Turvallisuussymposium 2019
Tampereen yliopisto
10.10.2019

X-risks – not only science-fiction anymore (prof. *Hiski Haukkala*, Tampereen yliopisto/kansainvälinen politiikka)

X-riskeiksi kutsutaan sellaisia globaaleja riskejä, jotka uhkaavat inhimillisen elämän edellytyksiä ja tulevaisuutta maapallolla. Tämän hetken olemassaolevia globaaleja riskejä ovat mm. hallitsematon ilmastonmuutos ja siihen liittyvät äärimmäiset sääilmiöt ja luonnonkatastrofit. Muita X-riskejä ovat ydinsota, pandemia, asteroidin putoaminen, ihmiskunnan henkistä kehitystä rajoittavan globaalin totalitaristisen järjestelmän rakentuminen ja ihmisälyyn nähden ylivertainen tekoäly. Kaikki X-riskit eivät tällä hetkellä kuitenkaan ole yhtä todennäköisiä.

Lisäksi on huomattava, että asteroidiriskiä lukuunottamatta edellä mainitut riskit ovat ihmisten toiminnasta joko suoraan tai välillisesti riippuvaisia. Niiden toteutumiseen vaikuttaa alati kasvava systeeminen kompleksisuus, teknologian kehittyminen ja talouskasvun ekologiset rajoitteet.

Riskienhallinnan näkökulmasta X-riskeihin liittyy lukuisia tuntemattomia tekijöitä. Useimpien X-riskien toteutumistodennäköisyys on melko matala, mutta toteutuessaan niiden vaikutus olisi huomattava. On tärkeää ottaa riskit vakavasti, mutta samalla pyrkiä välttämään tarpeetonta spekulointia ja paniikkitunnelman luomista.

Aiheesta on vuonna 2018 julkaistu Vulnerable world hypothesis -konsepti (Boström, N. 2018. The Vulnerable World Hypothesis. Future of Humanity Institute, University of Oxford. Working Paper, v. 3.46; http://www.nickbostrom.com/papers/vulnerable.pdf).

Riskien, myös X-riskien, laajuutta voidaan tarkastella seuraavien ulottuvuuksien kautta:

- henkilökohtaiset riskit
- paikalliset riskit
- globaalit riskit
- sukupolvien väliset riskit
- kaikkia sukupolvia, myös tulevia koskettavat riskit.

Teknologista kehitystä ei voi eikä kannata pysäyttää. Uuden teknologian hyödyntämisen ajoitus on keskeinen kysymys. Mahdolliset haittavaikutukset on tärkeää tunnistaa etukäteen ja minimoida riskit.

Riskienhallinnassa pääpainon on oltava ennaltaehkäisemisessä. Jos globaali X-riski toteutuu, on liian myöhäistä toimia tehokkaasti. Ihmiskunnalla on aikaa ennaltaehkäiseviin toimiin, mutta erityisesti ydinsota- ja ilmastonmuutosriskin suhteen tarvitaan nopeitakin toimia. X-riskien hallinta edellyttää ennakkoluulotonta ajattelua ja tutkimusta sekä strategista ennakointia ja ennaltaehkäisytoimien priorisointia. Myös resilienssi eli sopeutumiskyky muuttuviin tilanteisiin ja olosuhteisiin on tärkeää. X-riskien hallinta edellyttää poliittisia toimia esimerkiksi toimenpiteiden ajoituksen ja niiden edellyttämien resurssien allokoinnin näkökulmasta. Tämä ei ainakaan yksinkertaista käytännön toteuttamista.

Overview of the Network and Information Security Group (yliopisto-opettaja *Marko Helenius*, Tampereen yliopisto/tietoturvallisuus)

Tampereen yliopiston NISEC-tutkimusryhmä (Network and Information Security Group) toimii seuraavilla osa-alueilla:

- IoT-turvallisuus (Internet of Things)
- verkkoturvallisuus
- laiteturvallisuus
- yksityisyys ja käyttäjäturvallisuus.

NISEC-laboratorio (TUT Cyber Labs) sisältää eräänlaisen Internetin pienoismallin sisä- ja ulkoverkkoineen, niiden välisine DMZ-alueineen (Demilitarized Zone) sekä eri tyyppisine palvelimineen ja työasemineen. Täten laboratoriossa voidaan simuloida mm. verkkohyökkäyksiä, ja sitä voidaan käyttää tehokkaasti opetus- ja tutkimustoimintaan.

NISEC:n projekteja ovat mm.:

- ASCLEPIOS (pilvipohjaiset terveydenhuollon palvelut)
- CYBELE (big data, pilvilaskenta, suurteholaskenta ja IoT ruoantuotannossa)
- SCARE (ns. sivustakanavien, kuten virransyötön, sähkömagneettisen spektrin ominaisuuksien, ajoituksen ja akustisten ominaisuuksien kauta tapahtuvat verkkohyökkäykset ja niiden torjuminen).

NISEC:n opetustarjontaan kuuluvat mm. seuraavat 5 op:n laajuiset opintokokonaisuudet:

- Kyberturvallisuus I: perusteet
- Turvallinen ohjelmointi
- Verkkoturvallisuus
- Kyberturvallisuus II: erikoistuminen
- Identiteetin- ja pääsynhallinta
- Päivittäinen tietoturvallisuus
- Salausmenetelmät.

Protecting knowledge in digital transformation (yliopisto-opettaja TkT *Ilona Ilvonen*, Tampereen yliopisto/tietojohtaminen)

Digitaalinen murros on synnyttänyt organisaatioiden rajat ylittävän virtuaalisen kommunikaation, joka on paitsi lisännyt kommunikaation nopeutta ja määrää myös hämärtänyt yksityiselämän ja työelämän välistä rajaa.

Tiedon käsitteessä on erotettavissa (1) kokemuspohjainen mutta vaikeasti ilmaistavissa oleva hiljainen tieto, (2) helposti ilmaistavissa ja jaettavissa oleva eksplisiittinen tieto ja (3) erityistä innovointi- ja kilpailuetua tarjoava tärkeä tieto.

Tiedonhallintaan liittyviä riskejä ovat tiedon häviäminen tai sen joutuminen kilpailijoiden käsiin huonosti hoidetun tiedonhallinnan tai suoranaisen tietovarkauden kautta. Riskeiltä voidaan suojautua muodollisesti lainsäädännön (patentit, tavaramerkit, tekijänoikeudet, sopimukset jne.) ja teknillisten ratkaisujen (pääsynhallinta, viestintäkanavien, järjestelmien ja

tallennustilan suojaus jne.) avulla. Epämuodollisia suojautumiskeinoja ovat tiedon jakamisen ja tietoon pääsyn rajoittaminen, tiedon hajauttaminen siten, että vain asiaankuuluvilla henkilöillä on mahdollisuus sen perusteella muodostaa kilpailuetua tarjoava kokonaiskuva, koulutus ja organisaation itse määrittämät sosiaaliset normit.

Teknillisiin haasteisiin joudutaan vastaamaan myös ei-teknillisin keinoin. Digitalisaation murros korostaa yksilön asemaa. Tiedon suojaaminen edellyttää tärkeän tiedon ja sen mahdollisten leviämiskanavien tunnistamista ja näiden rajojen selkiyttämistä, johdon tukea yksilöiden tiedonhallintaa koskevalle päätöksenteolle ja tiedon jakamisen ja suojaamisen välistä mielekästä tasapainoa.

Suurten tapahtumien nivoutuminen kaupunkiturvallisuuteen ja sen kehittämiseen (riskienhallinta- ja turvallisuusjohtaja *Jouni Perttula*, Tampereen kaupunki/konsernihallinto)

Tampereen kaupungin strategiassa monimutkaistuva turvallisuusympäristö on määritetty yhdeksi keskeiseksi toimintaympäristötekijäksi yhdessä teknologisen kehityksen, työelämän muutoksen, kaupungistumisen, globalisaation, kaupunkien välisen kilpailun, kansalaisyhteiskunnan vahvistumisen ja ilmastonmuutoksen kanssa. Turvallisuutta kehitetään mm. kolmannen sektorin kanssa tehtävän verkostoyhteistyön kautta tavoitteena rakentaa Tampereesta Pohjoismaiden vetovoimaisin elämyskaupunki. Tampere ennakoi monimutkaistuvaa turvallisuusympäristöä ja kehittää kaupunkiturvallisuutta kokonaisvaltaisesti ja suunnitelmallisesti yhteistyössä turvallisuusekosysteemin toimijoiden kanssa.Tampere haluaa erottautua kansallisesti ja kansainvälisesti edelläkävijänä turvallisuuden kehittämisessä ja turvallisena asuin- ja työskentelypaikkakuntana. Yksi keino tavoitteiden saavuttamiseen on kuuden turvallisuusalan yrityksen ja julkisen sektorin toimijan yhteistyönä toteutettava kolmivuotinen SURE-projekti (Smart Urban Security and Event Resilience), jonka fokus on keskusta-alueen tapahtumaturvallisuus ja sen nivoutuminen kaupunkiturvallisuuteen.

SURE on yksi kolmesta EU-rahoitusta Suomessa saavasta turvallisuushankkeesta. Sen puitteissa kehitetään innovatiivista kokonaisratkaisua, jonka osina ovat dataintegraatioalusta, älykäs valaisinverkko, valokuituverkko, 5G ja muut nopeat langattomat verkkoratkaisut, kamerat ja infonäytöt. Tavoitteena on tamperelaisten ja kaupungissa vierailevien arjen turvallisuuden parantaminen. Hanketta toteutetaan lähtien turvallisuussuunnittelusta simuloinnin kautta harjoitustilanteisiin ja investointeihin. Keskeinen osa-alue on sensoriteknikka, jonka tarjoaman datan pohjalta tekoälyn ja analytiikan kautta palvellaan tapahtumapaikan, pelastuslaitoksen ja poliisin tilannekeskuksia ja Väyläviraston tieliikennekeskusta. Sensoritekniikka auttaa palvelumuotoilun kautta myös oikean ja oikea-aikaisen informaation tarjoamista kaupungissa ja tapahtumissa käyville. Esimerkkinä sensoritekniikan hyödyntämisestä on mm. odottamattoman voimakkaan tuulen aiheuttamista vaaratilanteista saatavat ennakkovaroitukset yleisötelttoja ajatellen.

Hyvinvoinnin ja yhdenvertaisuuden edistäminen on turvallisuuden edistämistä. Sisäministeriön turvallisuussuunnittelukonseptin mukaan hyvinvointi- ja terveystyö on kuntasektorin perustyötä, joka vaikuttaa turvallisuuden juurisyihin. Turvallisuussuunnittelulla pyritään ennaltaehkäisyyn, ja turvallisuuspalveluilla hoidetaan arjen rikokset, häiriöt ja onnettomuudet.

Varautumisen avulla etsitään keinoja selvitä epätavallisista ja/tai laajoista häiriötilanteista ja valmistaudutaan niistä palautumiseen.

Pirkanmaan turvallisuusklusteri tai -ekosysteemi on laajentanut turvallisuustoimijoiden joukkoa alueellisella tasolla perinteisestä viranomaisperustaisesta näkökulmasta erityisesti yrityksiin. Pirkanmaalla viranomaisten ja turvallisuuden vapaaehtoistoimijoiden, kuten järjestöjen ja yhdistysten välinen yhteistyö on ollut jo perinteisesti vahvaa.

Drone-turvallisuus yleisötapahtumissa (tutkijatohtori *Taneli Riihonen*, Tampereen yliopisto/sähkötekniikka)

Drone voidaan suomentaa esimerkiksi lennokkikopteriksi, kameralennokiksi, minikopteriksi tahi kuvauskopteriksi tai -lennokiksi.

Drone-turvallisuuden keskiössä on luvattomien dronejen havaitseminen ja torjuminen. Havaitseminen voidaan tehdä esimerkiksi radiosignaalien seurannan tai tutkan avulla. Torjunnassa voidaan käyttää esimerkiksi ohjaus- tai GPS-signaalin häirintää, mutta käytännössä jopa viranomaisilla on vielä melko vähän keinoja dronejen konkreettiseen torjumiseen. Drone-turvallisuuden tietopaketti on URL-osoitteessa http://drone-turvallisuus.fi/

Vuonna 2017 Lahdessa järjestetyissä hiihdon maailmanmestaruuskilpailuissa käytettiin luvatomasti dronea kilpailualueen päällä 300 m:n korkeuteen yltäneellä lentokieltoalueella. Kyseessä oli ilmailurikkomus, vaikka drone ei tiettävästi aiheuttanut vaaratilannetta yleisölle. Sen sijaan saman vuoden toukokuussa järjestetyissä presidentti Mauno Koiviston hautajaisissa käytetty luvaton drone aiheutti vaaratilanteen. Terrorismin välineenä räjähteellä varustettua dronea käytettiin elokuussa 2018 Venezuelan presidentti Nicolás Maduroa vastaan suunnatussa iskussa. On odotettavissa, että dronen käyttö terroristi-iskuissa yleistyy.

Dronejen käytön riskit, uhat ja haita yleisötapahtumissa ovat:
- yleisön ja esiintyjien henki ja terveystyöaineelliset vahingot
- tapahtumanjärjestelmän toiminnan häiritseminen
- tekijänoikeuskysymykset
- uusia asia huomioitavaksi turvallisuussuunnittelussa.

Droneista voi olla myös hyötyä tapahtumissa:
- tapahtuman luvallinen taltiointi
- työkalu turvallisuusorganisaatiolle
- show-elementti esityksessä esimerkiksi korvikkeena palo-, kemikaali- ja muita riskejä sisältävälle ilotulitukselle
- kokonaan uudet tapahtumat (FPV Drone Racing jne.)
- mahdolliset yleisölennätykset tulevaisuudessa.

Riskien vähentämiseksi dronejen luvaton käyttö yleisötapahtumissa tulisi kieltää. Ongelmaa ei saada ratkaistua pelkästään normiohjauksella, vaan tarvitaan myös lisää informaation jakamista.

Tilannekuvajärjestelmä tapahtumaturvallisuudessa (senior consultant *Sari Mäenpää*, Insta Group Oy/InstaDefSec Oy)

Insta Group -konserni on Puolustusvoimien strateginen kumppani. Yritys on vuonna 1960 perustettu perheyritys. Työntekijöitä on yli 1 000, ja rekrytointi on parhaillaan käynnissä. Liikevaihto vuonna 2018 oli noin 125 miljoonaa euroa. Noin puolet liikevaihdosta tulee älykkäästä teollisuudesta, puolustusteollisuudesta noin 20 % ja kansallisesta turvallisuudesta noin 20 %. Insta Group -konserni koostuu siviiliturvallisuuden Response-, puolustusteollisuuden DefSec-, teollisuusautomaatio Automation- ja digitalisaation Intopalo Digital -yhtiöistä.

Tapahtumaturvallisuuden, oli kyseessä sitten viihteellinen tapahtuma tai virallinen tapahtuma, kuten valtiovierailu, toimintaympäristölle ominaista on fyysisen ja digitaalisen ympäristön limittyminen ja informaation runsaus ja pirstaleisuus. Haasteena on tiedon kokoaminen ja tilanneympäristön muodostaminen. Turvallisuudentunne lisää viihtyisyyttä.

Älykäs tilannekuvajärjestelmä yhdistelee, käsittelee ja visualisoi dataa ohjaten ihmisten huomiota asioihin, jotka vaativat toimenpiteitä. Instan tuote vastaamaan haasteeseen on Itilannekuva-alusta IBA (Insta Blue Aware), jota kehitetään osana EU-rahoitteista SURE-projektia. IBA tarjoaa tilannekuvaa, mutta ei kykene sen analysointiin. IBA integroi dataa ja toimijoita, tarjoaa toiminta-alustan uusille palveluntuottajille, tukee operatiivista toimintaa ja toimii simulaatio- ja harjoitusalustana. Käytännössä IBA on kevyt selainpohjainen tilannekuvapalvelu, joka kytkeytyy erilaisiin tietolähteisiin ja esittää tiedot selaimessa samalla karttapohjalla. Päätelaitteena voi toimia esimerkiksi kannettava tietokone, taulutietokone tai älypuhelin.

IBA:lla voidaan jakaa tilannekuvaa tilannekeskuksin ja kentälle. Kyseessä voi olla esimerkiksi vaarallisiin aineisiin liittyvän onnettomuuden hallinta.

Tapahtumaturvallisuuden ja liiketoiminnan on kohdattava. Tilannekuvajärjestelmien painopiste siirtyy kuvailevista toiminnallisuuksista diagnosoiviin, automatisoituihin, ennakoiviin ja autonomisiin.

Crises of the West: Liberal identities and ontological (in)security (prof. *Marko Lehti*, Tampereen yliopisto/Rauhan- ja konfliktintutkimuslaitos)

Vakavin uhka liberaalille järjestelmälle on mm. EU:n perustana olevien perinteisten arvojen heikkeneminen, jopa romahtaminen. Liberaalinen järjestelmä on perinteisesti nähty kategorisena Yhdysvaltain johtamana monoliittisena hegemoniana ja sen pyrkimykset sen muuttamiseen uhkana. Vaihtoehtoinen gramscilainen näkemys pitää liberalismia johtavana periaatteena ja legitimoivana narratiivina, joka kuitenkin muuttuu ja kehittyy yhteiskunnallisen keskustelun seurauksena.

Liberaalin järjestelmän menestyksen taustalla on usko demokratiaan, ihmisoikeuksiin ja markkinatalouteen. Näiden länsimaisesta kulttuuriperinnöstä nousevien arvojen on katsottu oikeuttavan erilaiset interventiot humanitaarisuuden, demokratian, modernisoinnin ja si-

vistyksen nimissä. Pahimmillaan erityisesti 1800-luvulla se johti kolonialismiin ja imperialismiin.

Turvallisuus edellyttää kykyä pitää vahvaa narratiivia, jonka pohjalta kollektiivinen itsetunto rakentuu. Tällöin siitä poikkeaminen siitä näyttäytyy uhkana. (Giddens 1991).

Keskeisiä kysymyksiä ovat, (1) kykeneekö liberaali järjestelmä uudistamaan itseään, (2) miten se näyttäytyy länsimaisen kulttuuripiirin ulkopuolella ja (3) onko sille vaihtoehtoja ylläpitämään maailmanrauhaa.

Order – What order? The ontology of social order and its implications for the study of world politics (prof. *Tuomas Forsberg*, Tampereen yliopisto/kansainvälinen politiikka)

Kysymys liberaalista järjestelmästä on haastava. Järjestelmä nähdään määritelmällisesti myönteisenä asiaintilana, esimerkiksi anarkian vaihtoehtona. Vähimmillään järjestelmän tarkoitus on ehkäistä sotia ja muuta väkivaltaa sekä tarjota luottamus sopimiselle *pacta sunt servanda* -periaatteen kautta.

Kansainvälisen järjestelmän kehitys voidaan nähdä joko syklisenä vallanjakomallina tai lineaarisena liberalismin kehityksen mallina. Mallit ovat pitkälti vastakohtaiset toisiinsa nähden. Historiatieteeseen nojaavat selitysmallit eivät toistaiseksi tarjoa tukea näille yleistyksille, ja nähtyjen kehityskulkujen syiksi on esitetty milloin globaalia talouskriisiä, milloin älykkyyden tai empatian rappeutumista. Näkyvissä olevia oireita on vaikea erottaa taustalla olevia juurisyistä.

Liberaalin järjestelmän mahdollisia kehityskulkuja ja niihin vaikuttavia tekijöitä voidan kuvata seuraavasti:

	Liberaali järjestelmä loppuu	Liberaali järjestelmä säilyy
Materiaaliset tekijät	Ei-liberaalien suurvaltojen, kuten Kiinan kansantasavallan nousu. Teknologian mahdollistama valtiollinen diktatuuri.	Yhdysvallat säilyttää hegemonisen asemansa. Liberaali järjestys hyödyttää kaikkia ja varallisuus luo vapautta.
Ajatukselliset tekijät	Nationalismin ja/tai heimoajattelun nousu. Legitimaation puute.	Älykkyyden kasvu. Kollektiivinen identiteetti.

Feminist Perspectives on Safety and Security (apulaisprof. *Catia Confortini*, Wellsley College, MA, USA/rauhan ja oikeuden tutkimus)

Feminismi aatteena jakautuu useaan osa-alueeseen. Yhteistä useimmille näistä on se, että tarkastelun kohteena ovat erilaiset valtarakenteet, jotka vaikuttavat ihmisten välisiin suhteisiin. Feminististä käsitystä turvallisuudessa sen sekä safety- että security-merkityk-

sessä on vaikea määritellä, koska kokemuksen turvallisuudesta nähdään olevan yksilökohtaista.

Feministinen ajattelutapa pyrkii kehittämään kokonaisturvallisuutta kiinnittämällä huomiota marginaalissa eläviin, ihmisten ruumiillistamiseen ja arkielämässä erilaisin perustein, myös muin kuin sukupuoleen liittyvin, tapahtuvaan toiseuttamiseen, mitä kutsutaan intersektionaaliseksi lähestymistavaksi. Toiseuttamisen taustalla voi olla mm. henkilön kansallisuus, ikä, yhteiskuntakerrostuma tai ihonväri.

Intersektionaalisuuden yhtenä saavutuksena pidetään YK:n vuonna 2017 hyväksyttyä ydinasekieltosopimusta, jonka takana olivat mm. useiden alkuperäiskansojen huonot kokemukset menneiden vuosikymmenten aikana tehdyistä ydinkokeista heidän asuinalueillaan.

Yhteiskunnan kokonaisturvallisuutta edistetään tehokkaimmin yhteisöllisyyden ja ihmisten välisten tasa-arvoisten ja yhdenvertaisten vuorovaikutussuhteiden vahvistamisella.

Muistion vakuudeksi Tampereella 10.10.2019

Juuso Hyvärinen
Vapepan Etelä-Pirkanmaan paikallistoimikunta