Teknologian globaalit riskit

Teknologian globaalit riskit

Jouni Kivistö-Rahnasto & Veikko Rouhiainen

Poliisin toimintaympäristö : poliisiammattikorkeakoulun katsaus 2012. ed. / Honkonen Risto; Muttilainen Vesa. Tampere : POLIISIAMMATTIKORKEAKOULU, 2012. p. 50-58 (Poliisiammattikorkeakoulun raportteja; No. 102).

Julkaisu saatavilla:

http://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/25565_Raportteja102_toimintaymparistokatsaus2012.pdf?450a4b87532ad288

Johdanto

Teknologia tarjoaa uusia tapoja tehdä asioita ja luo ennen tuntemattomia mahdollisuuksia ihmisille. Se on vaurauden ja kasvun moottori ja voidaan kai sanoa, että teknologiset ratkaisut tarjoavat myös suojaa ja perusturvallisuutta. Hyötyjen rinnalla teknologiat ja niiden käyttötavat ovat luoneet arkeen ja globaaliin kehitykseen vaikuttavia ongelmia. Yksittäisiin teknologioihin liittyviä terveys- ja turvallisuusuhkia on tavallisesti helppo tunnistaa ja arvioida; sähkö voi aiheuttaa sydämen pysähtymisen tai vaikkapa palovammoja. Arvioiminen vaikeutuu, kun teknologiaa sovelletaan haluttuun tarkoitukseen jossain ympäristössä ja sosiaalisessa yhteydessä. Syntyy monimutkainen vuorovaikutusten verkosto, johon liittyy hyötyjen lisäksi tahattomia haittoja. Verkostot luovat myös mahdollisuuksia tahalliseen vahingontekoon ja rikollisen hyödyn tavoitteluun. Teknologian riskejä pitääkin tutkia monialaisesti ja eri ryhmien näkökulmasta (Hellström 2009). Riskien tunnistamisessa etsitään tarkasteluhetkellä usein heikosti näkyviä teknologioita ja sosiaalisia prosesseja, jotka voivat yhdessä muiden ilmiöiden kanssa muodostaa merkittäviä tulevaisuuden uhkia. Tarkastelun tavoitteena on tuottaa tietoa sekä teknologian kehittämiseen että säätelyyn. (Hellström 2009.)

Tunnettu teknologia hakee jatkuvasti sovelluskohteita uusissa tai muuttuvissa ympäristöissä ja käyttötarkoituksissa. Samalla uudet keksinnöt ja teknologiat hyötyineen ja haittoineen valtaavat elintilaa. Osa teknologioista ja niiden käyttötavoista on helppo tuomita haitallisiksi ja kestämättömiksi. Suurin osa teknologioista tarjoaa kuitenkin kiistattomia hyötyjä käyttäjilleen haittaamatta kohtuuttomasti muiden yleistä etua. Lähtökohtaisesti teknologian kehityksellä ja soveltamisella tavoitellaan hyötyä – mutta mitkä ovat keskeisiä teknologian uhkia tulevaisuudessa? Yleisessä keskustelussa esiin tulevia teemoja ovat tietoturvallisuus tai kyberturvallisuus eri muodoissaan, tuotteiden, palveluiden ja tuotantojärjestelmien riskit, ilmastonmuutos ja luonnonkatastrofit sekä nanotekniikka. Tulevaisuudessa pitää kuitenkin huomioida myös arkiset ongelmat, jotka nousevat esiin väestön ikääntyessä.

Tietomurrot

Vuoden 2011 aikana tietomurrot ovat saaneet paljon julkista huomiota. Esimerkiksi suuret kansainväliset pelialan yritykset Sony[1] ja Steam-verkkokauppa[2] ovat ilmoittaneet joutuneensa tietomurtojen kohteiksi, joiden seurauksena henkilö- ja luottokorttitietoja joutui vääriin käsiin. Tietomurrot eivät ole olleet vain kansainvälisten yritysten ongelma. Lukuisat suomalaiset verkkopalvelut ovat kertoneet tietomurroista järjestelmiinsä (Napsu.fi, Netcar.fi, Terve.fi, jne.). Myös verkkokauppojen tietoturvallisuudessa on raportoitu puutteita[3] ja erilaiset käyttäjätunnusten ja salasanojen kalasteluyritykset ovat lisääntyneet. Perinteisesti suomen kieli on suojannut suomalaisia räikeimmiltä kansainvälisiltä huijausyrityksiltä, mutta on oletettavaa, että huijaukset muuttuvat näiltä osin taitavammiksi.

Sosiaalisen median ja verkkopalveluiden määrä ja käyttö kasvavat voimakkaasti ja yhä useampi ihminen kohtaa myös niihin liittyvät turvallisuusongelmat. Tietojärjestelmissä oleva tiedon suuri määrä tekee jo yksittäisistä tietomurroista seurauksiltaan laajoja (Maillart ja Sornette 2010). Ongelmiin vaikuttavat yhtäältä palvelujen käytön kasvu sekä käyttäjien ja ylläpitäjien vaihtelevat tietoturvataidot, mutta myös teknologiaan ja sen soveltamiseen liittyvät puutteet. Teknologisesta näkökulmasta ongelmia esiintyy niin ohjelmointityökaluissa ja alustoissa kuin itse järjestelmien suunnittelussa, ohjelmointityössä ja järjestelmien ylläpidossa. Oman uuden haasteensa muodostaa pilvipalvelujen tietoturva. Huolta on esitetty myös langattoman tiedonsiirron, kuten WLAN, Bluetooth ja Near Field Communication (NFC)[4], haavoittuvuudesta.

Kyberturvallisuus

World Economic Forum (2011) nostaa kyberturvallisuuden yhdeksi viidestä seurattavasta globaalista riskistä. Perinteisten tietovarkauksien lisäksi tietoverkkojen avulla on jo useita vuosia toteutettu yhteisöjen ja yritysten toimintaa haittaavia operaatiota. Esimerkiksi vuonna 2007 Viron pronssisoturin siirrosta syntyneet levottomuudet johtivat Viron valtion verkkosivujen laajaan häirintään palvelunestohyökkäysten avulla. Vastaavien hyökkäysten kohteiksi on joutunut myös suomalaisia internet-sivustoja ja eri aktivistiryhmät sekä rikollisjärjestöt tulevat jatkamaan sivustojen häirintää eri yhteyksissä. Rikollisen toiminnan lisäksi pitää varautua myös kriittisten tietojärjestelmien toimintaan suuren kuormituksen tilanteissa. Esimerkiksi säteilyturvakeskuksen internet-sivut eivät pystyneet palvelemaan Fukushiman ydinonnettomuuden aikana kasvanutta käyttäjämäärää normaalisti, vaan niiden sivujen käyttöä estyi[5]. Vastaava tilanne syntyi syksyllä 2011, kun poliisi ilmoitti julkaisevansa listan tietomurron kohteena olleista ihmisistä[6].

Kyberturvallisuus voi tarkoittaa myös sodankäyntiä. Kesällä 2010 havaittiin Iranin ydinlaitoksissa Stuxnet-mato, joka oli tarttunut prosessin ohjaamisessa käytettävään ohjelmoitavaan logiikkaan ja haitannut uraanin rikastamisessa käytettävien laitteiden toimintaa. Tartunta oli

---

[1] http://www.soe.com/securityupdate/ Saatavilla 7.12.2011
[2] http://forums.steampowered.com/forums/announcement.php?f=14 Saatavilla 7.12.2011
[3] http://www.cert.fi/tietotTerve.fiurvanyt/2011/02.html Saatavilla 7.12.2011
[4] http://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues Saatavilla 7.12.2011
[5] http://yle.fi/uutiset/teemat/japanin_tsunami/2011/03/15_000_kayntia_kaatoi_stukin_sivut_2429251.html Saatavilla 11.12.2011
[6] http://www.poliisi.fi/poliisi/hallitus/home.nsf/PFBD/F41C0D5105EF6BE1C2257941004E8C45?opendocument Saatavilla 11.12.2011

välitetty USB-tikun avulla ja mato kykeni leviämään kohdeorganisaation tietoverkossa. Stuxnet vaikuttaa juuri tietynlaiseen sähkömoottorin kierrosnopeuden säätölaitteen ohjausjärjestelmään rajatuissa olosuhteissa. Madon aiheuttama uhka muunlaisille laitoksille jäi tämän vuoksi vähäiseksi[7]. On arvioitu, että Stuxnet-mato on ensimmäinen todellinen kyber-ase, joka on suunnattu Iranin ydinaseohjelmaa vastaan (Chen 2010). Oletusta vahvistaa Stuxnet:n jälkeen havaittu uusi haittaohjelma Duqu, joka pyrkii avaamaan pääsyn kohdeorganisaatioiden tietojärjestelmiin. Duqu:n ja Stuxnet:n arvellaan olevan samojen kirjoittajien laatimia[8]. Tulevaisuudessa valtiotason toimijat nostavat valmiuttaan vastata tietojärjestelmien kautta tehtäviin hyökkäyksiin ja ne myös tavoittelevat kykyä toimia itse aktiivisesti. Kehitysresurssien kasvaessa yhä kehittyneempiä teknologioita otetaan käyttöön ja niitä myös vuotaa vahingoittamistarkoituksiin.

Tuotteiden, palveluiden ja tuotantojärjestelmien turvallisuus

Tuotantojärjestelmissä käytettävien koneiden ja laitteiden turvallisuus on viimeisten vuosikymmenien aikana parantunut selvästi suhteessa tuottavuuteen. Kuolemaan johtaneiden onnettomuuksien absoluuttisessa määrässä ei kuitenkaan voida nähdä samaa kehitystä. Poikkeuksen tekevät automaattiset tuotantojärjestelmät, joiden osalta kehittynyt automaatio on pienentänyt järjestelmien käyttäjilleen aiheuttamaa vakavaa onnettomuusriskiä (Kivistö-Rahnasto 2009). Viimeisten vuosien aikana tietotekniikka on kuitenkin luonut uhkia, jotka mahdollistavat tuotantojärjestelmien ja tuotteiden toiminnan tarkoituksellisen häiritsemisen ja vahingoittamisen. Uhkien keskeiset kohteet ovat tuotannon ohjauksessa käytettävät tietojärjestelmät sekä itse tuotantoprosessin ja tuotteiden ohjausjärjestelmät. Erilaisten asiakasjärjestelmien sekä tuotannonohjausjärjestelmien tietoturva on ollut pitkään kiinteä osa yritysten tietoturvallisuutta. Uutena uhkana tulee huomioida tuotantoprosessien ja tuotteiden ohjauksessa käytettävä tietotekniikka.

Teknologian yleisen turvallisuuden kannalta kesällä 2010 havaittu Stuxnet-mato on merkittävä. Mato mursi oletuksen ohjelmoitavan logiikan puhtaudesta haittaohjelmilta. Yleisistä tietoverkoista suljettujenkin järjestelmien ohjaukseen voidaan puuttua ulkopuolelta ja periaatteessa kohteena voi olla mikä tahansa kodin elektroniikasta liikennejärjestelmiin tai aina suuronnettomuusvaarallisiin laitoksiin. Tulevaisuudessa tuotteet ja tuotanto yhdistyvät nykyistäkin voimakkaammin osaksi laajoja palvelujärjestelmiä, joissa uudet uhkakuvat pitää huomioida järjestelmien hankinnassa ja kehittämisessä. Teollisuus ja tutkimusyhteisö ovat tarttuneet ongelmaan ja uusia teknisiä ratkaisuja ja yhteistyömuotoja on alettu kehittää (kts. Ahonen 2011, Sundell ym. 2011)

Suuronnettomuudet, luonnonkatastrofit ja ilmastonmuutos

Suuronnettomuus aiheuttaa suuren määrän loukkaantumisia tai kuolemia, mutta se voi vahingoittaa myös merkittävästi ympäristöä, omaisuutta tai varallisuutta[9]. Suuronnettomuus voi aiheutua esimerkiksi ydinlaitoksen, tuotantolaitoksen, kaivostoiminnan jätealueen, ratapihan tai satama-alueen hallitsemattomasta tilanteesta[10]. Merkittäviä vahinkoja voi tapahtua myös

[7] http://www.f-secure.com/weblog/archives/00002066.html Saatavilla 7.12.2011
[8] http://www.symantec.com/connect/pt-br/w32_duqu_precursor_next_stuxnet Saatavilla 7.12.2011
[9] Turvallisuustutkintalaki 525/2011
[10] Sisäasiainministeriön asetus erityistä vaaraa aiheuttavien kohteiden ulkoisesta pelastussuunnitelmasta 3.5.2011/406

maa-, meri- ja ilmailuliikenteessä sekä erilaisissa rakennettuun ympäristöön liittyvissä onnettomuuksissa. Suuronnettomuusriskien hallinnassa on pitkään korostettu organisaation toimintatapojen ja turvallisuuskulttuurin merkitystä turvallisen toiminnan kehittymiseen. Usein onnettomuuksia kuitenkin selitetään yksinkertaisesti inhimillisellä virheellä, vaikka kyseessä olisikin laajempi järjestelmään ja toimintakulttuuriin liittyvä ongelma. Riskit kehittyvät paitsi tekniikan ja ihmisten aktiivisista virheistä, niin myös piilevistä olosuhteista (Reason 1997)

Suurimmat globaalit onnettomuus- ja vahinkoriskit liittyvät maanjäristyksiin ja hirmumyrskyihin. Niiden osalta Suomi sijaitsee turvallisella alueella. Japanissa 2010 tapahtuneen maanjäristyksen ja sitä seuranneen tsunamin seurauksena arvioitiin kuitenkin uudelleen mm. ydinvoimaloiden turvallisuutta ääriolosuhteissa (Säteilyturvakeskus 2011). Esimerkiksi voimakkaat tuulet voivat aiheuttaa ongelmia sähköverkolle ja maa-, meri ja ilmaliikenteelle. Myrskyt kasvattavat myös tulvavaraa rannikkoalueilla. Tulviin liittyvät riskit ovat erityisen merkittäviä, koska ne aiheuttavat sekä suoria aineellisia tuhoja että henkilövahinkoja. Lisäksi tulvista aiheutuu epäsuoria haittoja, kuten tuotannon menetyksiä, viivästymisiä sekä yleistä vaivaa ja hankaluutta (Jonkman 2008). Usein tulvaveteen pääsee myös vaarallisia aineita (Cozzani ja muut 2009) esimerkiksi jäte- ja raaka-ainevarastoista, kaatopaikoilta sekä jäteveden käsittelylaitoksista ja viemäreistä. Erityinen ongelma muodostuu saastuneiden tulvavesien sekoittumisesta juomaveteen. Rankkasateet voivat myös aiheuttaa maa-ainesten eroosiota, joka voi johtaa sortumiin siltojen tukirakenteissa, penkereissä, rummuissa sekä padoissa ja kaivannoissa (Ala-Outinen ym. 2004).

Laajoja luonnonkatastrofeja todennäköisemmät uhat Suomessa liittyvät ilmastonmuutoksen vaikutuksiin. Ala-Outinen ja muut (2004) arvioivat, että lämpötilan nousu lisäisi tieverkoston lumenpoistoa ja liukkaudentorjuntaa tammi-helmikuun aikana. Kunnossapidon tarve vastaavasti vähenisi marras-, joulu- ja maaliskuussa. Lisääntyvä sademäärä puolestaan nostaisi taajamatulvien riskiä (Aaltonen ym. 2008). Talven routakauteen sijoittuvat vesisateet ja sulamisvedet voisivat myös aiheuttaa talvitulvia (Ala-Outinen ym. 2004). Toisaalta jäätiköiden sulamisesta johtuva merenpinnan nousu ei välttämättä olisi Suomessa erityisen merkittävä ongelma, koska rannikkoalueiden maan kohoaminen kompensoi sen vaikutusta.

Nanotekniikan riskit

Nanotekniikka on uusi ja kasvava teknologian alue. Nanotekniikassa luodaan uusia materiaaleja, rakenteita ja laitteita hyvin pienten 0.1-100 nm kokoisten partikkeleiden avulla. Nanoteknologiaa sovelletaan jo nyt useilla teollisuuden aloilla. Koska kyseessä on uusi teknologia, ei sen kaikkia haittoja ja vaaroja tunneta. Ihmisiin ja ympäristöön kohdistuvien vaikutusten arvioiminen ja tunteminen ovat kuitenkin nanotekniikkaan perustuvien tuotteiden valmistuksen ja käytön sekä yleisen hyväksymisen edellytys. Tulevaisuudessa nanotekniikkaan liittyvä lainsäädäntö ja standardisointi kehittyvät, mikä osaltaan luo edellytyksiä teknologian turvalliselle käytölle. (Itävaara ja muut 2008.) Nanotekniikan riskien ymmärtämiseen ja hallitsemiseen panostetaan Euroopassa voimakkaasti. Tiedon lisäämiseksi ja toiminnan koordinoimiseksi on perustettu eurooppalainen NanoSafety Cluster[11], jonka yhteistyötä koordinoi Työterveyslaitos.

[11] http://www.nanosafetycluster.eu/ Saatavilla 7.12.2011

Teknologia ja ikääntyminen

Eurooppa ikääntyy ja suomalaiset sen mukana. Sisäministeriön toimintaohjelmassa ikääntyvien turvallisuuden parantamiseksi (Mankkinen 2011) esitetään useita turvallisuuden tunteeseen, asumiseen, tapaturmiin, liikkumiseen, erilaiseen kaltoinkohteluun ja rikollisuuteen sekä alkoholin käyttöön liittyviä ongelmia ja toimenpidesuosituksia. Monet ikääntymisen riskit liittyvät rakennettuun ympäristöön. Kaatumiset kotiaskareissa ovat esimerkki arjen riskeistä, joita voidaan pienentää yksinkertaisilla tekniikoilla: pitävät ja tasaiset alustat, tukevat kalusteet, tukikahvat, riittävä valaistus, jne. (Mänty ja muut 2007). Tulipalotilanteissa alentunut toimintakyky vaikeuttaa omatoimista pelastautumista tai tekee sen jopa mahdottomaksi. Myös liikkuminen ja siihen liittyvä infrastruktuuri aiheuttavat ikääntyville erityisiä riskejä. Yli 70-vuotiaiden riski joutua onnettomuuteen kasvaa voimakkaasti (Järvinen 2005). He myös vammautuvat helpommin kuin nuoret ja toipuminen on vaikeampaa.

Useissa läntisissä maissa kehitetään keinoja vastata ikääntyvän väestön tuki- ja hoitotarpeisiin. Myös yritykset etsivät uusia liiketoimintamahdollisuuksia, tuotteita ja palveluita aikaisempaa vauraampien ikäihmisten (Reinmoeller 2011) ja julkisen sektorin tarpeisiin. Ikääntyvät arvioivat tuotteita ja palveluita hyvin käytännöllisesti hyötyjen ja kustannusten näkökulmista. He ovat myös valmiita hyväksymään ja käyttöönottamaan avustavaa teknologiaa. (Giuliani ym. 2005.) Käyttöönoton halukkuus kuitenkin alenee, jos toimintakyky on ehtinyt laskea liian alhaiseksi tai tuotteiden ja palveluiden käyttö koetaan hankalaksi tai turvattomaksi (Laukkanen ja muut 2007). Ikääntyvien avuksi kehitettävän teknologian helppokäyttöisyydelle ja luotettavuudelle pitääkin asettaa tavallista korkeammat tavoitteet. Esimerkiksi haja-asutusalueilla tieto- ja sähköverkkojen toiminnassa sekä matkapuhelinverkkojen kuuluvuudessa voi ilmetä häiriöitä. Myös teiden kunto erityisesti talviaikaan voi haitata palveluiden perillepääsyä (Mankkinen 2011). Tulevaisuudessa ikääntyvät kansalaiset käyttävät myös erilaisia sähköisiä palveluita nykyistä enemmän, mikä altistaa heidät erilaisille tietoturvallisuusuhkille.

Yhteenveto

Teknologian riskit ovat laaja ongelma, jota pitää tarkastella useiden eri ryhmien näkökulmista. Keskeisimpiä tulevaisuuden teknologisia riskejä tulee olemaan kyberturvallisuuden ongelmat. Ne tulevat vaikuttamaan sekä kaikenikäisten yksityishenkilöiden että valtioiden ja yritysten toimintaan. Sosiaalisen median ja palveluiden sekä erilaisten tuotteiden nykyistäkin tiiviimpi sulautuminen tarjoaa paitsi hyötyjä käyttäjilleen, niin myös mahdollisuuksia rikolliselle toiminnalle. Internet on globaali foorumi ja sen käyttäjien määrä jatkaa kasvuaan erityisesti kehittyvissä maissa. Huomioitavaa on myös se, että tulevaisuudessa yhä useampi ikääntyvä käyttää tieto- ja viestintätekniikkaa nykyistä enemmän. Yritykset ovat jo ottaneet vauraat ikäihmiset tärkeäksi tuotteiden ja palveluiden kohderyhmäksi. Oletettavasti näin tekevät myös rikolliset verkossa.

Ilmastonmuutos on jo itsessään teknologian käytön aiheuttama toteutuva riski, joka aiheuttaa monia ongelmia erityisesti rakennetulle ympäristölle, liikennejärjestelmille sekä energiantuotannolle. Muutokset ovat hitaita ja uhat alkavat vaikuttaa vasta vuosien kuluessa. Toisaalta rakennettu ympäristö ja infrastruktuuri uudistuvat hitaasti ja tulevat muutokset pitää huomioida jo nykyisissä investoinneissa ja varautumissuunnitelmissa.

Nanotekniikka on uusi ja voimakkaasti kasvava teknologian alue. Sen aiheuttamia haittoja terveydelle ja ympäristölle ei täysin tunneta. Toisaalta Nanotekniikan kehitys seuraa muiden

uusien teknologioiden kehityskaarta, jolle on ominaista alun epätietoisuus ja sen edellyttämä varovaisuuden periaate. Vielä muutamia vuosia sitten keskustelun kohteena oli geeniteknologia. Nanoteknologiaa ja sen riskejä tutkitaan voimakkaasti ja uusi tieto auttaa ymmärtämään ja säätelemään sen turvallista käyttöä.

Ihmiset kokevat tuntemattomat ja pelottavat uhkat voimakkaammiksi kuin tutut arkiset vaarat. Teknologian riskien arvioimisessa huomio kiinnittyy luonnostaan uusiin ja tuntemattomiin uhkiin, joiden seuraukset saattavat olla suuria. Samalla unohtuvat arkiset vaarat, jotka aiheuttavat päivittäin suuria yksilötason vahinkoja, Tärkein tapaturmaisen kuoleman syy Suomessa on kaatuminen, jonka torjuntaan on olemassa paljon yksinkertaisia keinoja. Kaatumisten lisäksi tulipalot aiheuttavat merkittävän riskin erityisesti ikääntyville. Ongelmaa pahentaa sekä ikääntymiseen liittyvä toimintakyvyn heikkeneminen että asuntojen ja niiden varustelun sopimattomuus ikäihmisen itsenäiseen asumiseen. Myös ikääntymisen liittyvät liikenneriskit pitää huomioida tulevaisuuden teknologian kehitystyössä.

Lähteet

Aaltonen, J., Hohti, H., Jylhä, K., Karvonen, T., Kilpeläinen, T., Koistinen, J., Kotro, J., Kuitunen, T., Ollila, M., Parvio, A., Pulkkinen, S., Silander, J., Tiihonen, T., Tuomenvirta, H. & Vajda, A. 2008. Rankkasateet ja taajamatulvat. Suomen ympäristö 31. Suomen ympäristökeskus. 123 s.

Ahonen, P. 2010. TITAN-käsikirja. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektista. VTT julkaisuja. 152 s.

Ala-Outinen , T., Harmaajärvi, I., Kivikoski, H., Kouhia, I., Makkonen, L., Saarelainen, M., Tuhola, M. & Törnqvist, J. 2004. Ilmastonmuutoksen vaikutuksia rakennettuun ympäristöön. VTT tiedotteita 2227. 83 s. + 6 liites.

Chen, T. M. 2010. Stuxnet, the real start of cyber warfare? Editor's Note. Network, IEEE , Vol.24 (6). ss. 2-3.

Cozzani, V., Campedel, M., Renni, E., & Krausmann, E. 2009. Industrial accidents triggered by flood events: Analysis of past accidents. Journal of Hazardous Materials, Vol 175 (1-3). ss. 501-509.

Giuliani, M.V., Scopelliti, M. & Fornara, F. 2005. Elderly people at home: technological help in everyday activities. IEEE International Workshop on Robot and Human Interactive Communication. ss. 365-370.

Hellström, T. 2009. New vistas for technology and risk assessment? The OECD Programme on Emerging Systemic Risks and beyond. Technology in Society, Vol 31 (3). ss. 325-331.

Itävaara, M., Linder, M. & Kauppinen, E. 2008. Nanomateriaalien mahdollisuudet ja riskit – Esiselvitys. Eduskunnan tulevaisuusvaliokunta. Teknologian arviointeja 26. 26 s.

Jonkman, S.N., Bočkarjova, M., Kok, M. & Bernardini, P. 2008. Integrated hydrodynamic and economic modelling of flood damage in the Netherlands. Ecological Economics, Vol 66 (1). ss. 77-90.

Järvinen, M. 2005. Liikennetapaturmat. Kustannus Oy Duodecim. Saatavilla 11.12.2011: http://www.terveyskirjasto.fi/terveyskirjasto/tk.koti?p_artikkeli=suo00040

Kivistö-Rahnasto, J. 2009. Machine-related fatalities. Proceedings of the 17th World Congress on Ergonomics IEA 2009, CD-ROM. International Ergonomics Association. 4 s.

Laukkanen, T., Sinkkonen, S., Kivijärvi, M. & Laukkanen, P. 2007. Innovation resistance among mature consumers. Journal of Consumer Marketing, Vol. 24 (7). ss. 419-427.

Maillart, T. & Sornette, D. 2010. Heavy-tailed distribution of cyber-risks. The European Physical Journal B - Condensed Matter and Complex Systems, Vol. 75 (3). ss. 357-364.

Mankkinen, T. 2011. Turvallinen elämä ikääntyneille. Tomintaohjelma ikääntyneiden turvallisuuden parantamiseksi. Sisäasianministeriö, Muistio. 57 s. Saatavilla 7.12.2011: http://www.intermin.fi/intermin/biblio.nsf/9331E7C5615DB132C225789300406FF3/$file/19 2011.pdf

Mänty, M. Sihvonen, S., Hulkko, T & Lounamaa, A. 2007. Iäkkäiden ihmisten kaatumistapaturmat. Opas kaatumisten ja murtumien ehkäisyyn. Kansanterveyslaitoksen julkaisuja B29/2007. 72 s.

Säteilyturvakeskus. 2011. Selvitys varautumisesta ulkoisiin tapahtumiin suomalaisilla ydinvoimalaitoksilla. Selvitysraportti. 7 s. Saatavilla 7.12.2011: http://www.stuk.fi/stuk/tiedotteet/fi_FI/news_680/_files/85560184208228429/default/2_TEM -selvitysraportti.pdf

World Economic Forum. 2011. Global Risks 2011 Sixth Edition. An initiative of the Risk Response Network. World Economic Forum, 56 s. Saatavilla 7.12.2011: http://riskreport.weforum.org/global-risks-2011.pdf

Reason, J. 1997. Managing the Risks of Organizational Accidents. Ashgate Publishing Limited. 252 s.

Reinmoeller, P. 2011. Service Innovation: Towards Designing New Business Models for Aging Societies. Teoksessa: The Silver Market Phenomenon, Kohlbacher, F. & Herstatt, C. (toim.). Springer Berlin Heidelberg. ss. 133-146.

Sundell, M., Kuivalainen, J., Mäkelä, J., Gervais, A., Orava, J. & Hyppönen, M. H. 2011. White Paper on Industrial Automation Security in Fieldbus and Field Device Level. 43 s. Saatavilla 11.12.2011: http://www.vacon.com/Vacon-White-Paper-On-Industrial-Automation-Security-In-Fieldbus-And-Field-Device-Level.pdf