (Hiltunen-Hiltunen 2014, 185.)

2000-luku oli kuitenkin tietoverkkojen ja päätelaitteiden nopean kehityksen vuosikymmen. Käytämme verkkoja ja niissä toimivia laitteita päivittäin henkilökohtaisen elämämme hallintaan, viestintään ja työntekoon. Tässä luomassamme rinnakkaistodellisuudessa liikkuu paljon rahaa ja tietoa. Monet näistä arkisistakin toiminnoista eivät kuitenkaan ole olleet verkossa kuin hetken verrattuna koko ihmiskunnan historiaan.

Suomalainen omisti 1990-luvulla keskimäärin yhden internetiä hyödyntävän päätelaitteen, kun taas tänä päivänä tavallisessa suomalaisperheessä on jopa 10 erilaista laitetta, jotka ovat jatkuvasti yhteydessä nettiin. Tietokoneen lisäksi verkossa ovat mm. älypuhelimet, tabletit, pelikonsolit ja talojen valvontajärjestelmät. Suomesta pyrittiin määrätietoisesti rakentamaan tietoyhteiskuntaa. Lisäksi päätelaitteiden hinnat sekä viestiliikenteen ja internetin käyttömaksut ovat Suomessa 20 prosenttia alle eurooppalaisen keskitason. (Peltomäki-Norppa 2015, 17-18.)

2.1.1 Digitaaliteknologia

Tietoverkkojen myötä tulivat myös niitä hyödyntävät päätelaitteet, älypuhelimet ja tabletit, joilla internet palveluineen on käytettävissä kaikkialla. Älypuhelin on päätelaite, jolla voi perinteisten puheluiden lisäksi lukea sähköpostia, lukea ja jakaa kuvia sekä ladata sovelluksia, kun taas tabletti on kosketusnäytöllinen

taulutietokone. Ensimmäiset älypuhelimet tulivat markkinoille vuonna 2001, kun myyntiin tuli Nokian 3330 matkapuhelinmalli, jossa oli uusi mullistava keksintö ns. WAP-palvelu. Puhelimet olivat kalliita, ja siksi niitä myytiin lähinnä yrityskäyttöön. Vuonna 2006 Apple julkaisi ensimmäisen iPhonen, ja älypuhelinten maailmanvalloitus alkoi. Nykyisin lähes kaikki suomalaisoperaattoreiden myymät puhelimet ovat älypuhelimia, ja perässä tulivat melko pian tabletit, vaikka median ensireaktiot Applen iPadille olivat murskaavat. Laitetta kuvattiin isoksi iPhoneksi, jolla ei vain voinut soittaa. Alkuvaiheen arvosteluista huolimatta tabletteja löytyy nykyään lähes joka perheestä. Vuonna 2014 suomalaisiin koteihin myytiin eri arvioiden mukaan noin 800 000 kappaletta eri valmistajien tablet-tietokonetta. Nopeasti älypuhelimesta ja tabletista on tullut itsensä toteuttamisen, sosiaalisen kommunikoinnin, tiedon haun ja kuluttamisen väline. (Peltomäki-Norppa 2015, 19-20.)

Digitaaliteknologian kehitys on vaiheessa, jossa sen vaikutukset näkyvät lähes kaikilla toimialoilla, organisaatioissa, ajattelutavoissa, yhteiskunnan rakenteissa ja instituutioissa. Monet perinteisen fyysisen maailman rakenteet ovat muuttumassa, sillä kuluttajista on tullut tuottajia ja tuottajista kuluttajia. Virtuaalimaailma tarvitsee omat pelisäännöt, mikä tarkoittaa, että esimerkiksi aineettomat oikeudet olisi määriteltävä uudelleen. Toisin kuin fyysisessä maailmassa, globaali tietoverkko on sekä tuotantokoneisto että myös jakelukanava. Taloustieteilijä Brian Arthur (2011) mukaan muotoutumassa olevaa taloutta voisi kutsua nimellä second economy. Käsitteellä Arthur tarkoittaa sitä, että vanhan talouden rinnalle on kehittymässä toinen talous, jonka rakenteet ovat syntyneet osin huomaamatta ja ovat vaikeasti havaittavissa, koska näkyvän talouden rinnalle on huomaamattomasti syntynyt piilotalous. (Lehti-Rouvinen-Ylä-Anttila 2012, 6.)

Digitaalisaatio vaikuttaa maailmantalouteen yhdistämällä talouksia ja yhteiskuntia rajattomaksi maailmaksi, ja ensimmäistä kertaa maailmanhistoriassa lähes kaikki maat ja alueet ovat saman globaalitalouden piirissä. Monet kansalliset instituutiot muuttuvat kuitenkin hitaasti, ja toisaalta niiden kansallinen tai paikallinen luonne saattaa vain voimistua vastareaktiona

globalisaatioon. Siitä huolimatta, että yritykset toimivat globaalisti, ja maailmankauppa on vapautunut, lainsäädäntö on suurelta osin kansallista. Globaali tietotalous on täynnä eturistiriitoja, koska globaaleja pelisäännöt ovat riittämättömät. Tämä näkyy osaltaan myös siinä, että digitaalisten sisämarkkinoiden luominen Eurooppaan on osoittautunut erittäin vaikeaksi tehtäväksi. Julkisella sektorilla digitaaliteknologian vaikutukset ovat näkyneet hitaammin, koska kehitys on suurelta osin markkinavetoista. (Lehti-Rouvinen-Ylä-Anttila 2012, 8.)

On lukuisia esimerkkejä siitä, miten digitalisaatio ja globalisaatio ovat kietoutuneet toisiinsa ja muuttavat siten yhdessä maailmaa. Digitaaliteknologia on mahdollistanut sen, että monenlaiselle luovuudelle syntyy globaalit mikromarkkinat, jolloin ihmiset voivat hypererikoistua, jolloin voidaan tarjota hyvin kapeaa osaamista globaalisti. Berkeleyn yliopiston professori ja Googlen pääekonomisti Hal Varian kutsuu näitä toimijoita monikansallisiksi mikroyrityksiksi, mikä tarkoittaa, että kuka tahansa voi verkon välityksellä tulla globaalisti toimivaksi yrittäjäksi. (Lehti-Rouvinen-Ylä-Anttila 2012, 11.)

2.1.2 Digitaalitalous

Digitaalitalouteen liittyvästä yli-innostuksesta ei aina pysty erottamaan sitä osaa, mikä olisi realistista. Julkisuudessa on luotu kuvaa pilvipalveluista, jossa kaikki digitalisoitavissa oleva tieto ja tietokoneiden käyttämät ohjelmistot ovat yhdessä tietovarastossa ja aiemmin erilliset laitteet kuten matkapuhelimet, tietokoneet, radio ja TV olisivat tulevaisuudessa vain vaihtoehtoisia päätelaitevalintoja. Osittain tämä visio on toteutunut, mutta pilvipalveluiden tarjoamiseen liittyy kuitenkin paljon tietämättömyyttä, epävarmuutta ja ratkaisemattomia kysymyksiä, joista keskeisimmät liittyvät tietoturvaan ja pilvipalveluiden globaaliin hallintaan. Käsitteisiin big data ja 3D-tulostus liittyi vielä muutama vuosi sitten paljon epävarmuutta, onko todella mahdollista dataa louhimalla ratkaista yhteiskunnan suuria ongelmia, tai luoda uutta liiketoimintaa, tai voimmeko joskus tulostaa uuden vasaran tai keittiöveitsen kotona. Vaikka teknologia esineiden

tulostamiseen olisi nyt olemassa, emme ole pystyneet ratkaisemaan niitä monia lainsäädännöllisiä ja eettisiä ongelmia, joita datan louhiminen on nostanut esiin. (Lehti-Rouvinen-Ylä-Anttila 2012, 11.)

Huolimatta monista epävarmuuksista, joita vielä on olemassa, internetin läpimurron luoma digitaalitalous on tulossa todellisuudeksi. Vaikka talous muuttuu yhä enemmän palvelutaloudeksi, silti ei ole odotettavissa teollinen toiminta katoaisi kokonaan. Verkossa palvelun tuottamiseen tarvitaan kuitenkin usein teollisuustuotetta, ja monien teollisuustuotteiden käyttäminen taas vaatii siihen integroitavaa palvelua. Fyysinen ja sähköinen maailma jatkavat silti kilpailua kuluttajista, ja yhä useammin sähköinen maailma on saanut voiton. Sähköisen median kasvu perinteisen paperisen tiedonvälityksen kustannuksella on konkreettisimpia esimerkkejä, ja Suomen kannalta se on yksi merkittävimmistä tässä kehityksessä. Vastaava kehitys näkyy esimerkiksi Yhdysvalloissa, jossa alle 35-vuotiaista enää viidennes lukee päivittäin sanomalehteä, kun taas yli 65-vuotiaista niin tekee 60 prosenttia. Yksilöiden väliset tuottavuuserot kasvavat digitalisaation myötä, mikä on jo näkynyt viime vuosikymmeninä. Tuottavuuserojen kasvu selittyy sillä, että ICT-osaajan tuottavuus voi olla jopa satoja kertoja suurempi kuin tietotekniikkaa osaamattoman. Perinteisessä teollisuusyhteikunnassa näin suuria tuottavuuseroja ei syntynyt. (Lehti-Rouvinen-Ylä-Anttila 2012, 12-13.)

2.1.3 Digitaalitalouden ja teknologian kansainvälinen vertailu

Digitaalisaation vaikutuksia olisi tärkeä pohtia juuri nyt, sillä mikäli yleiskäyttöinen teknologia saa aikaan pitkään jatkuvan (eksponentiaalisen) kasvun, niin sen surauksia voi olla vaikea käsittää. Kahden teollisen vallankumouksen seurauksena monissa maissa on havaittu tapahtuneen vastaavanlainen kehitys, jolloin kasvu oli aluksi vaatimatonta mutta kiihtyi myöhemmin. Kansallisesena ongelmana on pidettävä sitä, että digitaaliteknologian soveltajana Suomi näyttää jäävän yhä kauemmas maailman kärjestä. Tilastot vuodelta 2015 kuvaavat tilannetta hyvin (kuva 1). (Digibarometri 2015, 19.)

Kuva 1. Edellytykset digitaalisuuden hyödyntämiseen (Digiparometri 2015, 19).

Suomella on kokonaisuutena vertailun parhaat edellytykset digitaalisuuden hyödyntämiseen. Suomen jälkeen tulevat Tanska ja Ruotsi (kuva 1). Myös Alankomaissa ja Norjassa edellytykset ovat parhaasta päästä. Yllättävää sen sijaan on, että häntäpäästä löytyvät BRIC-maat ja Italia sekä Itävalta ja Saksa. Käytössä kärkikolmikkona ovat pohjoismaiset kumppanimme Tanska, Norja ja Ruotsi. Lisäksi Suomen ohi ajaa Alankomaat (kuva 2).

Kuva 2. Digiteknologian käyttö (Digiparometri, 19).

Suomi peittoaa niukasti Yhdysvallat, ja reilusti taakse jäävät esimerkiksi Iso-Britannia, Japani ja Saksa, joka on yllättäen vertailun toiseksi viimeisenä. Vain Italia menestyy Saksaa heikommin. Myös Itävalta kerää heikot pisteet digin käytössä. (Digiparometri 2015, 18.)

Tällä kehityksellä saattaa olla merkittäviä seurauksia siksi, että Nokian ihmeen jälkeen Suomen asema ICT:n tuottajana on heikentymässä, emmekä soveltajina olleet päässeet muita edelle, ennen kuin putoaminen tuottajakärjestä alkoi. Digitaaliteknologian soveltamisessa ensimmäinen hyötyy aina eniten, minkä vuoksi pitäisi pyrkiä olemaan muita edellä, sillä muuten joutuu saamaan viimeisimmät digitaaliset innovaatiot tuontitavarana. Tosin Suomelle voisi olla mahdollisuus se, että ICT:n tuotannosta on vapautunut viime aikana tuhansia hyvin koulutettuja tieto- ja viestintäteknologian ammattilaisia. Heidän taitoaan ja osaamistaan tulisi käyttää kaikilla aloilla, jolloin digitaalisen palvelutalouden kasvun tarvitsemaa inhimillistä pääomaa on jo olemassa. (Lehti-Rouvinen-Ylä-Anttila 2012, 13-15.)

2.2 Digitaalisuus ja sähköinen asiointi

Digitaalisuudella tarkoitetaan sähköisessä muodossa olevan tiedon käsittelyä, siirtämistä ja varastointia sekä esittämistä, ja tieto sijaitsee yleensä erilaisissa tietokannoissa, ja tiedon rakenne määritellään tietokantaohjelmistoilla. Digitaalista tietoa siirretään ja käsitellään sovelluksilla tai ohjelmistoilla, jotka ovat myös itsessään sähköisessä muodossa tuotettuina joillakin tunnetuista ohjelmistokielistä. Digitaalinen tieto kulkee tietoverkoissa joko langattomasti tai langallisesti. Digitaalisessa muodossa olevaa tietoa on yleisesti ottaen tehokkaampi ja nopeampi käsitellä, siirtää, esittää ja varastoida kuin perinteisesti fyysisessä muodossa olevaa tietoa, kuten esimerkiksi paperia. (Lahti-Salminen 2014, 19.)

Organisaatioiden välinen tiedonsiirto on teknologiana ollut olemassa jo kolmen vuosikymmenen ajan, mutta silti sen käyttö ei ole niin laajalle levinnyt kuin teknologian olemassa olo olisi edellyttänyt. Organisaatioiden välisellä

tiedonsiirrolla (OVT, eng. Electronic data interchange EDI) tarkoitetaan määrämuotoista, automatisoitua ja ennen kaikkea sähköistä tiedonvaihtoa yritysten välillä. (Lahti-Salminen 2014, 20.)

Sähköinen asiointi puolestaan tarkoittaa sähköisessä muodossa sähköpostin, internetin tai muun tietoverkon yli tapahtuvaa asiointia ja digitaalisen tiedon käsittelyä. Käytännössä sähköisellä asioinnilla tarkoitetaan erilaisia asioita, joita on mahdollista hoitaa verkossa tai sähköpostin välityksellä. Myös tiedonhaku ja sähköisten lomakkeiden käyttö, esimerkiksi viranomaisten verkkosivuilla on sähköistä asiointia. Yritysten ja organisaatioiden toiminnassa sähköisestä asioinnista käytetään yleisesti termejä sähköinen liiketoiminta, sähköiset tai digitaaliset palvelut. Sähköistä liiketoimintaa kuvataan myös erilaisilla e-alkuisilla termeillä, kuten esimerkiksi e-liiketoiminta tai e-kauppa.

Sähköiset palvelut ja verkkokauppa ovat kasvaneet voimakkaasti 1990-luvun loppupuolelta saakka ja nykyään lähes kaikilla internettiä tai sähköpostia käyttäneistä henkilöistä ja yrityksistä on kokemuksia sähköisestä asioinnista. Yleisimpiä sähköisen asioinnin palveluita Suomessa ovat pankki- ja vakuutuspalvelut sekä erilaiset julkishallinnon tietopalvelut, kuten verottajan Kelan ja työministeriön sivut. Myös yritysten ja kuluttajien sekä muiden organisaatioiden harjoittama kauppa ja liiketoiminta tapahtuvat yhä enemmän tietoverkkoja hyödyntäen. (Lahti-Salminen 2014, 21.)

Verkkokaupalla tai e-liiketoiminnalla tarkoitetaan internetissä tapahtuvaa tuotteiden ja palveluiden kauppaa, ja liiketoimintaan liittyvien prosessien käsittelyä. Käytetyimpiä kaupallisia verkkopalveluita ovat pankkipalveluiden käyttö sekä matkojen ja matkalippujen ostaminen, mutta verkossa käydään myös digitaalisten tuotteiden ja palveluiden kauppaa, kuten musiikin, tiedon sekä matka- ja pääsylippujen ostamista ja jakelua. Erittäin nopeasti kasvava alue on myös fyysisten tuotteiden verkkokauppa, erityisesti vähittäis- ja erikoiskaupan tuotteet, kuten vaatteet, elektroniikka ja elintarvikkeet. Verkkopalvelu voidaan jakaa käsitteellisesti myös viestinnällisiin verkkopalveluihin ja operatiivisiin verkkopalveluihin. Viestinnälliset verkkopalvelut jakaantuvat joko informaatioon tai viihteeseen, jossa käyttäjä hyötyy palvelussa olevasta tekstistä, kuvista,

äänestä tai elävästä kuvasta. Operatiivisessa verkkopalvelussa puhutaan todellisista palveluista, joihin liittyy yleensä materiaali- tai palveluvirtaa, jamaksullisia palvelut ovat yleensä. (Lahti-Salminen 2014, 22.)

Digitaalinen taloushallinto on yleistynyt Suomessa lähes kaikkia ennusteita hitaammin, ja Suomi on menettänyt etumatkansa sähköisen taloushallinnon edelläkävijänä. Vielä 2000-luvun alussa näytti siltä, että Suomesta olisi voinut syntyä jopa kokonainen menestyvä klusteri, ja merkittävää kansainvälistä kasvua ja vientiä edustava toimiala sähköisen taloushallinnon ympärille. Suomi mahdollisti lainsäädännöllään sähköisen taloushallinnon ja paperittoman kirjanpidon jo vuonna 1997. Yhtenä esteenä sähköisen taloushallinnon kehitykselle on ollut puute sopivista taloushallintojärjestelmistä. Lisäksi ihmisten ja organisaatioiden kyky omaksua uusia nopeasti kehittyviä teknologioita ja toimintamalleja vaativat oman aikansa. (Lahti-Salminen 2014, 30.)

2.3 Fyysisen ja virtuaalimaailman yhteensulautuminen

Sana kyber tarkoittaa digitaalista maailmaa ja kaikessa laajuudessaan sitä bittien maailmaa, joka ympärillämme on, ja joka vaikuttaa päivittäiseen elämäämme voimakkaammin kuin aina edes käsitämme. Käsitteenä se usein rinnastuu kybertoimintaympäristöön tai kybermaailmaan, sillä harvoin kuitenkaan kyberiä käytetään yksittäisenä sanana. Kyber on enemmänkin digitaalista maailmaa kuvaavan yhdyssanan etuliite, joka saa merkityksensä vasta kun siihen liitetään loppuosa, kuten kyberrikollisuus, kyberuhka tai kyberturvallisuus. (Limnéll-Majewski-Salminen 2014, 29.)

Kyber sanana on peräisin kreikan sanasta kybereo - ohjata, opastaa, hallita. Aina siihen saakka, kun kirjailija William Gibson tieteiromaanissaan Neurovelho (alkuteos ilmestyi vuonna 1984, suomennos 1991) yhdisti kyber- ja space sanat yhdeksi kokonaisuudeksi, kyber oli tunnettu kybernetiikka tutkimusalan määrittäjänä. Kybernetiikan juuret johdetaan Norber Wienerin vuonna 1948 julkaisemaan teokseen Cybernetics: Or Control and Communication in the Animal and the Machine, jossa hän tutkii ohjaamisen ja valvonnan (control)

suhdetta viestintään. Wienerin mukaan tehokas toiminta vaatii ennen kaikkea viestintää, oli sitten kyse orgaanisen tai mekaanisen järjestelmän ohjaamisesta. (Limnéll-Majewski-Salminen 2014, 29.)

Kybernetiikka tutkii erilaisten järjestelmien viestintää, ohjaamista tai ohjautumista, sekä yleisesti itseohjautuvia automaattisesti säätyviä systeemejä. Se on systeemiteoriaan pohjaava poikkitieteellinen tutkimusala, jonka keskeisiä kysymyksiä ovat, mitä jokin asia tekee, tai mitä se voi tehdä. Toiminnan aikaansaava asia taas voi olla lähestulkoon mikä tahansa muuttuja inhimillisissä, keinotekoisissa tai luonnon järjestelmissä. Järjestelmänä voi silloin olla esimerkiksi kieli, tieteenala, teknologian eri sovellutukset tai vaikka sosiaaliset käytännöt kuten koulutus, taide ja johtaminen. (Limnéll-Majewski-Salminen 2014, 29-30.)

Historiallisesti kybernetiikalla on oma painolastinsa, koska se leimattiin 1950- ja 1960-lukujen taitteesta alkaen erityisesti neuvostoliittolaiseksi tieteeksi. Neuvostoliitossa kybernetiikasta muovautui tuolloin liike, jonka tavoitteena oli vapauttaa tiede stalinistisista opeista ja pyrkiä siten uudistamaan tiedemaailmaa. Käytännön sovellutuksena yhteiskunnassa kybernetiikka auttaisi lunastamaan kommunismin lupaukset. Ideologisesti kybernetiikka oli tiede kommunismin palveluksessa, mikä aiheutti vastaliikkeen länsimaissa. Kybernetiikasta vaiettiin tai puhuttiin uhkaavaan sävyyn, eikä sen kehittämiseen panostettu. Kuitenkin vähitellen kybernetiikka yhdistyi voimakkaammin tietokoneisiin, joista taas tuli kehityksen symboli. 1970-luvulta alkaen Neuvostoliitossa herättiin kybernetiikan vallankumouksellisista unelmista, ja toisaalta tieteenalaa kohtaan tunnettu vastenmielisyys länsimaissa alkoi vähentyä. 1980 luvulta alkaen tietokoneiden kehitys on ollut nopeaa, ja viimeistään internetin esiinmarssi 1990-luvulta lähtien on toteuttanut kyberneettisen unelman ihmisten ja koneiden saumattomasta yhteistyöstä osana arkipäivää. (Limnéll-Majewski-Salminen 2014, 30.)

Kybermaailma on tullut osaksi päivittäistä elämäämme ja sen myötä on alettu käydä keskustelua siitä, missä määrin kyberturvallisuus on sama asia kuin tietoturvallisuus, verkkoturvallisuus tai tietokoneturvallisuus. Rajapintoja ja päällekkäisyyksiä käsitteiden määrittelyissä on, ja kyberille löytyy maailmalla

satoja erilaisia määrittelyjä. Käsiteanalyyseihin ei kuitenkaan kannata kiinnittää liiaksi huomiota, vaan pelkistäen todeta, että kyber tarkoittaa bittien maailmaa. Kyber sanana kuvaa myös hyvin fyysistä ja digitaalista rajapintaa, kyberfyysistä maailmaa, jossa elämme. Kyber strateginen käsite, joka yhdistää datan informaation ja tiedon osaksi kokonaisvaikutusta, ja pyrkimystä ohjailla tuota vaikutusta oikeaan suuntaan. Kyber kuvaa muita termejä paremmin koko bittien maailmaa, josta nykymuotoinen elämämme, liiketoimintamme ja yhteiskuntamme ovat hyvin riippuvaisia. Kansainväliseen kielenkäyttöön sana on vakiintunut myös yleisesti. (Limnéll-Majewski-Salminen 2014, 30-31.)

Nykyään on vaikea kuvitella yhteiskuntien toimintoja tai yritysten tarjoamia palveluja irrallaan bittien maailmasta. Yhteiskuntamme ja koko länsimainen elämäntapamme on riippuvainen digitaalisen maailman toimivuudesta ja siten myös kyberturvallisuudesta. Bittien maailman tärkeyden korostuminen on useissa maissa siirtänyt turvallisuustarkastelua nimenomaan yhteiskunnan suojattavan kriittisen infrastruktuurin suuntaan. Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle. (Limnéll-Majewski-Salminen 2014, 31-32.)

Fyysisen ja bittien maailman yhteensulautumisen vaikutukset näkyvät yhä selvemmin myös kodeissamme. Yhä useammat kodinkoneet ja toiminnot, kuten lämmityksen sääteleminen ja kodin turvakameroiden ohjaaminen, ovat etäkäytettävissä internetin kautta. Yhä useammat arkiset esineet on varustettu jollakin tietoteknisellä ominaisuudella. Siksi puhutaan jo varsin yleisesti esineiden internetistä (Internet of Things), joskin sen kääntöpuolena voi lukea uutisia hakkeroiduista wc-pöntöistä tai älytelevisioista. Tuntuu, että vain hyvin lyhyen aikaa sitten, nämä nyt totta olevat asiat olisivat olleet uskomattomia tieteisromaanien aiheita.

Yhteiskunnan näkökulmasta fyysisen ja bittien maailman tiivis yhteen kietoutuminen merkitsee lisääntynyttä tarvetta varmistaa digitaalisen maailman toimivuus, sillä ilman sitä ei fyysinen yhteiskuntakaan toimi. Nykyisin sähköt, energianjakelu, rahoitusjärjestelmät ja elintarvikehuolto toimivat bittien varassa. Voi olla helpompi luetella ne fyysisen yhteiskunnan toiminnot, jotka eivät ole

riippuvaisia bittien maailmasta. Toimintaympäristömme on voimakkaasti ja nopeasti digitalisoitunut, ja siitä on tullut välttämätön osa yhteiskuntien, yritysten ja yksilöiden jokapäiväistä elämää. (Limnéll-Majewski-Salminen 2014, 31-32.)

Teknologia unohtuu usein silloin, kun kaikki toimii niin kuin odotetaan ja on siten jatkuvasti käytettävissä. Tiedostamme teknologian olemassaolon vasta, kun jotain yllättävää tapahtuu. Ilman ymmärrystä teknologiasta ja sen toimintaperiaatteista olemme aivan avuttomia. Suhteemme teknologiaan muodostui aikaisemmin rakentamisen ja käyttämisen kautta, koska teknologia käsitteenä sisälsi ajatuksen, että meidän on ensin itse rakennettava teknologiset puitteen ja hankittava sen käyttämiseen liittyvät taidot. Nykyään teknologia on meistä riippumaton, ja toimii oman automaationsa mukaan, ja usein on aina päällä. Kybermaailman tunkeutuminen syvemmälle atomien maailmaan muuttaa myös kulttuuriamme ja olemassa olemisen tapaamme, koska elämme yhdessä teknologian kanssa, jonka toimintaa emme kuitenkaan ymmärrä. Fyysisen tilan ohella meillä on useita minuuksia bittien maailmassa ja olemme hukassa ilman kybermaailman mahdollistavaa teknologiaa, vaikka emme edes tiedä mitä se on, ja missä se sijaitsee. (Limnéll-Majewski-Salminen 2014, 29-34.)

2.4 Tulevaisuuden kuvia ja huomioita

Uuden teknologian hypetyksen keskellä on kuitenkin pidettävä mielessä, kuinka uusi ja vanha aikakausi limittyvät toisiinsa, sillä uuteen teknologiaan perustuva talous ja yhteiskuntakehitys etenevät epätasaisesti sekä aloittain että alueittain. Suuressa osassa Afrikkaa odotellaan vielä sähkön tuloa, vaikka osittain on siirrytty jo mobiiliin internetiin. Kehittyneissäkin maissa esimerkiksi terveydenhuollossa on edetty suhteellisen hitaasti uusien teknologioiden soveltamisessa, kun taas rahoitus- ja vakuutussektori tai vaikkapa viihdeteollisuus ovat jo pitkälle siirtyneet digitaalitalouteen. (Lehti-Rouvinen-Ylä-Anttila 2012, 20.)

2.4.1 Teknologian innovaatiot

Teknologian kehitys ei pysähtynyt 2000-luvun alun pörssikuplan puhkeamiseen, mutta silti se opetti, että vanhan talouden lainalaisuudet ovat pääosin voimassa. Internet on edelleen talouden ja yhteiskunnan kehitystä voimakkaasti ajava tekijä. Uuden talouden tutkimus jätti paljon hyödyllistä tietoa myös tulevaisuuden pohdintaan, kuten esimerkiksi on verkostoteknologioiden ja -vaikutusten analyysin ja globalisaation seurauksena syntyneiden uusien tuotantomuotojen tutkimus. Alettiin ymmärtää tuotannon hajauttamisen ja arvoketjujen pilkkoutumisen seurauksia ja myös sitä, että globaali verkostotalous on haavoittuva ja altis talouden vaihteluille. (Lehti-Rouvinen-Ylä-Anttila 2012, 28-29.)

On syntynyt uusi globaali työnjako. Teollisuuden painopiste on siirtymässä pois alueelta, jossa teollinen vallankumous alkoi. Kun samaan aikaan palvelut digitalisoituvat, tietoliikenneyhteydet edelleen nopeutuvat ja niiden marginaalikustannukset lähentyvät nollaa, myös palvelutuotannon maantiede muuttuu. Digitaalisessa palveluyhteiskunnassa korkeaakin koulutustasoa edellyttävät tehtävät voivat siirtyä maasta toiseen nopeasti, jos tuotettavat palvelut ovat digitalisoitavissa. Muutokset voivat olla nopeita ja arvaamattomia, kuten esimerkiksi ohjelmistotuotannossa tai viihdeteollisuudessa on jo nähty. Korkea koulutustaso ei tulevaisuudessa välttämättä suojaa työtä, työpaikkoja tai toimialoja muutoksilta. (Lehti-Rouvinen-Ylä-Anttila 2012, 28-31.)

Tietotekniikan yhdestä uudesta innovaatiosta, ns. tekoälystä, on hyvin lyhyessä ajassa tullut iso osa elämäämme. Emme useinkaan tiedosta, että matkapuhelinten ja tietokoneiden lisäksi myös monista käyttämistämme laitteista, kuten pölynimureista, pesukoneista, televisioista ja jopa kahvinkeittimistä, löytyy teknologista älyä. Autot toimivat jo nyt osittain tekoälyn varassa, mutta on myös kehitetty auto, joka ei tarvitse kuljettajaa lainkaan. Nykyinen ifrastruktuurimme pohjautuu merkittävästi tietotekniikalle ja on osittain jopa riippuvainen siitä. Mitä enemmän tietotekniikka pienenee ja halpenee, sitä enemmän se muuttuu ihmisille näkymättömämmäksi ja jokapäiväisemmäksi.

Puhutaan ubiikista tietotekniikasta (ubiqutous computing) eli jokapaikan tietotekniikasta. Tähän jokapaikan tietotekniikkaan liittyy käsite, josta on paljon viime aikoina keskusteltu, nimittäin ns. tavaroiden internet (internet of things), mikä tarkoittaa, että esineet ovat yhteydessä toisiinsa netin välityksellä. (Hiltunen-Hiltunen 2014, 188.)

Tekoälyyn pohjaa myös ns. robotiikka, jonka ennusteet liittyvät tiiviisti tietotekniikan ennusteisiin, mikä tarkoittaa, että robottien äly kasvaa teknologian kehityksen myötä. Tulevaisuudessa robotit auttavat meitä esimerkiksi hoitotöissä, mutta muita sovelluksia on jo olemassa. Robottien motoriikan kehittämisen myötä on mahdollista parantaa laitteiden älyn laatua niin, että se parhaimmillaan voi sisältää myös tunnetta ja ns. maalaisjärkeä, jolloin robotit voisivat olla kumppaneitamme. Tulevaisuudessa robotteja on luultavasti erikokoisia alkaen pienenpienistä nanoroboteista, joita esimerkiksi lääketiede voi hyödyntää, aina suuriin teollisuusrobotteihin, jotka toimivat lukuisissa tehtävissä erilaisissa ympäristöissä meren alta avaruuteen. Tietotekniikan ja robotiikan kehittyminen vaikuttaa tulevaisuudessa yhä useampaan toimialaan, samalla kun yhä useampi voi nauttia tietotekniikan kehityksen tuomista mahdollisuuksista. Esimerkkinä tästä voidaan mainita lääketiede, automaattiliikenne ja energia-ala. (Hiltunen-Hiltunen 2014, 188.)

Robotiikan on sanottu olevan Suomelle suuri mahdollisuus, jopa Nokian veroinen, mikäli emme menetä tätä tilaisuutta. Niin tekoälyn kuin robotiikan mahdollistaa ns. sensorit, joita on kutsuttu tietokoneen aistielimiksi, sillä ne ovat tietokoneen komponetteja, jotka aistivat ympäristön fysikaalisia tiloja ja välittävät tiedot sähköisinä signaaleina tietokoneelle. Elektroniikan pienentyminen ja halventuminen on mahdollistanut sensorit myös tavallisen kuluttajan käyttöön, kuten esimerkiksi liitettyinä älypuhelimiin, joko valmiiksi asennettuina tai lisälaitteina. Tällaisia ovat esimerkiksi gyroskooppi, joka kertoo sen, miten päin matkapuhelinta pidetään kädessä ja muuttaa näytön suuntaa tämän tiedon mukaan tai esimerkiksi Fitbit Flex -rannesensori, joka mittaa muun muassa unen laatua ja liikuntaa, ja laitteen tuottamaa dataa voidaan tulkita älypuhelimella. Nämä sensoreita sisältävät laitteet ovat mahdollistaneet uuden

tiedon keräämisen tavan,ns. joukkoistamisen. Kun yhä useampi kuluttaja kantaa mukanaan sensorilla varustettua laitetta, joka on yhteydessä internettiin, tietoa ympäristöstä voidaan kerätä laajemmin ja ajankohtaisemmin. (Hiltunen-Hiltunen 2014, 198.)

2.4.2 Kybermaailman mahdollisuudet ja haasteet

Voimmeko enää edes kuvitella, miten yritysten tai valtioiden talous ja muut taloudelliset aktiviteetit toimisivat, jos näistä toiminnoista otettaisiin pois virtuaalimaailman mahdollistamat asiat. Yhteiskunnan eri toiminnot ja työnteko olisivat kovin erilaiset, jos edelleen kirjoittaisimme kaiken kynällä paperille, sillä asiat sovittaisiin kirjeillä ja maksut suoritetaan käteisellä. Sähköistyminen on luonut uutta liiketoimintaa, mutta muuttanut myös vanhaa, kuten esimerkiksi markkinointia ja mainontaa, sillä enää ei olla pelkästään kalliiden tienvarsi- ja sanomalehtimainoksien varassa. Sähkö on vanha keksintö, mutta jakelu on nykyisin digitalisoitu, jolloin ilman verkkoja ei sähkölaitteet toimi, mikä taitaisi olla nykymaailmassa todella hankalaa. (Limnéll-Majewski-Salminen 2014, 91.)

Kybermaailmassa joudutaan tasapainoilemaan sillä, miten hyödyntää tehokkaasti mahdollisuuksia, ja miten huolehtia siitä, että teknologian mahdollistamat toiminnot ja niiden turvallisuus kyetään joka hetki varmistamaan. Taloudelliseen menestykseen tarvitaan sekä mahdollisuuksien hyödyntämistä että turvallisuuden varmistamista. Kybermaailman turvallisuuden varmistamisesta on tullut keskeinen taloudellinen kilpailutekijä, sillä silloin, kun kansainväliset yritykset etsivät globaalisti sijoituskohteita toiminnoilleen, on kyberturvallisuustekijät nostettu yhdeksi arvioitavaksi asiaksi muiden perinteisempien, kuten halvan työvoiman, kuljetuskustannusten ja raaka-aineiden saatavuuden rinnalle. Turvallisuus koetaan tärkeäksi, jopa välttämättömäksi, asiaksi yritystoiminnalle. Valtiot ovat puolestaan alkaneet rakentaa mahdollisimman turvallisia verkkoympäristöjä houkutellakseen ulkomaisia sijoittajia ja liiketoimintaa alueelleen. Yhtenä esimerkkinä Iso-Britannia, jonka kansallisessa kyberstrategiassa kerrotaan ensimmäisenä

tavoitteena olevan luoda yksi maailman turvallisimmista paikoista harjoittaa liiketoimintaa kybertoimintaympäristössä. Kilpailu maailman kyberturvallisimman valtion tittelistä on alkanut. (Limnéll-Majewski-Salminen 2014, 91.)

Kybermaailman ratkaisut lupaavat usein olemassa olevan toimintatavan tehostumista ja tuottavuuden lisääntymistä, mikä usein toteutuukin laskettuna perinteisillä mittareilla, kuten säästöt ja turhien toimintojen karsiminen. Tehokkuuden lisääntyminen ei ole kuitenkaan mikään itsestäänselvyys, ja mahdollinen kustannushyöty voidaan menettää väärillä ratkaisuilla. Jotta teknologian hyödyntämisen vaatimat investoinnit eivät vaihtuisi hukatuiksi resursseiksi, kybermaailmaa varten on kehitettävä siihen sopivat tuottavuuden ja tehokkuuden mittarit, jotka mahdollistavat yrityksen tai hallinnon suurimittaisenkin uudelleen organisoimisen. Onnistuminen edellyttää kuitenkin, että organisaatiossa ymmärretään kybermaailman hyödyntäminen tuottama lisäarvo kun halutaan säästää rahaa ja lyhentää tuotantoon kuluvaa aikaa. (Limnéll-Majewski-Salminen 2014, 93.)

On ristiriitaisia näkemyksiä siitä, onko kaupallisuus edistänyt vai hidastanut teknologian omaksumista ja liikkumista talouden ja yhteiskunnan alueelta toiselle, vaikka teknologian laaja levinneisyys, ja uusien sovelluksien jatkuva käyttöön ottaminen todistaisi edistyksen puolesta. Siltikään ei olla yksimielisiä siitä, onko esimerkiksi internetin laajakaistayhteys kansalaisoikeus, joka valtion pitää taata kaikille kansalaisilleen, tai onko kyberuhkista saatavilla oleva tieto luonteeltaan kaupallista vai yleishyödyllistä. Taloudelliselta näkökulmalta nämä näkemykset sisältävät moninaisia mahdollisuuksia, sillä laajakaista saattaa lisätä kansalaisten nettiaktiivisuutta ja sitä kautta muuttaa heidän käyttäytymistä. Lisäksi kyberuhkista saatava tieto voi taas tuottaa taloudellista hyötyä joko yritykselle, joka kyseisen tiedon pystyy tuottamaan, tai talouselämälle yleisesti, ja koko yhteiskunnalle, kun tiedolla voidaan edesauttaa järjestelmien toimintavarmuutta, ja lisätä niiden yleistä turvallisuutta. (Limnéll-Majewski-Salminen 2014, 94-95.)

3 LAINSÄÄDÄNTÖ JA SOPIMUKSET

Jokaisella internetverkkoon liitetyllä laitteella on merkitystä, sillä vaikka laite sisältäisi ainoastaan yleistä muutenkin julkista tietoa, sitä voidaan väärinkäyttää monella tavalla. Laite voi elää omaa elämää omistajansa huomaamatta, se voi toimia esimerkiksi osana alamaailman tietoverkkorikollisten verkkoa, josta tehdään kohdistettuja hyökkäyksiä, kuten esimerkiksi yritetään murtautua työpaikkasi tietojärjestelmiin, lähetetään roskapostia tai pyöritetään laittomia elokuvia jakelevaa tiedostopalvelinta. Rikolliset voivat haluta tietoja laitteeltasi, kuten tunnuksia ja salasanoja tai tietoja, mitä sinulla on tietokoneella, puhelimessa tai tabletissa. Tietojen, jotka koskevat kotia, rahaliikennettä, yksityiselämää, terveyttä, työpaikkaa, vapaa-aikaa ja mitä tahansa muita sellaisia asioita, joiden ei yleensä haluta päätyvän julkisuuteen tai häviävän tai muuttuvan sisällöltään.

Lakien ja sopimuksien pyrkimyksenä ei ole hankaloittaa tietokoneen palveluiden käyttämisestä yhtään sen enempää kuin mitä se muutoinkin olisi. Itse asiassa tietokoneiden, ohjelmien ja erityisesti nettipalveluiden käyttö on helpottunut melkoisesti verrattuna esimerkiksi 90-lukuun, johtuen yhdenmukaisempien käyttöliittymien ja päätelaitteiden, kuten älypuhelimien ja kosketusnäyttöä käyttävien päätelaitteiden kehittymisestä. (Rousku 2014, 124-125.)

3.1 Kansallinen sääntely

Keskusrikospoliisin rikoskomisario Timo Piiroisen mukaan, Suomessa on rikoslaissa huomioitu melko kattavasti eri rikoksentekomahdollisuudet, mutta rikoslaissa ei kuitenkaan ole riittävästi vielä huomioitu rangaistusmaksimeja verkkorikoksissa, sillä ne eivät ole tämän päivän uhkakuvien mukaisia vaan 10-15 vuoden takaa. Rangaistusmaksimit heijastuvat siihen, millaiset lakityökalut poliisilla on käytössään tutkinnassa. Suurin haaste on kansainvälisyys, sillä kansainväliset oikeusapuprosessit toimivat luvattoman hitaasti (Peltomäki-Norppa 2015, 73.)

Kansallisessa lainsäädännössä ei ole kyberuhkia koskevaa yhtenäistä sääntelyä. Eri hallinnonalat määrittelevät kyberrikokset ja -uhkat sekä niitä koskevat toimivaltuudet omasta näkökulmastaan, vaikka kybertoiminta ei katso hallinnonaloja sen enempää kuin valtioidenkaan rajoja. Sama toiminta voi tulla arvioitavaksi yksittäisenä rikosoikeudellisena tekona, terrorismirikoksena tai valtioiden välisten suhteiden näkökulmasta. Oikeudellinen arviointi ja yhtenäinen kansallinen oikeudellinen tulkinta tässä tilanteessa on erittäin haastavaa. Rikoksen ja lain yhteensovittaminen on yleensä tuomioistuinten tehtävä. Tällä hetkellä ei kuitenkaan ole riittävästi lainsäädäntöä eikä oikeuskäytäntöä, jonka avulla voisi tehdä kattavia päätelmiä kyberrikollisen teon rangaistavuudesta. Lisäksi monien uusien kyberrikosten, kuten identiteettivarkauksien rankaisemista vasta harkitaan. (Peltomäki-Norppa 2015, 73-74.)

Kyberrikoksen olemuksen ja sen rangaistavuuden ymmärtämiseksi, on syytä tarkastella lainsäädäntöä ja sopimuksia nimenomaan kansainvälisestä näkökulmasta, ja sitä miten nämä sopimukset on saatettu voimaan Suomessa. Lakeihin säädetyillä rangaistuksilla on pyrkimyksenä rangaista rikokseen syyllistynyttä tahoa, mikä perustuu ns. sovitusteorialle. Rangaistuksen ankaruus riippuu siitä, miten paheksuttavaksi lainsäätäjä on sen katsonut. Perinteisesti omaisuuteen kohdistuvia rikoksia ei ole katsottu yhtä paheksuttaviksi kuin ihmisiin kohdistuvia rikoksia. Tämä ajattelutapa on havaittavissa myös tietotekniikkarikoksissa. Lainsäädännössä rangaistuksella katsotaan myös olevan ns. yleisestävä- eli preventiovaikutus, joka perustuu ajatukselle, että rangaistuksen pelko estää muita tekemästä rikosta. Rangaistuksilla on katsottu olevan myös erityisestävä vaikutus, jolloin rangaistuksen tarkoituksena on estää rikoksentekijää uusimasta rikosta. (Peltomäki-Norppa 2015, 74.)

Kansallisella tasolla Suomen perustuslaki määrää, että julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Perusoikeuksia on suojeltava myös tietoverkoissa, jotka myös edistävät kansalaisten sananvapauden toteutumista. Oikeustieteellisten määritelmien mukaan, rikos on teko tai laiminlyönti, joka on laissa määrätty rangaistavaksi. Rangaistavuuden edellytys on, että tekijä on syyllistynyt rikokseen tahallaan tai tuottamuksellisesti,

ja että tekijä on ollut rikoksen tekohetkellä syyntakeinen. Rikoksen tahallisuus tarkoittaa, että rikoksen tekijä on rikkonut lakia tietoisesti, ja ymmärtänyt mitä seurauksia hänen teollaan on. Tuottamuksellisuudella tarkoitetaan, että tekijän menettely on huolimatonta, jos hän rikkoo olosuhteiden edellyttämää ja häneltä vaadittavaa huolellisuusvelvollisuutta, vaikka hän olisi kyennyt sitä noudattamaan. (Peltomäki-Norppa 2015, 75.)

Puhtaasta vahingosta ei joudu syytteeseen, mutta huolellisuusvelvoitetta ei sen sijaan saa rikkoa, sillä siitä voi joutua syytteeseen tuottamuksen perusteella. Tällöin arvioidaan sitä, olisiko vahingolta vältytty, jos tekijä olisi toiminut toisin. On kuitenkin muistettava, että vahingon tekijä voi silti joutua korvaamaan aiheuttamansa vahingon, vaikka syytettä ei tulisikaan, eikä rikosta ole tapahtunut. Nuoret voivat usein vahingossa ja tahallaankin syyllistyä kyberrikokseen. Alle 15-vuotiaat eivät voi saada rangaistusta rikoksen tekemisestä, mutta he ovat korvausvelvollisia aiheuttamistaan vahingoista, jotka kyberrikosten kohdalla voivat olla hyvin suuriakin. Lisäksi poliisi ilmoittaa alle 18-vuotiaiden tekemistä rikoksista lastensuojeluun. (Peltomäki-Norppa 2015, 75.)

Vaikka nuorten tekemistä rikollisista teoista ei tule merkintää rikosrekisteriin, jää niistä merkintä poliisin ja viranomaisten tiedostoihin. Näiden tietojen perusteella poliisi antaa pyydettäessä tietyille yrityksille ja oppilaitoksille ns. turvallisuusselvityksen. Leikkimielisesti tai vahingossa tehty kyberrikos voi siis estää työ- tai opiskelupakan saamisen. Alle 15-vuotiaiden vahingonkorvauksia voidaan sovitella, ja sovittelun kautta voi olla mahdollista neuvotella maksettavan summan kohtuullistamisesta ja maksuaikataulun pituudesta. Sovittelu on vapaaehtoista ja perustuu nuoren omaan halukkuuteen selvittää asia. Viime kädessä asianomistaja voi viedä vahingonkorvauksen siviilikanteella oikeuteen, myös alle 15-vuotiaiden osalta, jolloin oikeuden päätöksen jälkeen maksu voi siirtyä ulosottoon (Peltomäki-Norppa 2015, 73-76).

Organisaatiot joutuvat huolehtimaan tietoturvallisuudesta, koska Suomen lait ja asetukset sekä EU velvoittavat niin tekemään. Organisaatioissakin saatetaan katsoa joitakin tietoturvallisuuden velvoitteita ajoittain läpi sormien, mutta olipa menettely tietoista tai tiedostamatonta, kansalaiset ja organisaatiot voivat

tietoturvasta tinkiessään aiheuttaa valtavia taloudellisia, aineellisia ja jopa henkilövahinkoja. Esimerkiksi satunnainen väärän www-linkin napsauttaminen huijaus-sähköpostiviestissä, tai yes-painikkeen napsauttaminen väärällä www-sivulla, voi asentaa tietokoneellesi haittaohjelman, joka kerää koneellasi ja työpaikan palvelimilla olevia tietoja ja lähettää niitä väärinkäyttäjille, kuten tietoverkkorikollisille, kenenkään huomaamatta mahdollisesti jopa vuosien ajan. (Rousku 2014, 125-126.)

Lakien ja asetusten ohella organisaatiota velvoittavat sopimukset muiden organisaatioiden, kuten toimittajien, alihankkijoiden sekä muiden yhteistyötahojen kanssa. Sopimukset pakottavat organisaatiota huolehtimaan, ei pelkästään organisaation omista luottamuksellisista tiedoista, vaan myös muiden organisaatioiden ja asiakkaiden tiedoista. Tällaisen organisaatioiden välisen turvallisuus sopimuksen noudattamatta jättäminen, tai osittainenkin laiminlyöminen, voi johtaa esimeriksi sanktiomaksuihin ja jopa sopimuksen purkamiseen. Huolellisuutta on noudatettava myös kodin luottamuksellisien tai merkittäviä taloudellisia arvoja edustavien asiakirjoihin suhteen. Harva säilyttää esimerkiksi asuntojen osake- tai muita omistusasiakirjoja tai suuria summia käteistä rahaa kotona, vaan vie ne parempaan turvaan, esimerkiksi pankin kassaholviin. (Rousku 2014, 125.)

Rikokset voivat olla ns. yleisen syytteen alaisia taikka asianomistajarikoksia. Vakavimmat rikokset ovat yleensä yleisen syytteen alaisia, jolloin syyttäjä on velvollinen nostamaan syytteen, jos syytekynnys ylittyy. Tietotekniikkaan kohdistuvat rikokset ovat yleensä asianomistajarikoksia, jolloin poliisi voi aloittaa rikoksen tutkinnan vasta, mikäli asianomistaja ilmoittaa asiasta poliisille, ja vaatii samalla tekijälle rangaistusta. Asianomistaja on se, joka on joutunut rikoksen kohteeksi. Asianomistajana pidetään esimerkiksi henkilöä, jonka tunnuksia ja salasanoja on käytetty väärin tai yhteisöä, jonka palvelimelta rikoksen tekijä on hankkinut luvattomasti oikeuksia. (Peltomäki-Norppa 2015, 76-77.)

Suomessa tietotekniikkarikokset on otettu huomioon rikoslainsäädännössä kahdella tavalla. Kun tietotekniikan väärinkäytökset ovat verrattavissa fyysisessä maailmassa tehtäviin rikoksiin, on voimassa olevia säännöksiä tarkistettu

tietotekniikan osalta. Muun muassa petossäännöstä on muutettu siten, että koneellisen tietojenkäsittelyn lopputuloksen muuttaminen on rinnastettu perinteiseen ihmisen erehdyttämiseen. Niiltä osin, kun tietotekniikka on tuonut mukanaan kokonaan uudenlaista käyttäytymistä, on säädetty uusia tietotekniikkaan liittyviä tunnusmerkistöjä täyttäviä lakeja. (Peltomäki-Norppa 2015, 77.)

Tietoturvallisuuteen liittyvää sääntelyä on rikoslain eri luvuissa. Lisäksi tietoturvaan liittyviä säännöksiä löytyy tekijänoikeuslaissa, aluevalvontalaissa, valmiuslaissa, puolustustilalaissa ja puolustusvoimista annetussa laissa, sekä viestintämarkkinalaissa ja sähköisen viestinnän tietosuojalaissa. Lisäksi rikoslain kokonaisuudistuksessa lain 38 luku vahvistettiin 21.4.1995 kattamaan myös tieto- ja viestintärikokset. Laki tuli voimaan 1.9.1995. (Peltomäki-Norppa 2015, 77-78.)

3.2 Tietotekniikkaan kohdistuvat rikokset

Tietotekniikkaan kohdistuvan rikoksen tunnusmerkistö täyttyy silloin, kun ns. tietojenkäsittelyn rauhaa loukataan. Käsitteenä tietojenkäsittelyrauha on verrattavissa kotirauhaan. Laki suojaa tietojenkäsittelyrauhaa, mikä tarkoittaa tiedon luottamuksellisuutta, käytettävyyttä ja eheyttä. Tietomurtoon syyllistyy, kun käyttää luvatta toisen käyttäjätunnusta ja salasanaa tai ylittää saamansa käyttäjäoikeudet (rikoslain 38 luvun 8 §). On huomattava, että tietomurtorikoksessa ei välttämättä tarvitse murtaa mitään, vaan rikoksena pidetään jo sitä, kun ylitetään omat oikeudet, tai käytetään luvatta toisen oikeuksia. Laki säätää tietomurrosta rangaistukseksi sakkoa tai vankeutta enintään yhdeksi vuodeksi. Mikäli pääsee luvatta toisen tietokoneelle, teko katsotaan yleensä joksikin muuksi rikokseksi kuin tietomurroksi. Rikoksen määrittely riippuu hyvin pikälle siitä, mitä tunkeutuja tietokoneessa tekee. Jos on luvatta toisen tietokoneella, tekijä käyttää toiselle kuuluvaa tietokone-aikaa ja mikä katsotaan luvattomaksi käytöksi. Teko on verrattavissa auton luvattomaan käyttöön (rikoslain 28 luvun 7 §) ja jo teon yrityskin on rangaistava. Kuitenkin on huomattava, että vuonna 2011 tähän pykälään lisättiin kolmas momentti, jonka

mukaan luvattomana käyttönä ei enää pidetä suojaamattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttämistä (Peltomäki-Norppa 2015, 78.)

Mikäli tekijä asentaa erilaisia omia tarkoitusperiään palvelevia ohjelmia toisen koneelle, voidaan luvattoman käytön lisäksi katsoa, että tällöin täyttyy myös vahingontekorikoksen tunnusmerkistö. Vahingonteko olisi vastaava rikkomus, jota sovelletaan esimerkiksi ikkunan rikkomiseen (rikoslain 35 luvun 1 §). Siinä tapauksessa, että vahingonteko on törkeä, voidaan siitä rangaista ankarammin (35 luvun 2 §). Myös molempien edellä mainittujen tekomuotojen yrityskin on rangaistava.

On olemassa keinoja, joilla murtautuja voi hankkia itselleen myös palvelintasoisesta koneesta oikeuksia, jotka mahdollistavat esimerkiksi palvelimella olevien sähköpostien lukemisen. Murtoa varten tekijän on ensin tehtävä erityisesti tätä tarkoitusta varten uusi ohjelma, tai muutettava koneessa olevaa ohjelmaa. Teko täyttää törkeän viestintäsalaisuuden loukkaamisen tunnusmerkistön (rikoslain 38 luvun 4 §). ja myös tämän rikoksen yritys on rangaistava. (Peltomäki-Norppa 2015, 79-80.)

Tietojärjestelmän häiritsemiseen syyllistyy se, joka dataa syöttämällä, tai eräillä muilla säännöksessä mainituilla tai tarkoitetuilla tavoilla, estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä,. (rikoslain 38 luvun 7 a §). Tietojärjestelmän häiritseminen voi rikoksena toteutua myös sekä lievänä (rikoslain 38 luvun 7 §) että törkeänä (rikoslain 38 luvun 7 b §). Kaikkien näiden rikosten yrityskin on rangaistava. (Peltomäki-Norppa 2015, 80.)

3.3 Tietotekniikkaa hyväksi käyttävät rikokset

Tietotekniikkaa hyväksikäyttäviä rikosmuotoja on paljon. Nykyisessä digitalisoituneessa maailmassa tietotekniikka on lähes aina osallisena mm. talousrikoksissa, joissa kirjanpito ja muu tietoaines on suurelta osin talletettu elektroniseen muotoon. Niitä ei kuitenkaan pidetä varsinaisina tietotekniikkarikoksina. Yleisesti voidaan sanoa, että tavallisen tietokoneen ja

tietoverkkojen käyttäjän kannalta tärkein sääntö on se, että mikä on kiellettyä tietoverkkojen ulkopuolella, on kiellettyä myös verkoissa. Käytännössä tämä tarkoittaa, ettei myöskään verkon kautta saa esimerkiksi herjata tai uhkailla ketään ja lapsi- ja eläinpornografian levittäminen on kiellettyä.

1.1.2014 tuli voimaan uusia tietotekniikkarikoksiin liittyviä säädöksiä:

- Rikoslakiin, tarkemmin yksityisyyden rauhan ja kunnian loukkaamista koskevaan 24 lukuun, lisättiin uusi viestintärauhan rikkomista koskeva rangaistussäännös. ”Viestintärauhan rikkomiseen (rikoslain 24 luvun 1 §) syyllistyy se, joka häirintätarkoituksessa toistuvasti lähettää viestejä tai soittaa toiselle siten, että teko on omiaan aiheuttamaan huomattavaa häiriötä tai haittaa. Rangaistuksena on sakkoa tai vankeutta enintään kuusi kuukautta.”

- Rikoslain 25 lukua sen sijaan täydennettiin uudella vainoamista koskevalla rangaistussäännöksellä. ”Vainoamiseen (25 luvun 7 a §) syyllistyy se, joka toistuvasti uhkaa, seuraa, tarkkailee, ottaa yhteyttä tai muuten näihin rinnastettavalla tavalla, oikeudettomasti vainoaa toista siten, että se on omiaan aiheuttamaan vainotussa pelkoa tai ahdistusta. Vainoamisesta voitaisiin tuomita sakkoa tai enintään kaksi vuotta vankeutta. Vainoaminen on yleisen syytteen alainen rikos.” (Peltomäki-Norppa 2015, 80-81.)

Identtiteettivarkauksiin aiemmin sovellettu mm. rikoslain säädöksiä kunnian loukkauksesta tai petoksesta, mutta syksyllä 2015 tuli voimaan laki, jossa identtiteettivarkaus määritellään rikokseksi, josta voi seurata sakkorangaistus. Merkittävää on myös se, että laki koskee yksityishenkilöiden lisäksi myös esimerkiksi yrityksiä. (Yle Uutiset 2015.)

3.4 Tekijänoikeudet

Tekijänoikeudet pitää myös tavallisen verkon käyttäjän ottaa huomioon ja tietää muutamat perussäännöt. Yleisesti pitäisi olla tiedossa, että verkkoon ei saa laittaa tekijänoikeuden suojaamaa aineistoa ilman sen tekijän lupaa. Tämä

tarkoittaa muun muassa sitä, että omien kotisivujen kuvituksena ei saa käyttää kuvia, joiden käytölle ei ole kuvan tekijän lupaa. Ilman lupaa ei verkosta myöskään saa kopioida aineistoja edes omaan käyttöön. Vuoden 2006 alussa tuli voimaan tekijänoikeuslain muutos, jonka mukaan yksityiseen käyttöön saa kopioida vain sellaista aineistoa, joka on laillisesti saatettu yleisön saataville, ja jonka kopiointia ei ole estetty teknisellä suojauksella. Aineiston suojausta ei saa murtaa kopion tekemistä varten. Myöskin aineistojen imurointi eli lataaminen internetistä luvatta omalle koneelle on kiellettyä. (Peltomäki-Norppa 2015, 81.)

Tekijänoikeusrikoksista on säädetty rikoslaissa rangaistukset. Lain mukaan henkilö, joka ansiotarkoituksessa, tekijänoikeuslain säännösten vastaisesti ja siten, että teko on omiaan aiheuttamaan huomattavaa haittaa tai vahinkoa loukatun oikeuden haltijalle tavoilla, jotka on rikoslain 49 luvun 1 §:ssä tarkemmin esitetty, voidaan tuomita sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Tekijänoikeusrikkomus, josta voidaan määrätä sakkorangaistus, on tekijänoikeusrikosta lievempi teko, ja siitä on säännökset tekijänoikeuslain 56 a §:ssä. (Peltomäki-Norppa 2015, 81.)

3.5 Yksityisyyden suoja

Tietoturvallisuuden merkitys ja toteuttaminen korostuvat työpaikoilla erilaisia tietoja käytettäessä. Yleensä käytetään monenlaisia tietoja, jotka voivat olla yleisellä tasolla tai liittyä henkilötietoihin. Erityisesti henkilötietojen käsittelyyn liittyvät yksityisyydensuoja ja tietosuoja-asiat. Henkilötietolaki (523/1999) on perustuslain 10 §:n ja 12 §:n ohella Suomessa keskeinen säädös yksityisyyden suojan toteuttamisessa. Yksityisyydensuoja keskittyy vahvasti henkilötietojen varaan. Henkilötiedoista (esim. nimi ja osoite) syntyy henkilörekisteri, ja se edellyttää rekisteriselostetta, jossa kuvataan henkilötietojen käsittely. Erityisen huolellinen tulee olla käsiteltäessä arkaluonteisia henkilötietoja, jotka on määritelty henkilötietolain 11 §:ssä.

”3 luku Arkaluonteiset tiedot ja henkilötunnus

11 § Arkaluonteisten tietojen käsittelykielto

Arkaluonteisten henkilötietojen käsittely on kielletty. Lain mukaan arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan

- rotua alkuperää
- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta
- henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai muita niihin verrattavia toimia
- henkilön seksuaalista suuntautumista tai käyttäytymistä tai
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja tukitoimia ja muita sosiaalihuollon etuuksia.”

Näistä useimmin käytettyjä perusteita tietoja luokittelemiseksi arkaluonteisiksi ovat yllä oleviin kohtiin 2 ja 4 liittyvät tiedot. Henkilörekisteri voi olla manuaalinen, esimerkiksi paperille kirjoitettu lista, tai se voi olla sähköisessä muodossa, esimerkiksi jokin henkilöstöhallinnon tietojärjestelmä, Excel-tiedosto tai sähköpostijärjestelmä.

Kun organisaatio kerää henkilötietoja tuloksena on henkilörekisteri, ja organisaatiosta tulee tällöin rekisterinpitäjä. Rekisterinpitäjän on huolehdittava tietojen oikeellisuudesta sekä tietoturvallisuudesta. Jokaisella on omien tietojensa tarkastusoikeus, mikä pitää sisältää tiedonsaantioikeuden, tarkastusoikeuden ja kielto-oikeuden. Tiedonsaantioikeudella kysyjä voi saada tiedon rekisterinpitäjästä ja käyttötarkoituksesta sekä tietojen luovutuksista. Tarkastusoikeus käsittää rekisterin tietojen sisällön saamista kirjallisena kysyjän niin halutessa. Kielto-oikeus kohdistuu mainostarkoituksiin ja erilaisiin matrikkeleihin ja sukututkimuksiin. (Rousku 2014, 132.)

Rekisteriseloste pitää laatia kaikista henkilötietoja sisältävistä rekistereistä eli henkilörekistereistä. Selosteesta ilmenee, kuka on henkilötietojen käsittelystä vastaava rekisterinpitäjä, mitä henkilötietoja rekisterissä on, mihin tietoja

käytetään, ja minne niitä säännönmukaisesti luovutetaan, sekä tietojen suojauksen periaatteet. Jos organisaatio käyttää palveluntuottajan tarjoamaa valmista palvelua, tai muuten ostopalveluna palveluntarjoajan tuottamaa palvelua, palveluntarjoaja on vastuussa rekisteriselosteen laatimisesta, ja asiakasorganisaatio voi hyödyntää palveluntarjoajan laatimaa rekisteriselostetta. (Rousku 2014,140.)

Laissa on rikkomuksiin myös rangaistukset, kuten rikoslain 38 luvun

9 §: ssä todetaan henkilörekisteririkoksesta:

”Joka tahallaan tai törkeästä huolimattomuudesta

- käsittelee henkilötietoja vastoin henkilötietolain (523/1999) käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä, henkilötietojen tarpeellisuutta tai virheettömyyttä, arkaluonteisia tietoja, henkilötunnusta tai henkilötietojen käsittelyä erityisiä tarkoituksia varten koskevia säännöksiä, taikka rikkoo henkilötietojen käsittelyä koskevia erityissäännöksiä (8.6.2001/480)

- antamalla rekisteröidylle väärän tai harhaanjohtavan tiedon, estää tai yrittää estää rekisteröityä käyttämästä hänelle kuuluvaa tarkastusoikeutta tai

- siirtää henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain 5 luvun vastaisesti, ja siten loukkaa rekisteröidyn yksityisyyden suojaa, tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava henkilörekisteririkoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi”

Kolmas kohta on mielenkiintoinen uusien verkossa toimivien palvelujen kannalta, sillä jos organisaatiossa on kerätty henkilötietoja, ja nämä henkilötiedot tallennetaan pilvipalveluun, joka sijaitsee EU-/ETA-alueen ulkopuolella on menetelty lainvastaisesti. (Rousku 2014,142.)

Laki yksityisyydensuojasta työelämässä (759/2004) määrittää miten yksityisyyden suoja pitää työelämässä ottaa huomioon.

”2 luku Henkilötietojen käsittelyn yleiset edellytykset

3 § Tarpeellisuusvaatimus

Työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, työnantajan työntekijöille tarjoamiin etuuksiin tai johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.” (Rousku 2014, 136-137.)

Yksityisyydensuojalla huolehditaan siitä, että henkilön tietoja käsitellään voimassaolevan lainsäädännön velvoitteiden mukaisesti. On kuitenkin monenlaisia käsityksiä siitä, mitä asioita me tulkitsemme yksityisiksi kuin myös siitä, miten haluaisimme meihin liittyviä tietoja käsiteltävän. Esimerkiksi Facebookin käyttämisestä on olemassa monia mielipiteitä, samoin kuin siitä, millaista henkilökohtaista tietoa itse kukin siinä ympäristössä julkaisee. (Rousku 2014, 136.)

Yksityisyydensuojaan liittyvät kysymykset nousevat uuden teknologian yleistymisen myötä esille yhä erilaisimmissa yhteyksissä. Tällaisia ovat esimerkiksi tietoliikenteen valvonta ja seuranta internetin käytössä, päätelaitteiden, tietojärjestelmien ja tietoliikennelaitteiden lokien keräämisessä sekä lokien käsittelyyn liittyvissä asioissa. ICT-järjestelmiin syntyy lokitietoja arviolta useita miljardeja per sekunti, koska esimerkiksi jokainen sähköposti, jokainen www-sivun avaaminen ja jokainen muun nettipalvelun käyttö aiheuttaa kymmeniä jopa satoja lokimerkintöjä globaalisti. (Rousku 2014, 137.)

Yksityisyyden suojasta on myös kysymys tilanteissa, joissa henkilön ollessa poissa, työnantajalle tulee tarve saada hänen sähköpostilaatikossaan oleva sähköpostiviesti käyttöönsä. Kulunvalvonnassa ja kameravalvonnassa ollaan myös tekemisessä yksityisyyden suojan kanssa. Vaikka työnantajalla on oikeus määrätä, mitä ja miten hänen henkilöstölle antamiaan työvälineitä saa ja pitää

käyttää, työnantaja ei voi valvoa määräyksiään muuten kuin erikseen määritellyissä tilanteissa. (Rousku 2014, 137.)

Sähköisen viestinnän tietosuojalaki (516/2004), jota uudistettiin vuonna 2009, ottaa erityisesti kantaa yksityisyydensuojaan liittyviin asioihin, kun niitä käsitellään sähköisesti. Tiensuojaan (data privacy) sisältyvät esimerkiksi tietoturvallisuus ja muut keinot, joilla pyritään huolehtimaan henkilötietojen vaatimustenmukaisesta käsittelystä. (Rousku 2014, 129.)

”Sähköisen viestinnän tietosuojalaki

1 luku Yleiset säännökset

1 § Lain tarkoitus

Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyydensuojan toteutuminen, sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.

2 § Määritelmät

Tässä laissa tarkoitetaan:

viestillä viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa.” (Rousku 2014, 127-142.)

3.6 Kansainväliset pelisäännöt

Tällä hetkellä kybermaailmaa voi kutsua villiksi länneksi, jossa eri toimijat tekevät mitä haluavat ilman kansainvälistä kontrollia ja normistoa, koska pelisäännöt puuttuvat. Kybersodankäynnin pohtimisen ohella tulisikin kiinnittää huomiota kyberrauhaan ja sen edistämiseen. Vakoilun osalta tilanne on haastavin, vaikka se on tunnetusti ikiaikainen ilmiö, joka on nyt siirtynyt verkkoon. Valtioilla ei ilmeisesti ole halua tai keinoja sen rajoittamiseksi. Niiltä löytyy kuitenkin yhteisiä intressejä esimerkiksi kyberrikollisuuden ehkäisemiseksi ja sodankäynnin

säännöstön ulottamiseksi kybermaailmaan. Kansainvälisen normiston saaminen bittien maailmaan on tavoiteltavaa. Tilanne muistuttaa ydinasekysymystä toisen maailmansodan jälkeen, kun kansainvälinen yhteisö koki ensin olevansa lähes mahdottoman tehtävän edessä miettiessään lakeja ja sopimuksia, joilla voidaan säädellä ydinaseita. Hiljalleen kansainväliset pelisäännöt ja niiden valvontatoimet onnistuttiin kuitenkin muodostamaan. (Limnéll-Majewski-Salminen 2014, 149.)

Yhdessä sovittujen sääntöjen voima on siinä, että ne vähitellen muokkaavat osapuolten käyttäytymistä tai ainakin pakottavat sääntöjen vastaisesti toimivan perustelemaan toimintansa kansainvälisen yhteisön painostuksen edessä. Pelisäännöt koostuvat sopimuksista ja käytännöistä, toisin sanoin sanoista ja toiminnasta. Huomionarvoista on myös kyberulottuvuuden eettinen vaikutus ja sen merkitys sodan tulevaisuudelle. Perinteisesti on pidetty tärkeänä siviilien koskemattomuutta, joka saattaa kuitenkin olla vaikeaa, kun hyökätään kyberkyvyillä siviili-infrastruktuuria kohtaan. (Limnéll-Majewski-Salminen 2014, 149.)

Ennen pelisääntöjen laatimista pitää miettiä kumpi olisi parempi vaihtoehto, eli neuvotella koko kybermaailmaan erillinen kansainvälinen sopimus, vai laajentaa olemassa olevaa lähinnä fyysistä maailmaa koskevaa säännöstöä kybermaailmaan. Pelkkä kybermaailmaa koskeva säännöstö lienee hankala toteuttaa, koska valtiot käsitteellistävät kybermaailman monin eri tavoin, ja niiden intressit ovat niin moninaisia, että yhteisen käsitteistön löytäminen on vaikeaa. Kyberkysymysten sisällyttäminen esimerkiksi kansainvälistä kauppaa ja lainvalvontaa koskeviin säännöstöihin vaikuttaisi lupaavammalta. Jonkinlainen lähtökohta pelisäännöille on tällöin jo olemassa, ja yhteisesti määriteltävillä teknologiastandardeilla puolestaan ohjataan sitä, millaisin pelivälinein peliä pelataan. (Limnéll-Majewski-Salminen 2014, 149.)

Yksi vaihtoehto kansainvälisen säännöstön luomiselle olisi pyrkiä saavuttamaan yhteisiä pelisääntöjä kahden voimakkaan valtion välille. Mikäli Yhdysvaltojen ja Kiinan välille saataisiin luotua yhteisiä pelisääntöjä, voisivat ne toimia esimerkkinä koko muulle maailmalle ja lähtökohtana laajemman säännöstön

luomiselle. Tämä lienee helpompi lähestymistapa kuin koota kaikki maailman valtiot yhden pöydän ääreen. (Limnéll-Majewski-Salminen 2014, 149.)

Vaikka kansainvälisen kybersäännöstön kehittäminen ja sen valvonta on haastavaa, niin silti se pakostakin vähitellen muodostuu. Kovin jäykän oikeusnormiston luominen kybermaailmaan on tuskin tavoiteltavaa. Säännöstön on jäätävä riittävän väljäksi, jotta sen avulla kyetään vastaamaan alati muuttuviin kyberuhkiin. (Limnéll-Majewski-Salminen 2014, 149-150.)

Vuonna 1991 Euroopan neuvosto asetti asiantuntijakomitean selvittämään tietotekniikkarikoksiin liittyviä prosessioikeudellisia kysymyksiä. Komitea päätti työnsä vuonna 1995. Julkaistussa raportissa käsitellään rikostutkinnan kohteena olevaa elektronisessa muodossa olevaa dataa. Siinä asetettiin kyseenalaiseksi, onko viranomaisilla käytettävissään vastaavia keinoja todistusaineiston hankkimiseksi tietoverkkoihin ja -järjestelmiin kohdistuneista rikoksista, verrattuna tilanteisiin, joissa kysymyksessä on aineellisiin ja konkreettisiin kohteisiin kohdistuneet rikokset ja niiden tulkinta. (Limnéll-Majewski-Salminen 2014, 125.)

Cybercrime-työryhmä aloitti toimintansa vuonna 1997, ja sen päämääränä oli valmistella kansainvälinen yleissopimus suositusten pohjalta. Yleissopimus tunnetaan ns. Budapestin sopimuksen nimellä, ja se valmistui vuonna 2001. Viralliselta nimeltään yleissopimus on Convention on Cybercrime, eli Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus, ja se on avoin kaikille valtioille. Suomessa rikoslain 38 luku muutettiin yleissopimusta vastaavaksi syyskuussa 2007. Merkittävimpinä uudistuksina voidaan pitää tietojärjestelmän häirintää sekä törkeää tietomurtoa koskevia säännöksiä, ja lisäksi eräitä muita rangaistuksia kovennettiin. (Peltomäki-Norppa 2015, 72.)

Nykyisin kyberrikollisuuden ytimessä on globaalin tietoteknologian käyttö rikollisiin tarkoituksiin. Euroopan unionin Budapestin sopimus, joka on usein arvioitu kattavimmaksi kansainvälistä kyberrikollisuutta koskevaksi sopimukseksi, luokittelee kyberrikokset neljään pääluokkaan.

- Tiedon ja tietojärjestelmien luottamuksellisuutta, eheyttä ja saatavuutta vastaan tehdyt hyökkäykset. Tämä tarkoittaa ulkopuolisen pääsyn hankkimista tietojärjestelmään, kuten salakuuntelua, vakoilua, tiedon tai järjestelmän ulkopuolista muokkaamista ja laitteiden väärinkäyttöä.

- Tietokoneita hyödyntävät rikokset, kuten petokset ja väärentäminen. Kategoriaa voidaan täydentää identiteettivarkaudella.

- Sisällöltään rikolliset toimet, kuten lapsipornografian levittäminen, mikä voidaan täydentää myös muun vahingollisen pornografian levittämisellä, rasistisella väkivaltaa ihannoivalla tai vihapuhemateriaalilla, laittomilla uhkapeleillä, väärän tai valheellisen tiedon levittämisellä ja roskapostilla.

- Kopiosuojaa tai tuotemerkkiä loukkaavat rikokset.

Vuonna 2007 Euroopan komissio listasi kyberrikollisuuden osa-alueiksi seuraavat asiat (Limnéll-Majewski-Salminen 2014, 125).

- Tavanomaiset rikokset jotka kuitenkin tehdään sähköisten tietojärjestelmien ja viestintäverkkojen kautta tai yli

- Laittoman sisällön julkaiseminen sähköisessä muodossa ja foorumeilla

- Rikokset jotka voidaan tehdä vain sähköisissä verkoissa tai niiden välityksellä

Olemassa oleva Euroopan unionin lainsäädäntö ja kansalliset lainsäädännöt tunnistavat kyberrikoksiksi

- Yksityisyyden loukkaukset eli henkilökohtaisten tietojen laittoman keräämisen varastoimisen, muokkaamisen, paljastamisen ja levittämisen

- Sisällöltään rikolliset toimet eli pornografian levittäminen, rasistiset lausumat ja väkivaltaan yllyttävän materiaalin levittäminen

- Talousrikokset, ulkopuolinen pääsy ja sabotaasi eli ulkopuolisen pääsyn järjestelmään ja sen hyväksikäyttäminen, näistä esimerkkinä hakkerointi, sabotaasi, virusten levittäminen, vakoilu, väärentäminen ja petokset

- Aineellisten oikeuksien loukkaukset, eri tietokoneohjelmia ja tietokantoja suojelevien sääntöjen rikkominen, kopiosuojan ja muiden vastaavien oikeuksien rikkomukset

Muitakin luokitteluja on olemassa, mutta sisällöltään ne ovat samansuuntaisia edellä mainittujen kanssa. Kuten on useasti todettu, pääosa rikollisuudesta on taloudellisesti motivoitunutta, ja se muodostaa kolmasosan globaalista kyberrikollisuudesta. Kyberhyökkäykset ja turvallisuusloukkaukset ovat yleistymässä, samalla, kun niiden hienostuneisuus lisääntyy. Ne muuttuvat vielä monimutkaisemmiksi, vakavampaa vahinkoa aiheuttaviksi, ja myös vaikeammiksi estää, huomata ja reagoida kuin nykyiset hyökkäykset. Usein hyökkäykset havaitaan vasta kauan aikaa tapahtuman jälkeen, mikäli niitä huomataan lainkaan. Tämä aiheuttaa vakavan haasteen niin taloudelle kuin kansalaisten turvallisuudelle. Kyberrikollisuus on kuitenkin ensisijaisesti lainvalvontaan eikä puolustukseen liittyvä ongelma. (Limnéll-Majewski-Salminen 2014, 124-126.)

Kriminaalipoliittinen yksikkö on toiminut 1980 –luvulta lähtien YK:n sihteeristön yhteydessä. Sen toiminta on keskittynyt niin kutsuttuun valkokaulusrikollisuuteen ja vallan väärinkäyttöön. Kuitenkin vasta 1990-luvulla YK tunnisti tietotekniikan väärinkäytön rikokseksi, joka ylittää valtioiden rajat ja on julkaissut päätöslauselmia informaatioteknologian väärinkäyttöä vastaan. YK:n päätöslauselmista yksi tärkeimpiä on tietotekniikkakäsikirja, jossa käsitellään esimerkiksi tietotekniikkarikosta ilmiönä, aineellista rikosoikeutta datan, informaation haltijan ja yksityisyyden suojan kannalta sekä kansainvälistä yhteistyötä. Se poikkeaa aikaisemmista raporteista siinä mielessä, että se ei anna jäsenvaltioille lainsäädäntösuosituksia, eikä edellytä jäsenvaltioiden tekevän minkäänlaisia toimenpiteitä. YK:n peruskirja sääntelee voimankäyttöä valtioiden välisissä suhteissa, ja parhaillaan käydäänkin keskustelua siitä, voiko kyberhyökkäys jossain tilanteissa tarkoittaa sitä, että se ylittää YK:n peruskirjassa tarkoitetun aseellisen hyökkäyksen kynnyksen, jolloin valtiolla olisi oikeus aseellisiin vastatoimiin. (Peltomäki-Norppa 2015, 70-71.)

Euroopan unionin toimesta on laadittu lukuisia kyberrikollisuutta ja sen torjuntaa koskevia yleissopimuksia puitepäätöksiä ja direktiivejä. Nämä eivät kuitenkaan

sido useimpia niitä maita, joissa kyberrikollisuutta paljon esiintyy. Ainoa järjestö, joka on saanut aikaan konkreettisen sopimuksen, erilaisten suositusten lisäksi, on Euroopan neuvosto. Euroopan neuvosto on lähes kaikki Euroopan valtiot käsittävä sosiaali-, kulttuuri-, ihmisoikeus- ja lainsäädäntöyhteistyökysymyksiä käsittelevä kansainvälinen järjestö. Sen antamat suositukset ovatkin olleet useassa valtiossa ohjeena kansallisia rikoslakeja uudistettaessa, minkä vuoksi kriminalisoinnit ovat jokseenkin yhdensuuntaisia Euroopassa. (Peltomäki-Norppa 2015, 69-72.)

4 TIETOTURVASTRATEGIAN RAKENTAMINEN

Elisan tietoliikenneverkoista ja kyberturvallisuudesta vastaava liiketoimintajohtaja Pasi Korhosen mukaan, osaamme jo rakentaa varautumissuunnitelmia luonnonilmiöiden, henkilö- ja omaisuusvahinkojen, Iakkojen ja tulipalojen varalle, joten nyt tämä reaalimaailman varautumisosaaminen tulee vain ulottaa kyberturvallisuusriskeihin, osana yrityksen Iiiketoiminnan jatkuvuuden turvaamista. (Peltomäki-Norppa 2015, 98.)

Yksi syy yrityksiin kohdistuvan kyberrikollisuuden kasvuun on rikollisten verkottuminen. Sen myötä toisensa ovat löytäneet hyökkäystyökalujen valmistajat ja niitä hyödyntävät käyttäjät. Kansainväliset rikollisliigat saavat vuosittain jopa kahden miljardin dollarin hyötyjä hakkeroimalla yritysten ja laitosten verkkosivuja eri puolilla maailmaa. Käytännössä yrityksen verkkosivusto lamautetaan ensin haittaohjelmalla, ja sen jälkeen yritystä kiristetään maksamaan suojelurahaa toiminnan palauttamiseksi ennalleen. Pasi Korhosen mukaan palvelunestohyökkäyksillä kiristävien rikollisten kohteiksi on joutunut myös suomalaisia verkkokauppoja, pankkipalveluyrityksiä ja julkisen hallinnon laitoksia. (Peltomäki-Norppa 2015, 98.)

Vuonna 2012 tehdyn tutkimuksen mukaan kohteeksi valikoituivat erityisesti suuret yritykset. Suuryrityksistä 43 prosentissa oli havaittu luvattomia yrityksiä tunkeutua tietoverkkoon. Vastaava luku keskisuurien yritysten kohdalla on 24 prosenttia. Tutkimukseen vastanneiden yritysten havainnoista ei pääsääntöisesti tehty poliisille rikosilmoitusta. Yrityksen ja yhteisön kannalta katsottuna kyberuhka on merkittävä toiminnallinen riski, joka vaarantaa liiketoiminnan. Yrityksen kuin yrityksen tärkein pääoma on nykyisin tieto, jonka ylläpitoon tarvitaan toimivia tietoverkkoja. Lähes jokainen yritys käytännössä halvaantuu, jos palvelimet ja yhteydet eivät toimi ja sähköpostiserveri, laskutus sekä tili- ja asiakastiedot ovat jumissa. Kyberturvallisuuden tulee käytännössä olla osa yrityksen strategiaa, ja henkilöstöllä on oltava pelisäännöt ja laitehallinnan ajan tasalla. (Peltomäki-Norppa 2015, 99-98.)

4.1 Strategisen tason tietoturva

Yrityksen kyberturvallisuuden rakentaminen alkaa strategiselta tasolta, jonka tuottama suhteellisen abstrakti visio muunnetaan operatiivisella tasolla toimintaohjeiksi ja näin mahdollistamis- ja turvallisuussuunnitelmaksi. Strategian tekninen toteuttaminen tapahtuu suorittavalla, teknisellä kyvykkyyksien tasolla. Näin kyberstrategia viedään aina organisaation alimmalle tasolle asti, ja kyberturvallisuuden näkökanta tulee huomioiduksi koko liiketoiminnassa. Tämä ei silti tarkoita sitä, että kyberstrategia saneltaisiin vain ylhäältä alas. Liian usein tekniikka ja teknologia ohjaavat kyberturvallisuuden rakentamista, vaikka lähtökohtana tulisi olla yrityksen liiketoimintaprosessi. Silti pyrittäessä yritystoiminnan ylläpitämiseen ja tehostamiseen, ei teknisen tason osaamista ja operatiivisia näkökohtia voi jättää huomioimatta. Koska strategisella tasolla ei ole kaikkea vaadittavaa suorittavan ja teknisen tason ymmärrystä käytännön tehtävistä ja yrityksen arkipäivän toimintaan vaikuttavista kyberhaasteista, olisi strategiaprosessi hyvä toteuttaa yhteistyössä ja koko yrityksen laajuisessa vuorovaikutuksessa. Monimutkaisuuden johtamisessa ja moninaisiin ongelmiin vastaamisessa keskeistä on kommunikaatio kaikkien organisaation toimijoiden välillä ja viiteryhmien kanssa. Siten kaikkien osaaminen valjastetaan ongelmien ratkomiseen, ja huolenaiheet käsitellään laaja-alaisesti. (Limnéll-Majewski-Salminen 2014, 157.)

Kyberturvallisuuden näkeminen strategisen tason kysymyksenä, sitouttaa yrityksen johdon turvallisuusprosessiin ja sijoittaa vastuun oikealle tasolle. Se myös mahdollistaa keskitetyn kyberturvallisuusjohtamisen. Tavoitteena on tehokas turvallisuuden tuottaminen, inhimillisten virheiden vähentäminen ja tuotannon laadun varmistaminen. Yrityksen kannalta ratkaisevat päätökset pitää tehdä strategisella tasolla, ja niin yrityksen johdon kuin johtoryhmän on tunnistettava kyberturvallisuuden keskeinen asema liiketoiminnassa. Keskeisiä pohdittavia kysymyksiä ovat, miten koetut tai mahdolliset kyberhyökkäykset vaikuttavat yhtäältä yrityksen toimintatapoihin ja toisaalta koko teollisuudenalaan tai liiketoimintaympäristöön, ja miten ne vaikuttavat liiketoimintaa koskeviin päätöksiin. Tärkeä kysymys on myös, miten liiketoiminta tulisi järjestää, jotta

mielekkäiksi koetut kybermaailman mahdollisuudet voitaisiin hyödyntää turvallisella tavalla. (Limnéll-Majewski-Salminen 2014, 158.)

Täydellistä kyberturvallisuutta ei ole olemassa, sillä epäonnistumiset ja järjestelmien pettämiset ovat väistämättömiä, mutta aktiivisilla turvallisuustoimilla voidaan kuitenkin estää yritystoiminnan katkeaminen tai loppuminen häiriötilanteissa, sekä mahdollistetaan nopea toipuminen. Oikeita tai vääriä ratkaisuja tietoturvallisuusongelmiin ei ole olemassa. Yksittäisiin ongelmiin muotoillut ratkaisut vievät aina uudenlaisten ongelmien ja haasteiden eteen. Ketterä ja tasapainoinen kyberstrategia auttaa ennakoimaan syntyviä ongelmia, sillä se tarjoaa valmiin viitekehyksen, jonka puitteissa ongelmia voidaan lähteä ratkomaan, ja joka selkeästi määrittelee kunkin toimijan vastuun, yhteistyön mallit, ja luo rakenteet yhteistoiminnalle. Kyberstrategian tulee ohjeistaa jatkuvasti muuttuvien tilanteiden varalle. (Limnéll-Majewski-Salminen 2014, 159.)

4.1.1 Mahdollisuuksien kartoittaminen

Kybermaailman mahdollisuuksien kartoittaminen alkaa yrityksen ja sen toimintaympäristön vallitsevasta tilanteesta. Yritysjohdolla pitäisi olla selkeä ymmärrys siitä, mitä digitalisoinnin avaamia mahdollisuuksia yritys jo hyödyntää, missä on onnistuttu, ja missä on parantamisen varaa. Johdon pitäisi myös päättää mitä uusia mahdollisuuksia yritys pyrkii lyhyellä aikavälillä ottamaan käyttöön. Tilanteen kartoittaminen ja eri vaihtoehtojen toteuttamiskelpoisuuden arvioiminen on aikaa vievää työtä, sillä kaikkien tarjolla olevien mahdollisuuksien hyödyntäminen ei ole tarkoituksenmukaista, vaan yrityksen olisi katsottava, mikä sopii sen omaan toimintaperiaatteeseen ja ydinosaamiseen, ja mikä vastaa asiakaskunnan tarpeisiin ja on taloudellisesti järkevää. (Limnéll-Majewski-Salminen 2014, 159.)

Nykyinen toimintaympäristö vaikuttaa mahdollisuuksien toteuttamiskelpoisuuden arviointiin, mutta se ei saisi rajoittaa visiointia liikaa. Toimintaympäristöä on mahdollista muuttaa, mutta se voi tarkoittaa yritystoiminnan uudelleen muotoilua ja järjestämistä. Strategiatyön ohjaamiseksi yritysjohdolla pitäisi olla pitkän

aikavälin visio siitä, mihin suuntaan yritystoimintaa halutaan digitalisoituvassa ja yhteenkietoutuvassa maailmassa viedä. Strategiatyössä yrityksen nykyisiä vahvuuksia ja kartoittamisvaiheessa esiin nostettuja mahdollisuuksia tasapainotetaan kybermaailman sisältämiin uhkiin ja riskeihin. Kyberuhkamallisto on laaja ja jatkuvasti uudelleen muotoutuva, minkä vuoksi yrityksen on mahdotonta suojautua kaikilta mahdollisilta uhkilta, eikä osa kybermaailman uhkista, kuten kybersodankäynti tai –terrorismi, koske yritystoimintaa kuin vain epäsuorasti. Uhkiin varaudutaan lähinnä keskittymällä ensisijaisempiin, kuten kyberrikollisuuden eri muotoihin. (Limnéll-Majewski-Salminen 2014, 159-160.)

Strategiatyön tavoitteena on tasapainoinen kyberstrategia, jonka avulla yritys toteuttaa tarkoituksenmukaisiksi arvioimiaan bittien maailman mahdollisuuksia. Strategiatyön ohella ohjataan yrityksen kyberturvallisuustyötä, määrittellään sille tavoitteet, ja muodostetaan ne rakenteet, joilla kyberturvallisuuden jatkuvaa prosessia yrityksen sisällä hallinnoidaan. Kyberturvallisuuden hallinnointi ja keskitetty turvallisuusjohtaminen vaativat tuekseen aina ajanmukaista tilannekuvaa. Tilannekuva syntyy yrityksen sisällä, sen eri viiteryhmien välityksellä, ja se kyetään ylläpitämään, mikäli kyberstrategiassa on selkeästi määritelty rakenteet ja prosessit, joiden kautta yritys kerää tietoa itsestään ja ympäristöstään, tulkitsee sitä ja muuttaa sen käytännön toimintatavoiksi. (Limnéll-Majewski-Salminen 2014, 159.)

Kyberstrategiaa mietittäessä huomio kiinnitetään usein uhkiin ja riskeihin unohtaen kokonaan mahdollisuudet. Nykyisen toimintamallin suojaaminen kyberuhkilta ei yksinään tuo yrityksille uusia toimintamahdollisuuksia, vaan lähinnä aiheuttaa kustannuksia laiteinvestointien ja henkilöstökulujen muodossa. Kyberstrategia pitäisi ottaa osaksi normaalia liiketoiminnan strategiaprosessia, jolloin suojaudutaan automaattisesti juuri liiketoiminnan kannalta merkityksellisiltä kyberuhkilta. Turvallisuus-strategian yhdistäminen osaksi normaalia strategiaprosessia tuo it-osaston läheisempään yhteistyöhön liiketoimintayksiköiden kanssa. (Limnéll-Majewski-Salminen 2014, 161.)

Internetvuoden sanotaan olevan kolme kuukautta, mikä tarkoittaa nopeaa muutostahtia kybermahdollisuuksissa ja –uhkissa. Yrityksen strategiaprosessin

pitää olla riittävän ketterä ja nopeasti päivitettävä jotta muutokset voidaan ottaa huomioon. Kyberstrategian pitää lähteä liikkeelle mahdollisuuksien suunnasta, ja vasta sen jälkeen keskittyä niihin uhkiin, jotka liittyvät strategisesti tärkeiksi katsottuihin kybermahdollisuuksiin. (Limnéll-Majewski-Salminen 2014, 162.)

Mikäli kyberstrategia on osa normaalia strategiaprosessia, hyödynnettävät kybermahdollisuudet valikoituvat automaattisesti sellaisiksi, että ne tukevat suoraan liiketoiminnan kasvu- tai tehokkuusvaatimuksia. Näin muodostuu kehys, jonka avulla voidaan suojautua liiketoiminnan kannalta merkityksellisiä kyberuhkia vastaan. Kyberstrategia auttaa myös budjetoinnissa, koska sen avulla voidaan helpommin arvioida kuinka paljon rahaa kannattaa laittaa uhkilta suojautumiseen, niiden poistamiseen tai niitä vastaan vakuuttamiseen. Strategiaprosessissa olevat henkilöt tulevat tietoisiksi niin uusimmista mahdollisuuksista kuin niihin liittyvistä uhkista ja voivat entistä paremmin edesauttaa liiketoimintaa. Syntyy myös uusia innovaatioita, kun eri liiketoiminta-alueiden ihmiset soveltavat kybermahdollisuuksia omaan erikoisosaamisalueeseensa turvallisesti. (Limnéll-Majewski-Salminen 2014, 162.)

4.1.2 Esimerkkejä strategioista

Kyberympäristössä toimimisen perusedellytys on sietokyky, sillä toimintaedellytysten pystyttävä säilymään jatkuvankin hyökkäyksen alla. Yrityksen toiminta pitää suunnitella alusta pitäen sellaiseksi, että se voi toimia tilanteessa kuin tilanteessa, eikä yrityksen toiminta katkeaa, kun sitä vastaan tehdään kyberhyökkäys. Pitäisi pystyä alentamaan asteittain toimintatasoa hyökkäyksen aikana, mutta silti säilyttämään toimintakyky. Hyvänä esimerkkinä toimii sanomalehden webbisivut, jotka suuren kuorman alla lakkaavat näyttämästä kuvia, sillä kuvat kuluttavat paljon verkkokaistaa, joten niiden poistaminen vapauttaa kapasiteettia varsinaiseen tekstitiedon esittämiseen. Verkkosivun käyttäjä huomaa palveluntason heikkenemisen, mutta silti hänellä on tekstipohjainen uutispalvelu käytössään. Ennen syyskuun 11. päivä 2001

kuberuhat olivat suurelle osalle yrityksistä tuntemattomia, eivätkä ne siten olleet varautuneet niihin. Monet maailman suurimmista uutispalveluista menivät silloin polvilleen, koska niiden sivuille tuli liian paljon käyttäjiä yhdellä kertaa hakemaan jatkuvasti tietoa World Trade Centerin terrori-iskusta. (Limnéll-Majewski-Salminen 2014, 163.)

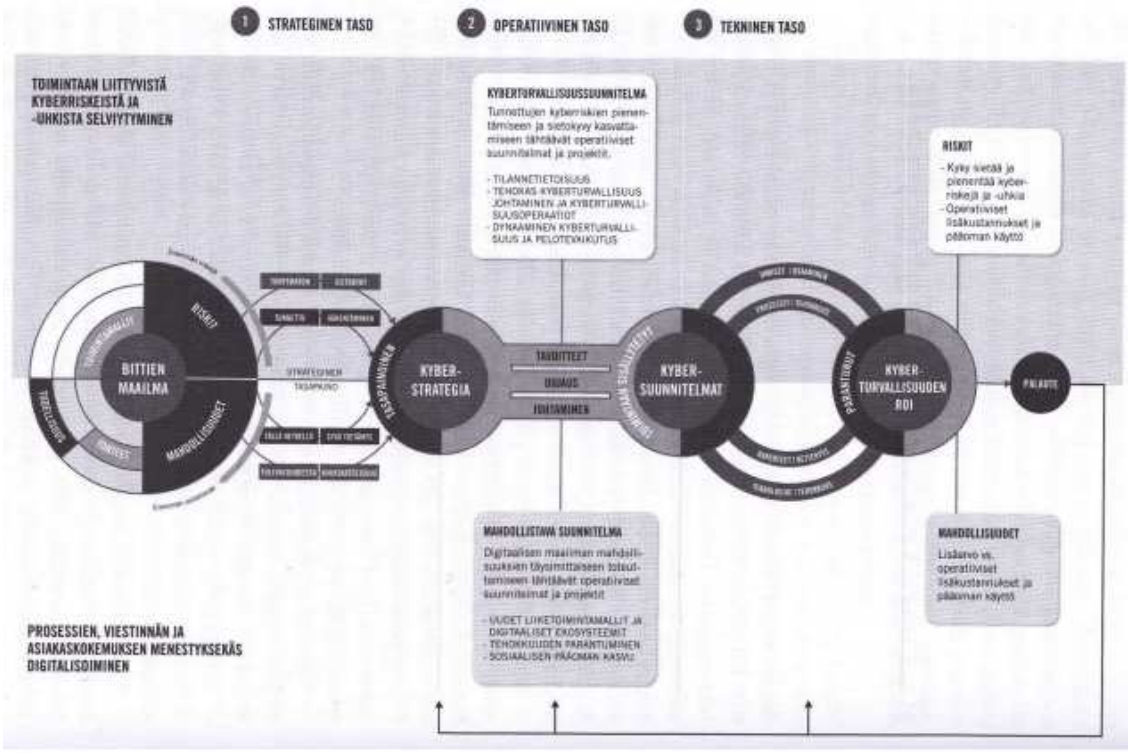
Energiateollisuudessa ja erityisesti sähkönjakelussa ei tuotetta eli sähköä voida varastoida, vaan sitä toimitetaan kuluttajalle tarpeen mukaan. Tämä aiheuttaa sen, että sähköntuottajat joutuvat optimoimaan kuinka tuottaa juuri oikea määrä sähköä juuri oikeaan aikaan. Optimoiminen ilman tietokoneiden apua on hidasta ja työlästä, jolloin tehokkaammin tulokseen päästään tietokoneiden avulla, sillä ne pystyvät optimoimaan sähköntuotannon, sähkönsiirron ja siitä kullakin hetkellä perittävän hinnan. Sähköyhtiöiden kannattavuus parani, mutta toisaalta erilaiset optimoinnit tulivat yhä monimutkaisemmiksi, jotta niillä päästiin parempaan tarkkuuteen. Sähköverkkojen hitaat mekaaniset osat korvautuivat siten nopeammilla ja etäohjattavilla laitteilla, jotka voivat toteuttaa tietokoneiden optimoimat sähkönsiirrot silmänräpäyksessä. Kehityksen myötä sähköyhtiöt ovat tulleet yhä riippuvaisemmiksi sähköisestä maailmasta, ja kaikkein moderneimmat niistä ovat niin riippuvaisia kybermaailmasta, etteivät enää voi palata entiseen manuaaliseen järjestelmään. (Limnéll-Majewski-Salminen 2014, 163-164.)

Kun kahden eurooppalaisen sähköyhtiön tietohallintojohtajan haastattelussa kysyttiin, olisiko heidän yrityksissään mahdollista palata takaisin entiseen manuaaliseen toimintamalliin, pienemmän paikallisen sähköyhtiön tietohallintojohtaja sanoi heille sen olevan vielä mahdollista. Jos kyberrikollinen esimerkiksi laukaisee muuntamon kytkimen ja pysäyttää sähkönjakelun sillä alueella, niin heiltä lähetetään mies paikan päälle laittamaan kytkin takaisin toimivaksi. Isomman kansainvälisen sähköyhtiön tietohallintojohtajan mukaan heillä vastaava ei enää onnistu. Yhtiön sähköverkon käyttö on heillä täysin optimoitu, ja kaikki muuntamot ovat täysin automaattisia ja etäohjattavia, joten siinä tapauksessa, että sähköverkon optimointi menee pois päältä, tuotanto loppuu siihen hetkeen. (Limnéll-Majewski-Salminen 2014, 164.)

Edellä esitellyillä sähköyhtiöillä on todennäköisesti hyvin erilainen kyberstrategia, koska heidän liiketoimintaympäristönsä ja sen kyberalttius ovat erilaisia. Yrityksen täytyykin löytää itselleen sopiva tasapaino kybermahdollisuuksien hyödyntämisen ja niihin liittyvien kyberuhkiin varautumisen välillä. Kyberstrategia pitää olla osana normaalia strategiaprosessia, jolloin kyberstrategiasta ei tule irrallista omaa listausta, vaan se on sisällä yrityksen yleisessä strategiassa, ja saa siten rahoituksensa samalla tavalla kuin muutkin liiketoimintaprosessit. (Limnéll-Majewski-Salminen 2014, 163-164.)

4.2 Tietoturvastrategian tasot

Kyberstrategia pitää laatia yhteistyössä organisaation eri tasojen kanssa, mutta strategiaprosessin johto pitää organisaatiossa tulla yhtäältä alaspäin. Kyberstrategiassa on kolme tasoa, jotka ovat strateginen, operatiivinen ja kyvykkyyksien eli tekninen taso. Strategisella tasolla tehdään suuret linjaukset siitä, mitä kybermahdollisuuksia yritys tulevaisuudessa käyttää, ja miten niihin liittyvät riskit otetaan huomioon. Operatiivisella tasolla laaditaan kaksi suunnitelmaa, jotka ovat mahdollistamissuunnitelma ja turvallisuussuunnitelma. Mahdollisuuksien suunnitelmassa esitetään, mitä pitää tehdä, jotta strategisella tasolla valitut kybermahdollisuudet voidaan toteuttaa. Turvallisuussuunnitelmassa kerrotaan mitä pitää tehdä, jotta tunnetut kyberriskit saadaan minimoitua, mikä nostaa sietokykyä tuntemattomia kyberuhkia vastaan.



Kuva 3. Kyberturvallisuus (Limnéll-Majewski-Salminen 2014, 166).

4.2.1 Strateginen taso

Kyberstrategian strategisella tasolla on sellaiset pääalueet kuin mahdollisuudet ja riskit. Koska uhkat ovat pitkälle riippuvaisia käytetyistä mahdollisuuksista, suunnittelu kannattaa aloittaa niistä mahdollisuuksista, joita kybermaailma tarjoaa. Mahdollisuudet jakautuvat niihin, jotka jo tunnetaan ja niihin tulevaisuuden mahdollisuuksiin, joita kukaan ei vielä ole osannut tai huomannut hyödyntää. (Limnéll-Majewski-Salminen 2014, 167.)

Myös riskien puolella vallitsee vastaava jako nykyisiin tunnettuihin riskeihin ja tulevaisuuden vielä tuntemattomiin riskeihin, joita kutsutaan usein mustiksi joutseniksi, mikä käsitteenä on peräisin lintujen maailmasta, sillä pitkään oli vallalla käsitys, ettei mustia joutsenia ole olemassa kunnes niitä yllättäen löytyikin. Mustat joutsenet jäivät vertauksena tarkoittamaan, miten jokin hyvin epätodennäköinen mutta mahdollinen tapahtuma tapahtuu. Tapahtuma voi vaikutuksiltaan olla niin merkittävä, että se muuttaa olemassa olevaa

ajattelutapaa, ja jälkikäteen se pyritään selittämään mahdollisimman järkiperäisesti. (Limnéll-Majewski-Salminen 2014, 169.)

Tyyppipuhtaana esimerkkinä mustasta joutsenesta voidaan pitää oikeutetusti syyskuun 11 päivän tapahtumat New Yorkissa. Ennen kyseistä päivää lentokoneen kaappaaminen tarkoitti ihan eri asiaa kuin sen jälkeen, eikä lentokoneen törmäämistä pilvenpiirtäjään pidetty kovin todennäköisenä, joten korkeat pilvenpiirtäjät kaupungin keskustassa olivat haluttuja asumiskohteita. Tapahtumat muuttivat kaiken kertaheitolla, ja turvallisuusviranomaisiin kohdistettiin kritiikkiä, koska he eivät olleet ymmärtäneet varautua tapahtumaan, ja lisäksi monenkirjavat salaliittoteoriat alkoivat elää omaa elämäänsä. (Limnéll-Majewski-Salminen 2014, 168.)

Tunnettujen riskien käsittely on ainakin isommissa yrityksissä hyvin ymmärretty strategian osana, siksi maailmalta löytyykin useita erilaisia standardeja ja toimintatapoja riskianalyysiin. Suurin osa yrityksistä on onnistunut löytämään perinteiset yritystoimintaansa kohdistuvat riskit ja pystyneet joko poistamaan ne tai rajoittamaan niiden vaikutusta. Kybermahdollisuuksien hyödyntäminen tuo kuitenkin joukon uusia riskejä, joita ei välttämättä ole aikaisemmin otettu huomioon. Yritykset ovat ajan mittaan tulleet yhä riippuvaisemmiksi kybertoimintaympäristöstä ja sen tarjoamista palveluista, mutta kehitystä on ollut vaikea huomata, koska se tapahtuu niin hitaasti. (Limnéll-Majewski-Salminen 2014, 169.)

Yksi kasvava riskialue on uusien palvelujen tuottaminen siten, että lopullinen palvelu koostuu useasta eri osasta, joita toimittavat useat eri yhtiöt. Kysymys ei ole alihankintaketjusta vähittäiskaupan tapaan vaan palvelusta, jossa yhdistetään olemassa olevia palveluja uusiksi paremmiksi palveluiksi. Kännykkäsovellus voi esimerkiksi kertoa milloin ja millä joukkoliikennevälineellä pääsee paikasta A paikkaan B. Lisäksi kännykkä voi GPS-paikantimella ottaa huomioon nykyisen sijainnin ja kertoa miten juuri tästä sijainnista päästään haluttuun kohteeseen joukkoliikenteen avulla. Palvelu koostuu useasta eri osasta, joita toimittavat eri toimijat. Sovellustoimittaja toimittaa varsinaisen sovelluksen, hosting-yhtiö pyörittää sovellusta palvelinfarmissaan, joukkoliikenneyhtiöt tuottavat

aikataulutiedot, teleyhtiö toimittaa interneryhteyden puhelimeen ja GPS-toimittaja antaa paikkatiedon, kuitenkin yhdenkin lenkin pettäessä palvelu lakkaa toimimasta. (Limnéll-Majewski-Salminen 2014, 169-170.)

Moniosaisissa palveluissa tulisi olla sisäänrakennettua sietokykyä, jotta ne voivat selvitä tilanteista, joissa ketjun yksi lenkki hetkellisesti pettää. Tämä edellyttää, että palveluprosessin mukanaan tuomia kyberriskejä on ajateltu etukäteen. Palvelun sisältämiä riskejä on useita, mutta niitä kaikkia vastaan ei välttämättä tarvitse suojautua. Riskianalyysilla voidaan selvittää ne riskit, joita vastaan kannattaa suojautua samoin kuin sen, missä määrin pitää suojautua. Kyberstrategian pääajatuksena on saada aikaan yritykselle sopiva tasapaino mahdollisuuksien ja niihin liittyvien riskien välillä. (Limnéll-Majewski-Salminen 2014, 167-170.)

4.2.2 Tietoturvastrategian operatiivinen taso

Operatiivisia suunnitelmia on hyvä olla ainakin, kaksi nimittäin mahdollistava suunnitelma ja turvallisuussuunnitelma. Mahdollistavan operatiivisen suunnitelman tulisi sisältää ainakin ne suunnitelmat ja projektit, joilla edesautetaan valittujen kybermaailman mahdollisuuksien hyödyntämistä. Mahdollistavat suunnitelmat ja projektit voi ryhmitellä luonteensa mukaan eri luokkiin, kuten esimerkiksi uudet liiketoimintamallit ja ekosysteemit, prosessientehostaminen ja sosiaalinen pääoma. Turvallisuussuunnitelmaan taas kuuluvat operatiiviset suunnitelmat ja projektit, joilla hallitaan kyberriskejä ja parannetaan sietokykyä. Näiden ylätasot voivat olla ajantasainen tilannetietoisuus, tehokkaat ja toimivat turvallisuusoperaatiot ja johtaminen. Dynaaminen turvallisuuden tuottaminen ja tehokas pelote. (Limnéll-Majewski-Salminen 2014, 179.)

Kuva 4. Operatiiviset suunnitelmat (Limnéll-Majewski-Salminen 2014, 179).

Ensimmäiseksi kannattaa käsitellä mahdollistava suunnitelma, koska se rajaa niitä asioita, joita pitää ottaa huomioon sitä vastaavassa turvallisuussuunnitelmassa. Toisaalta on hyvä ajatella asioita ensin vapaasti ilman rajoittavia tekijöitä. Uusilla ideoilla on mahdollisuus päästä pinnalle eikä niitä heti ammuta liiallisella kriittisyydellä alas. Kun strategiselta tasolla on saatu selville kaikkein kyberalteimmat prosessit, seuraavaksi valitaan niistä parhaiten yrityksen liiketoimintaan sopivat ja tehdään niille mahdollistamissuunnitelma. Jos strategiaprosessi ei ole vielä yrityksessä hallussa, kannattaa ottaa käsittelyyn vain yksi prosessi kerralla, ja viedä se koko kyberstrategiaprosessin läpi, jolloin organisaatiossa kaikki näkee ja oppii miten strategiaprosessi toimii. (Limnéll-Majewski-Salminen 2014, 181.)

Kybermahdollisuudet vaativat uudenlaisen liiketoimintamallin, sillä vanhat liiketoimintamallit saattavat olla liian hitaita, väärin suunnattuja ja usein liian jäykkiä soveltuakseen kybermahdollisuuksien hyödyntämiseen. Tästä tyypillinen esimerkki on se, kun vielä 1990-luvulla jokaiselle yrityksen ohjelmistolle piti olla

oma palvelin, joka oli optimoitu juuri sitä tehtävä varten, sillä hajauttamisesta katsottiin aiheutuvan monia etuja. Vuosikymmenen aikana palvelimien määrä kasvoi niin suureksi, että niitä oli hankala hallita eivätkä ne käyttäneet resurssejaan tehokkaasti. Lisäksi uudet vihreät arvot alkoivat vaikuttaa ja syntyi ns. green IT, ja yrityksiltä alettiin vaatia toimia ympäristöystävällisyyden parantamiseksi ja energiankäytön vähentämiseksi. (Limnéll-Majewski-Salminen 2014, 182.)

1990-luvulla virtuaalisointiteknologia siirtyi mainframe-tietokoneista halvempiin PC-laitteisiin, jolloin olikin mahdollista vähentää tarvittavien palvelimien määrää, ja silti toimittaa samoja palveluja kuin aikaisemmin. Aluksi virtualisoitiin tärkeitä mutta vähän resursseja kuluttavia palveluja samaan fyysiseen laitteeseen, jolloin saavutettiin nopeasti merkittäviä hyötyjä, ja yritykset innostuivat asiasta. Vähitellen virstualisointia alettiin soveltaa muihinkin prosesseihin, ja siitä löydettiin paljon muitakin etuja kuin vain palvelujen yhdistäminen. Virtualisointitekniikka toimi myös yhtenä peruspilarina uudelle liiketoimintamallille, nimittäin pilvipalveluille. Pilvipalvelut ovat haaste monelle perinteiselle liiketoiminta-alueelle, sillä ne ovat muuttaneet käsitystämme asiakkuudenhallintajärjestelmistä, sanomalehdistä, pankkitoiminnasta tai kännykkäpeleistä. (Limnéll-Majewski-Salminen 2014, 182-183.)

Rikolliset käyttävät varastettuja luottokortteja ja saavat lähetettyä suuret määrät roskapostia, ennen kuin pilvipalvelun tarjoaja huomaa asian ja alkaa tutkia sitä. Rikollista ei kuitenkaan saada kiinni, koska tämä on käyttänyt varastettua luottokorttia maksaessaan palvelusta. Toisaalta voi hyvin uskoa, ettei rikosta tutkita kovin innokkaasti, koska huijaus ei aiheuttanut vahinkoa pilvipalvelun tarjoajalle, koska se sai kyllä maksun kapasiteetistaan. Monet aloittelevat yritykset käyttävät pilvipalveluja kasvavassa määrin hyväkseen, koska silloin yrityksen ei tarvitse investoida omiin palvelimiin ja palveluihin. Internetyhteys tarvitaan, ja sitten kaikki palvelut löytyvät pilvestä erittäin kustannustehokkaasti. (Limnéll-Majewski-Salminen 2014, 183.)

Kybermahdollisuuksia kannattaa miettiä myös henkilökunnan tuottavuuden parantamisen näkökannalta. Esimerkiksi erilaiset sosiaalisen median

hyödyntämismahdollisuudet, mobiilisovellukset, etäneuvottelumahdollisuudet, työryhmäsovellusten käyttö ja uudet tiedon keräämis- ja jalostamisohjelmistot vapauttavat työntekijät ajan ja paikan kahleista. Monotoniset ja usein toistuvat tehtävät voidaan monesti digitalisoida ja hoitaa automaattisesti, jotta työntekijät voivat keskittyä paremmin hankaliin ja luovuutta vaativiin tehtäviin. (Limnéll-Majewski-Salminen 2014, 185.)

Kybertoimintaympäristö on hyvin monipuolinen, ja yrityksen kaikki toiminnot käyttävät sitä jollain tavalla hyväkseen. Usein ongelmana on, ettei yrityksellä ole kokonaiskuvaa siitä, mitä kyberympäristössä tapahtuu. Sen eri osa-alueita hoitavat yrityksen eri osastot, eivätkä ne välttämättä jaa tietoa keskenään. Siksi kattavaa tilannekuvaa muodostavan järjestelmän täytyisi ensin normalisoida eri osa-alueiden järjestelmistä saatava tieto, muuten vastaanotetut tiedot eivät ole yhteneväisessä muodossa. Hankaluutena on muutostenhallinta, sillä aina kun jokin lähettävä järjestelmä muuttaa omaa tietoaan, kuten esimerkiksi lisää yhden uuden kentän tietovirtaansa, vastaanottavan järjestelmän on tehtävä sama muutos jotta se pysyy ajan tasalla. Juuri tämä on ongelma, kun tietoja eri tietolähteistä kerätään yhteen tietokantaan, uudelleen yhdisteltäviksi ja analysoitaviksi ns. BI-työkaluilla, johtamisen tietojärjestelmissä. Pilvipalveluiden yleistyessä osa näistä ongelmista katoaa, koska pilvipalvelun tarjoaja huolehtii tilannekuvan luomisesta ja kohtaa samat ongelmat pilvensä sisällä kuin yritykset omassa verkossaan. Siksi on usein hankalaa saada kattavaa tilannekuvaa pilvipalveluiden tarjoajaltakaan. (Limnéll-Majewski-Salminen 2014, 188-189.)

Kattavaa tilannekuvaa kannattaa kuitenkin vaatia. Se on yksi peruspilari sille, että yritys pystyy käsittelemään kyberympäristön riskejä luotettavasti ja nopeasti. Tilannekuvan luominen lähtee siitä, että tunnetaan kaikki oman yrityksen järjestelmät sekä niiden kytkökset toisiinsa ja ulkopuoliseen maailmaan. IT-osastolla on yleensä tarvittavat perustiedot inventaarion tekemiseen. Sen lisäksi kannattaa käydä yrityksen eri osastot läpi ja kysyä mitä järjestelmiä he käyttävät toiminnassaan. Tällä tavalla löytyy usein järjestelmiä, joista IT-osasto ei ole koskaan kuullutkaan, ja tilannetta kutsutaankin usein nimellä varjo-IT. (Limnéll-Majewski-Salminen 2014, 190.)

Järjestelmät ovat syntyneet tarpeeseen, johon oma IT-osasto ei jostain syystä ole pystynyt vastaamaan. Esimerkkinä voidaan mainita Google Analytics, jota käytetään analysoimaan yrityksen www-sivustolla kävijöiden toimintaa ja verkkomainonnan tuloksia. Moni markkinointijohtaja oli kyllästynyt oman IT-osaston tarjoamaan hyvin tekniseen webbisivujen analyysipalveluun ja halusi ymmärrettävämpää tietoa, joka olisi lähempänä liiketoiminnan tarpeita. Googlen palvelu tarjosi tätä ja niin pientä kuukausimaksua vastaa, että se oli helppo hankkia ja ottaa käyttöön. Yrityksen oma IT-osasto ei yleensä edes tiennyt, että kyseistä palvelua oli alettu käyttää. Palvelusta kuullaan yleensä vasta sitten, kun palvelun kanssa tuli ongelmia. Ongelmien ilmentyessä yritys on täysin palvelua tuottavan organisaation armoilla, siksi tämä kannattaa ottaa huomioon palvelua ostettaessa (Limnéll-Majewski-Salminen 2014, 190).

Kybermaailmassa yrityksen omien järjestelmien lisäksi on huomioitava myös yhteiskunnan infrastruktuuri ja yrityksen yhteistoimintakumppanit. Kybermaailmassa palvelut kootaan usein palasista, joita eri palveluntuottajat tuottavat. Käyttäjät käyttävät koottuja palveluita internetin kautta. Kybermaailmassa toimiminen tarkoittaa, että olemme yhä enemmän riippuvaisia muista sen toimijoista. Sen vuoksi on erityisen tärkeää saada tilannekuva kattamaan myös muut yrityksen toimintaan olennaisesti vaikuttavat tekijät. Tällä alueella on vielä paljon tehtävää, sillä yritysten tilannekuva koostuu edelleen lähinnä niiden omista järjestelmistä. Tämä ei enää riitä vaan yritysten pitää pystyä luomaan kattava tilannekuva kyberympäristöstään, jotta kyberriskien käsittely tulisi mahdolliseksi. (Limnéll-Majewski-Salminen 2014, 190.)

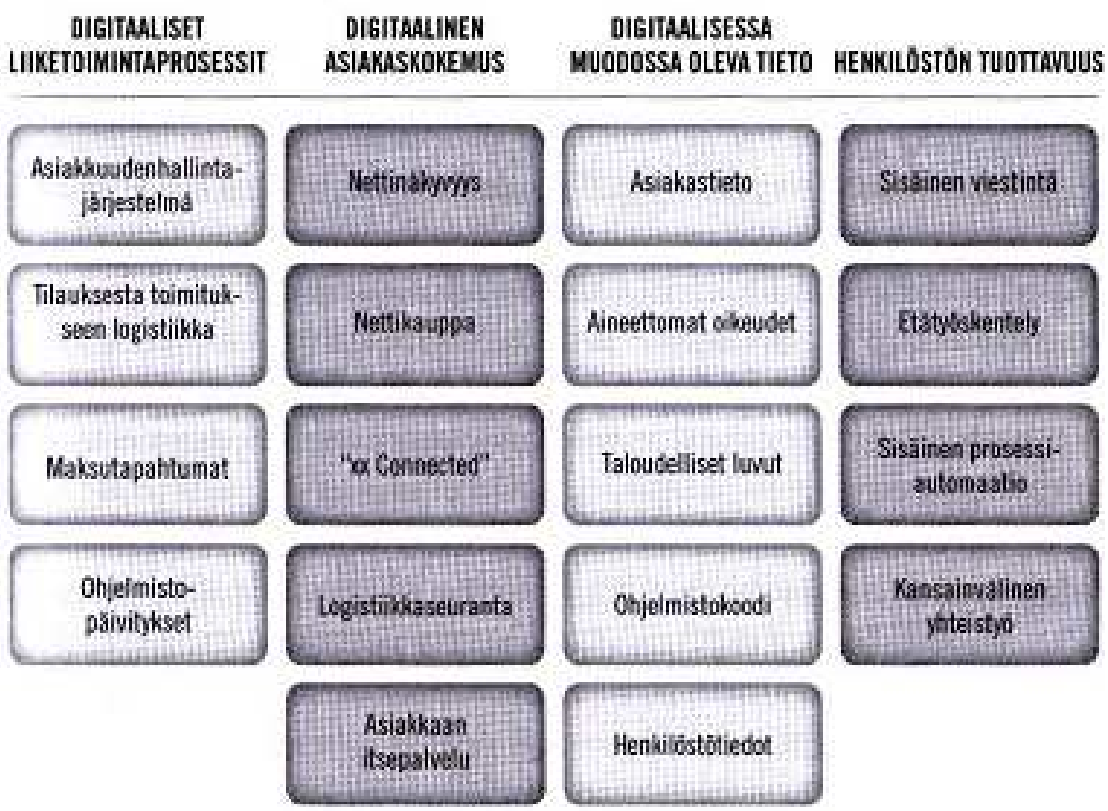
Kyberympäristössä tapahtuvat muutokset ovat usein nopeita, ja vain ajanmukaisen tilannekuvan avulla voimme reagoida niihin riittävän pikaisesti. Tilannekuva-analyysillä etsitään usein poikkeamia tavallisesta tilanteesta, sekä vaikutuksia, joita näillä on liiketoimintaprosessiin. Tämä auttaa poikkeamien priorisoinnissa, ja niiden ratkaisemiseen asetettavien resurssien laadun ja määrän valinnassa. Tilannekuvan käyttäjiä ovat usein liiketoimintaprosesseista vastaavat henkilöt, joten sen pitää olla ymmärrettävä heidän lähtökohdistaan,

eikä niinkään teknisen tietoturvallisuuden näkökulmasta katsottuna. (Limnéll-Majewski-Salminen 2014, 191.)

Keskitetty kyberturvallisuusjohtaminen tarkoittaa turvallisuuden ja yrityksen turvallisuuspolitiikkojen aktiivista hallinnointia ja toteuttamista. Tilannekuva kertoo sen, missä tilanteessa juuri sillä hetkellä ollaan, ja mikä on kybertoimintaympäristön nykytila. Kyberturvallisuus ei synny sivutuotteena tai ylläpidä itse itseään, vaan se vaatii jatkuvaa uudelleen arviointia ja johtamista. Digitalisoituminen tarkoittaa automatisoitujen prosessien lisääntymistä, mikä parhaimmillaan nopeuttaa toimintaa ja parantaa kustannustehokkuutta. Vaikka automatisoidut toiminnot parantavat kyberrurvallisuutta, ne ovat samalla kyberturvallisuudesta riippuvaisia. Ne, kuten koko kyberturvallisuuden prosessi, vaativat tuekseen keskitettyä valvontaa ja raportoimista eli tehokasta palauteprosessia. Keskitetty turvallisuusjohtaminen mahdollistaa nopeiden päivitysten ja parannusten tekemisen arkkitehtuuriin, mikä edesauttaa kyberturvallisuuden ylläpitämistä. (Limnéll-Majewski-Salminen 2014, 191.)

4.3 Haasteelliset prosessit tietoturvastrategian kannalta

Haasteellisinta kyberstrategian teossa on löytää yrityksestä ne prosessit ja toiminnot, jotka eniten hyötyvät kybermaailman kehityksestä. Yleensä niitä ovat kaikki pitkälle digitalisoidut prosessit, kuten esimerkiksi viestintään tiedon välitykseen ja asiakaskokemukseen liittyvät prosessit. Niitä kutsutaan ns. kyberalttiiksi prosesseiksi. Ne voidaan jakaa neljään luokkaan, joita ovat digitaaliset liiketoimintaprosessit, digitaalinen asiakaskokemus, digitaalisessa muodossa oleva tieto ja sen hyödyntäminen ja henkilöstön tuottavuus. (Limnéll-Majewski-Salminen 2014, 170)



Kuva 5. Kyberalttiita prosesseja (Limnéll-Majewski-Salminen 2014, 171).

Digitaaliseen asiakaskokemukseen kuuluvat nettinäkyvyys, nettikaupankäynti, itsepalveluporatalit, logistiikkaseuranta ja laitteet, jotka lähettävät tilatietoa valmistajalle. Tällaisia laitteita esimerkiksi hissi, joka kertoo käyttöä koskevaa tilastotietoa valmistajalle, joka voi tämän perusteella määritellä ennaltaehkäisevän huoltokäynnin oikean ajankohdan. Pakettikuriirien paketin seuranta on myös yksi sovellus tästä prosessista. Jokainen, joka joskus ostanut jotain nettikaupasta, on saanut ostoksensa pakettikuriirin kautta. Toimitusaika voi olla pitkä varsinkin, jos paketti tulee ulkomailta. Pakettien seurannan pitää olla pitkälle automatisoitua, jotta miljoonien pakettien seuraaminen onnistuu ja on kustannustehokasta. Tämän mahdollistaa sellaiset keksinnöt kuin viivakoodi, RFID-tunnisre, kannettavat viivakoodien lukulaitteet ja jatkuvat etäyhteydet logistiikkakeskuksen tietokantoihin. Siinä, kuten muissakin kyberalttiissa prosesseissa, on monta toimijaa, jotka pelaavat saumattomasti yhteen saadakseen aikaan ylivertaisen asiakaskokemuksen. Koko prosessi vaikuttaa yksinkertaiselta, mutta kuitenkin prosessiin kuuluu useita toimijoita, joiden tulee

pystyä vaihtamaan tietoja keskenään automaattisesti ja ilman virheitä. (Limnéll-Majewski-Salminen 2014, 173.)

Aikaisemmin tiedon jatkojalostusta ei ehkä tehty, koska se ei ollut teknologisesti mahdollista. Olisi erinomaista asiakaspalvelua, jos asiakaspalvelijalla olisi heti ensimmäisen tunnistautuminen jälkeen käytössään koko asiakkaan ostohistoria, käytössä olevat tuotteet ja tiedot avoimista ja muista palvelupyynnöistä. Yrityksissä nämä tiedot yleensä on olemassa, mutta valitettavasti kaikki eri järjestelmissä, jotka eivät pysty vaihtamaan tietoja keskenään. Edellä kuvattu on tyypillisesti kyberaltis prosessi. (Limnéll-Majewski-Salminen 2014, 173.)

Usein henkilöstön tuottavuuteen liittyvät prosessit sisältävät paljon kyberalttiita prosesseja. Tähän luokkaan kuuluvia prosesseja ovat mm. sisäinen viestintä, etä- ja mobiilityöskentely, sisäinen prosessiautomaatio ja ryhmätyö organisaation eri maissa olevien henkilöiden välillä. Henkilöstön tuottavuutta lisää esimerkiksi video- ja puhelinneuvottelut, mikäli niiden avulla voidaankin matkustamista ja lisätä tiedonkulkua ihmisten välillä. Ne vapauttavat ihmiset suunnittelemaan ajankäyttöään joustavammaksi, koska aina ei tarvitse olla läsnä toimistolla. Tämä lisää työmotivaatiota, joka taas vaikuttaa suoraan tuottavuuteen. Kyberstrategian muodostamisen ensimmäisiä tehtäviä on löytää yrityksestä tärkeät kyberalttiit prosessit. Kyberstrategia kannattaa suunnata kohti näitä prosesseja, koska ne ovat riippuvaisia kyberympäristöstä, ja niiden kautta saadaan aikaan näkyviä tuloksia nopeasti. Koska yrityksen strategiaa tehdään usein moneksi vuodeksi eteenpäin, on hyvä ottaa myös mukaan uudet lähitulevaisuuden prosessit. (Limnéll-Majewski-Salminen 2014, 175.)

Kuva 6. Kyberalttiit prosessit (Limnéll-Majewski-Salminen 2014, 177).

Prosessien valinta tulisi perustua liiketoimintatavoitteisiin ja tukea näitä tavoitteita. Seuraava askel kyberstrategiassa on suunnitella, mitä pitää tehdä kybermahdollisuuksien toteuttamiseksi ja samalla ottaa huomioon siihen liittyvät riskit sopivalla riskitasolla. Tällöin siirrytään kyberstrategian operatiiviselle tasolle ja laaditaan mahdollistamis- ja turvallisuussuunnitelma. (Limnéll-Majewski-Salminen 2014, 179.)

5 YHTEENVETO

Digitalisaation myötä syntyy uudenlaisia palvelualustoja, ekosysteemejä ja liiketoimintamalleja. Philipsin varatoimitusjohtaja Alberto Pradon mukaan digitaalisuus mahdollistaa asiakasuhteiden luonnin kokonaan uudelleen, sillä sähköisessä maailmassa voimme olla jatkuvassa vuorovaikutuksessa ja sitä kautta muuttaa ansaintamallimme ja ohjailla rahavirtoja. Digitalisaatio mahdollistaa uuden palvelulisäarvon luonnin teollisiin tuotteisiin samaan aikaan, kun se itsessään mahdollistaa palveluliiketoiminnan kasvun ja kansainvälistymisen. Palveluita ja teollisuutta ei ole enää tarpeen asettaa vastakkain, koska ne molemmat luovat samaa vaurautta ja hyvinvointia. Tulevaisuudessa, kun kuluttajat omaksuvat aina vain nopeammin uudet digitaaliset palvelut, ei näiden palveluiden toimitusetäisyyksillä ole globaalissa maailmassa enää merkitystä. (Turun Sanomat 2015.)

Digitalisaatio haastaa auktoriteetit yrityksissä ja yhteiskunnassa, koska kysymyksessä ei ole ilmiö, joka vain tulisi palvelun päälle. Se ei ole vain viestintäkanava, jota kautta tietoa jaetaan, vaan haastaa miettimään koko liiketoiminnan, sekä asiakkaan ja yrityksen välissä olevan palvelumallin uudestaan. Muutoksen myötä myös johtamisen mallit ja työn määritelmä vaativat uudistusta, koska auktoriteettien pelko katoaa, ja joustavuutta vaaditaan yhä enemmän niin yrityksiltä, yhteiskunnalta kuin työntekijöiltäkin. (Solita.fi)

Tulevaisuudessa ei menestytä vain tarjoamalla huippulaatuista tuotetta tai palvelua, vaan on oltava esillä siellä, missä ihmiset viettävät aikaansa, ja markkinointi on sidottava kohderyhmän identiteettiin, elämäntapaan sekä tarpeisiin. Yritysten ongelmana on miten saada viestit omissa medioissa ja kanavissa eteenpäin tavoitelluille kohderyhmille. Digitaalisessa ympäristössä viestintää ei pitäisi rakentaa vain tietylle kanavalle, koska kohderyhmät saattavat vaihtaa kanavaa milloin tahansa. Ihmisen tarve oman identiteetin rakentamiseen ja yhteydenpitoon pysyy samana, vaikka käytetty alusta tai palvelu muuttuisikin. (Solita.fi.)

Digitalisaatio aiheuttaa vääjäämättömästi muutoksia myös yritysten sisäiseen organisoitumiseen, koska tavat joilla ihmisten aikaa hallitaan ja mitä heiltä odotetaan pakostakin muuttuvat. Asiakkaat vaativat tulevaisuudessa vastauksia jatkuvasti ja yhä nopeammin. Työnantajien ja muiden työmarkkinoiden osapuolten tulee määritellä uudelleen mitä työllä tarkoitetaan. Pitää ratkaista vaaditaanko läsnäoloa, voidaanko työtä tehdä monesta paikasta, kenen kanssa työskennellään ja miten ollaan yhteydessä muuhun organisaatioon. Digitalisaatio mahdollistaa rajojen rikkoutumisen, jolloin yhteistyötä voidaan tehdä paljon paremmin ja tehokkaammin, mutta silloin edellytetään myös, että ihmiset suhtautuvat omaan työnkuvaansa joustavammin, ottavat palautetta paremmin vastaan ja myös hakevat apua herkemmin. Muutosprosessissa vaaditaan asennemuutosta niin työnantajilta kuin -tekijöiltä. (Solita.fi.)

Digitalisaatio on laaja alue ja vaikuttaa ympärillämme niin moneen asiaan, että kokonaisuutta sen eri ilmenemismuodoista on haasteellista ennustaa. Digitalisaation myötä asiat virtaviivaistuvat, mikä edellyttää meiltä oma-aloitteisuutta, sillä asioita pitää tehdä enemmän itse, mutta toisaalta meille tarjotaan myös paremmat mahdollisuudet tehdä asioita itse. (Solita.fi)

Valtiovallan tehtävänä olisi toimia edelläkävijänä, ja varmistaa julkisten palveluiden toimivuus ja kehittäminen. Valtiovallan tulisi luoda edellytykset sille, että Suomessa voidaan luoda todella menestyviä yrityksiä. Digitalisaatio pitää irrottaa pelkästä teknologian kehittymisestä. Valtiovalta onkin nyt ottanut hallitusohjelmaansa digitalisaation kehittämisen yhtenä keinona Suomen talouden saattamiseksi nousu-uralle. (Solita.fi)

Digitaalisen muutokset ovat tapahtuneet nopeasti, mikä on tullut monille aloille yllätyksenä, kuten esimerkiksi sähköisen median aiheuttama ahdinko perinteisille lehdille. Vaikka oma liiketoiminta olisikin vielä kannattavaa, pitää kuitenkin olla visio siitä, miten se toimii tulevaisuuden teknologiaympäristössä. Kehitystyöhön pitää investoida, olla vastaanottavainen myös organisaation sisältä tulevaan informaatioon. Olisi uskallettava resursoida muutokseen, vaikka sen liiketoiminta-arvo ei juuri sillä hetkellä näyttäisi hyvältä, silti mahdollisuuksiin on uskallettava panostaa. (Solita.fi.).

Tietoturvan kohteena yrityksissä perinteisesti on ollut aineettomat oikeudet (patentit, tekijäinoikeudet, mallisuojat, tavaramerkit, kehitysprosessit), tietokannat, sopimustekstit ja -luonnokset, viiteryhmien yhteystiedot ja asiakastiedot, prosessikuvaukset ja niin edelleen. Tavoitteena on ollut turvata tiedon säilyminen, saatavuus, liikuteltavuus, tiedon yhtenäisyys ja luottamuksellisuus. Käsitteenä kyberturvallisuus sisältää kuitenkin tietoturvaa huomattavasti laajemman ja kokonaisvaltaisemman tavan ajatella, sillä kyberturvallisuuden kohteena on myös ihmisen ja virtuaalimaailman muodostama kokonaisuus, jossa pelkkä tietoturva-ajattelu ei riitä. (Limnéll-Majewski-Salminen 2014, 55-56.)

LÄHTEET

DIGILE, Liikenne- ja viestintäministeriö, Tekes, Teknologiateollisuus ja Verkkoteollisuus (17.3.2015). Digibarometri 2015. Helsinki: Taloustieto Oy. Saantitapa: http://www.digibarometri.fi

Hiltunen, E; Hiltunen, K. 2014. Teknoelämää 2035. Helsinki: Tallentum Media Oy

Järvinen, P. 2014. NSA näin meitä seurataan. Jyväskylä: Docendo Oy

Kananen, J. 2008. Kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylä: Jyväskylän ammattikorkeakoulu

Kauppalehti Oy 2015.Suomalaisyritykset varautuneet huonosti vakavaan uhkaan. [Viitattu 7.6.2015] http://www.kauppalehti.fi/uutiset/suomalaisyritykset-varautuneet-huonosti-vakavaan-uhkaan/czhCD5DL

Keskuskauppakamari ja Helsingin seudun kauppakamari. Yritysten rikosturvallisuus 2012 – tutkimus. http://kauppakamari.fi/wp-content/uploads/2012/01/Yritysten_rikosturvallisuus_2012-.pdf

Lahti,S; Salminen, T. 2014. Digitaalinen taloushallinto. Helsinki: Sanoma Pro Oy

Lehti, M; Rouvinen, P. & Ylä-Anttila, P. 2012.Suuri Hämmennys: Työ ja tuotanto digitaalisessa murroksessa.Helsinki: Taloustieto Oy (ETLA B254)

Limnéll,J; Majewski, K; Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy

L22.4.1999. Henkilötietolaki. https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

L13.8.2004/759. Laki yksityisyyden suojasta työelämässä. http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

L16.6.2004516/2004. Sähköisen viestinnän tietosuojalaki http://www.finlex.fi/fi/laki/alkup/2004/20040516

Mäntyneva,M; Heinonen, J; Wrange, K. 2008. Markkinointitutkimus. Porvoo: WSOY Oppimateriaalit Oy

MTV Uutiset 2015. CNN: Mies hakkeroi lentokoneen tietojärjestelmään lennon aikana. Viitattu 7.6.2015 http://www.mtv.fi/uutiset/ulkomaat/artikkeli/cnn-mies-hakkeroi-lentokoneen-tietojarjestelmaan-lennon-aikana/5097778

Peltomäki,J; Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Tallentum Media Oy

Rousku, K. 2014. Kyberturvaopas. Helsinki: Tallentum Media Oy

Savon Sanomat Oy 2015. Rikoksia pian enemmän verkossa kuin fyysisesti. [Viitattu 7.6.2015] http://www.savonsanomat.fi/uutiset/kotimaa/kyberasiantuntija-jo-ensi-vuonna-suomessa-tehdaan-enemman-rikoksia-verkossa-kuin-fyysisesti/2034070

Solita.fi. [Viitattu 7.6.2015] http://www.solita.fi/think-tank/digitalisaatio-haastaa-auktoriteetit-yrityksissa-ja-yhteiskunnassa/

Suomen virallinen tilasto (SVT): Poliisin tietoon tullut rikollisuus [verkkojulkaisu].
ISSN=1797-3651. Helsinki: Tilastokeskus [viitattu: 7.6.2015].
Saantitapa: http://www.tilastokeskus.fi/til/polrik/index.html
Tietosuojavaltuutetun toimisto.
http://www.tietosuoja.fi/27212.htm

Turun Sanomat. Digitalisaatio – teollisuuden kuudes vallankumous. [Viitattu 7.6.2015]
http://www.ts.fi/mielipiteet/lukijoilta/774694/Digitalisaatio++teollisuuden+kuudes+vallankumous

Yle Uutiset 2014. Tällaisia ovat suomalaisiin kohdistuvat identiteettivarkaudet. [Viitattu 7.6.2015]
http://yle.fi/uutiset/tallaisia_ovat_suomalaisiin_kohdistuvat_identiteettivarkaudet__harvemmin_nama_selviavat/7303477

Yle Uutiset 2015.Identiteettivarkaus ei enää pelkkää petkuhuiputusta vaan oikea rikos.[Viitattu 14.9.2015]
http://yle.fi/uutiset/identiteettivarkaus_ei_enaa_pelkkaa_petkuhuiputusta_vaan_oikea_rikos/8255013