ESPOO 2006 VTT TIEDOTTEITA 2327

Security-tutkimuksen roadmap

VTT TIEDOTTEITA – RESEARCH NOTES 2327

Security-tutkimuksen roadmap

Toimittajat
Mika Naumanen & Veikko Rouhiainen

ISBN 951–38–6769–2 (nid.)
ISSN 1235–0605 (nid.)

ISBN 951–38–6770–6 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 3, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 3, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

VTT, Vuorimiehentie 3, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 7090

VTT, Bergsmansvägen 3, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 7090

VTT Technical Research Centre of Finland, Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 7090

VTT, Tekniikankatu 1, PL 1300, 33101 TAMPERE
puh. vaihde 020 722 111, faksi 020 722 3499

VTT, Tekniikankatu 1, PB 1300, 33101 TAMMERFORS
tel. växel 020 722 111, fax 020 722 3499

VTT Technical Research Centre of Finland,
Tekniikankatu 1, P.O. Box 1300, FI-33101 TAMPERE, Finland
phone internat. +358 20 722 111, fax +358 20 722 3499

Kansikuva: Wikipedia, Andreas Tille

Toimitus Leena Ukskoski

Otamedia Oy, Espoo 2006

Security-tutkimuksen roadmap [Technology roadmap of security research]. Mika Naumanen & Veikko Rouhiainen (toim.). Espoo 2006. VTT Tiedotteita – Research Notes 2327. 69 s.

Avainsanat energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks

Tiivistelmä

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaaminen on noussut Euroopassa merkittäväksi haasteeksi. EU:n seuraavaan puiteohjelmaan on tulossa aihealue ”Space and security”, jonka laajuus tulee olemaan hyvin merkittävä. Aihealueen perusteluissa todetaan, että ”teknologia ei voi taata turvallisuutta, mutta turvallisuutta ei voida saavuttaa ilman teknologian tukea”. Edelleen perusteluissa korostetaan sitä, että turvallisuus- ja puolustustutkimus lähestyvät yhä enemmän toisiaan. Näin vanha erottelu siviili- ja sotilastutkimukseen on pienenemässä, koska on todettu, että molemmat hyödyntävät samaa osaamista.

Suomessa on jo nyt merkittävää turvallisuuteen liittyvää yritystoimintaa. Osa yrityksistä toimii pelkästään Suomessa, mutta jotkut ovat alallaan kansainvälisesti johtavia. Turvallisuusalan merkitys on kasvamassa. Tutkimuksen kautta voidaan löytää merkittäviä kasvumahdollisuuksia myös uusille liiketoiminnoille.

VTT:llä on käynnissä turvallisuustutkimusta kaikissa nykyisissä osaamiskeskittymissä ja klustereissa. Valtaosa tutkimuksesta kohdistuu yleiseen turvallisuuteen, mutta VTT osallistuu myös useisiin puolustusvälineteollisuutta tukeviin hankkeisiin.

Osaamistensa ja tutkimustarpeiden tarkemmaksi määrittämiseksi VTT:ssä laadittiin vuonna 2005 laajan tutkijajoukon yhteistyönä VTT:n Security-tutkimuksen roadmap. Siinä turvallisuuden kannalta erityisen tärkeiksi nousi kolme aihealuetta. Yhteiskunnan järjestelmien turvaamisessa korostuvat energiaverkostot, tietoliikenneverkot, vesihuolto, liikenne ja kuljetukset sekä ihmisten suojaaminen. Elinkeinoelämän turvallisuuden varmistamisessa tärkeiksi aihealueiksi nousivat tuotannon ja palvelutoiminnan turvallisuus, kiinteistö ja toimitilaturvallisuus sekä sulautettujen järjestelmien tietoturva. Keskeisinä tarvittavina osaamisina ja teknologioina nousivat esiin kokonaisturvallisuuden hallinta, ilmaisu, tunnistus, paikannus ja tiedonsiirto, tietoverkkojen ja järjestelmien suojaus sekä fyysinen suojaus.

Tämä julkaisu tarkastelee yksityiskohtaisesti security-aihealueen osaamis- ja kehitystarpeita sekä tulevaisuuden kehitysnäkymiä.

Security-tutkimuksen roadmap [Technology roadmap of security research]. Mika Naumanen & Veikko Rouhiainen (eds.). Espoo 2006. VTT Tiedotteita – Research Notes 2327. 69 p.

Keywords energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks

Abstract

Requirements for increasing security have arisen in Europe after highly visible and tragic events in Madrid and in London. While responsibility for security rests largely with the national activities, the EU has also started planning a research area "Space and security" as a part of the 7th Framework Programme. As the justification for this research area it has been presented that "Technology alone can not assure security, but security can not be assured without the support of technology." Furthermore, the justification highlights that security and military research are becoming ever closer. The old separation between civil and military research is decreasing, because it has been noticed that both areas are nowadays utilising the same knowledge.

In Finland, there is already now noteworthy entrepreneurship related to security. Although some of the companies are currently only operating in Finland, others are already international leaders in their area. The importance of the security area is increasing and remarkable potential for new growth business areas can already be identified. This however also requires an increase in research efforts.

VTT has a broad range of security research ongoing in many technology areas. The main areas have been concentrating on public safety and security, but VTT is participating also in several research projects related to the defence technology.

For identifying and defining in more detail the expertise and research goals, the Security research roadmap was developed. The roadmap identified three particularly significant areas related to security. The assurance of critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport, and obviously also the citizens. For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for embedded systems. The most important security products and technologies needed are, for example, management of total security, detection, identification, localisation and communication, protection of information networks and systems, and physical protection.

This report presents in more detail the knowledge and development needs as well as future development potentials seen in the security area.

Alkusanat

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaamista turvaavan EU:n Security-hankkeen perusteluissa todetaan, että ”teknologia ei voi taata turvallisuutta mutta turvallisuutta ei voida saavuttaa ilman teknologian tukea”. VTT:llä onkin käynnissä turvallisuustutkimusta kaikissa osaamiskeskittymissään ja klustereissaan. Alueella on suuri tutkimuspotentiaali. Turvallisuuden parantamiseen tähtäävien tuotteiden ja järjestelmien kehittäminen on vasta käynnistynyt. Innovaatioille on vielä tilaa.

Tuotteiden ja järjestelmien parantaminen edellyttää kuitenkin teknologioiden kehittämistä ja yhdistämistä sekä laaja-alaista soveltamista. Tämä Security-tutkimuksen roadmap on syntynyt tästä lähtökohdasta. Roadmap keskittyy erityisesti seuraaviin panostusalueisiin: yhteiskunnan järjestelmien turvaaminen, elinkeinoelämän turvallisuuden varmistaminen sekä turvateollisuuden teknologiat ja palvelut. Julkaisussa tunnistetaan yhteiskunnan ja elinkeinoelämän lähivuosien kehitysnäkymistä lähtien VTT:n ja EU:n Security-tutkimuksen kannalta keskeiset VTT:n osaamisalueet ja niiden antamat mahdollisuudet sekä tehdään suunnitelmat uuden osaamisen kehittämiseksi. VTT:n osaaminen turvallisuutta edistävien kriittisten teknologioiden alueella on hyvä, mihin pohjautuen VTT:n tulee pyrkiä ottamaan vetovastuu suurista turvallisuusalan hankkeista Suomessa. VTT:llä on hyvät mahdollisuudet entisestään laajentaa osallistumistaan kansainvälisiin verkostoihin ja teollisuuden kehitystyöhön security-tutkimusalueella.

Ajankohtaisen lisämausteensa yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaamiseen antaa hirmumyrsky Katrina: Siitä huolimatta, että julkisessa strategiassa korostettiin ennakoitavuutta, ei ennakoitavankaan riskin pienentämiseen oltu valmiita panostamaan. Taloudellinen riskinhallinnan optimointi oli puutteellinen. Patojen rakentaminen katsottiin liian kalliiksi, vaikka laiminlyönnistä aiheutuneet kustannukset olivat suuruusluokaltaan valtavat ja riskin toteutumisen todennäköisyys kohtuullisen korkea. Louisianassa verkostoituminen paikallisviranomaisten, liittovaltion viranomaisten ja elinkeinoelämän kanssa ei myöskään toiminut. Kaikki siirsivät vastuuta toisilleen. Tapauksesta on opittavana verkostoitumisen tärkeys siten, että kukin vastuunalainen ja osaava taho on mukana omalla ydinosaamisalueellaan. Tämä pätee tietysti myös jo teknologiaa kehitettäessä ja markkinoitaessa.

Security-tutkimuksen roadmap on osa VTT:n sisäistä ”Yhteiskunnan turvallisuuden varmistaminen tutkimuksen ja teknologian avulla” -strategisen hankealueen työtä. Hankkeen johdossa on toiminut Veikko Rouhiainen ja sihteerinä Marinka Lanne. Roadmapin laatimiseen on osallistunut lukuisa joukko VTT:n asiantuntijoita. Heitä ovat olleet ainakin Pasi Ahonen, Heikki Ailisto, Osmo Auvinen, Seppo Enbom, Jarkko Holappa, Henrik Huovila, Markku Jenu, Arto Juhola, Veli-Pekka Kallberg, Matti Kokkala, Veikko Komppa, Juhani Korkealaakso, Kirsi Kujanpää, Ilpo Kulmala, Marinka Lanne,

Veijo Lappalainen, Auli Lastunen, Hannu Maula, Hanna Miettinen, Päivi Mikkonen, Aarne Oja, Antti Permala, Juuso Pesola, Outi Priha, Laura Raaska, Veikko Rouhiainen, Ismo Ruohomäki, Jukka Räsänen, Anni Sademies, Reijo Savola, Kristiina Takkinen, Teuvo Uusitalo, Jouko Viitanen, Matti Vuorio ja Gun Wirtanen.

Tämä julkaisu vetää yhteen VTT:n roadmap-hankkeen tulokset. Sen ovat toimittaneet ja koonneet yhteen Mika Naumanen ja Veikko Rouhiainen.

Sisällysluettelo

Tiivistelmä 3

Abstract 4

Alkusanat 5

1. Johdanto 9

2. Security tutkimusalueena 12
   - 2.1 Taustaa 12
   - 2.2 Turvallisuuden varmistamisen hyödyt 15
   - 2.3 Uudet tuotteet ja palvelut 17
   - 2.4 Turvateollisuuden teknologiat ja palvelut 18
     - 2.4.1 Teknologiat sovelluskohteissa 18
     - 2.4.2 Kokonaisturvallisuuden hallinta 21
     - 2.4.3 Ilmaisu, tunnistus, paikannus ja tiedonsiirto 22
     - 2.4.4 Tietoverkkojen ja -järjestelmien suojaus 26
     - 2.4.5 Fyysinen suojaus 29

3. Yhteiskunnan järjestelmien turvaaminen 31
   - 3.1 Energiaverkostot 31
     - 3.1.1 Teknologiaperusta 31
     - 3.1.2 VTT:n toiminta 32
   - 3.2 Tietoliikenneverkot 33
     - 3.2.1 VTT:n toiminta 36
   - 3.3 Vesihuolto 37
     - 3.3.1 Teknologiaperusta 38
     - 3.3.2 VTT:n toiminta 39
   - 3.4 Liikenne ja kuljetukset 40
     - 3.4.1 Teknologiaperusta 41
     - 3.4.2 VTT:n toiminta 43
   - 3.5 Ihmisten suojaaminen terrori-iskujen seurauksilta 44
     - 3.5.1 Teknologiaperusta 45
     - 3.5.2 VTT:n toiminta 46

4. Elinkeinoelämän turvallisuuden varmistaminen 49
   - 4.1 Tuotannon ja palvelutoiminnan turvallisuus 49
     - 4.1.1 Teknologiaperusta 50
     - 4.1.2 VTT:n toiminta 52

4.2 Kiinteistö- ja toimitilaturvallisuus 56
4.2.1 Teknologiaperusta 57
4.2.2 VTT:n toiminta 59
4.3 Tuotteiden ja järjestelmien tietoturva 62
4.3.1 Teknologiaperusta 62
4.3.2 VTT:n toiminta 64

5. Yhteenveto 65

1. Johdanto

Turvallisuuden parantamiseen tähtäävien tuotteiden ja järjestelmien kehittäminen on lisääntynyt voimakkaasti parin viime vuoden aikana. Näitä, osin tulevaisuuden, tuotteita ja palveluja tarkastellaan tässä julkaisussa yhteiskunnan järjestelmien turvaamisen ja elinkeinoelämän turvallisuuden varmistamisen näkökulmista. Mahdollisia turvateollisuuden teknologioita tarkastellaan sovellusalueiden kautta. Pääpaino on kehitysmahdollisuuksien ja saavutettavissa olevien hyötyjen kuvaamisessa.

Suomenkielen käsite turvallisuus, kattaa englanninkielen käsitteet ”safety” ja ”security”. Käsitteitä ei tässä pyritä määrittelemään tarkasti. Yleisesti voidaan todeta, että safety-käsite liittyy tahattomiin onnettomuuksiin, tapaturmiin ja menetyksiin. Security-käsite vastaavasti liittyy tahalliseen vahingontekoon, rikollisuuteen ja terrorismiin. Tässä julkaisussa turvallisuudella tarkoitetaan lähinnä security-aihealuetta.

Yhteiskunnan järjestelmien turvallisuuden kannalta tarkasteltaviksi keskeisiksi sovelluskohteiksi on tunnistettu energiaverkot, tietoliikenneverkot, vesihuolto, liikenne ja kuljetukset sekä ihmisten suojaaminen. Yhteenveto näihin liittyvistä tavoitteista, visioista sekä kehitysmahdollisuuksista on taulukossa 1.

Elinkeinoelämän turvallisuuden varmistamiseen liittyviksi tarkasteltaviksi sovelluskohteiksi on tunnistettu tuotannon ja palvelutoiminnan turvallisuus, kiinteistö- ja toimitilaturvallisuus sekä tuotteiden ja järjestelmien tietoturva. Yhteenveto näihin liittyvistä tavoitteista, visioista sekä kehitysmahdollisuuksista on taulukossa 2. Tämän raportin tarkoitus on tarkastella tietoturvatutkimusta yleisen turvallisuuden näkökulmasta, ja ei näin ollen sisällä kaikkia tietoturvatutkimuksen aihepiirejä.

Yleisesti lyhyen tähtäimen tavoitteena on analysointi ja olemassa olevien teknologioiden soveltaminen security-tutkimusalueelle. Keskipitkällä ajanjaksolla tavoitellaan päätöksenteon tukijärjestelmiä ja pyritään saamaan security osaksi laajempaa järjestelmää. Pitkällä ajanjaksolla tavoitteena ovat älykkäät ja varmatoimiset security-järjestelmät.

Turvallisuutta takaavia geneerisiä teknologioita ovat esimerkiksi kokonaisturvallisuuden hallinnan, hälytys- ja monitorointijärjestelmien ja tietoturvan teknologiat. Kokonaisturvallisuuden hallinnassa ja johtamisessa korostuvat riskien analysointi, arviointi ja hallinta, turvallisuustiedon hallinta sekä eri toimijoiden yhteistyö sekä turvallisuusjohtamisen menetelmät ja mallit. Riskin muuttaminen liiketoimintamittareilla mitattavaksi (due diligence) on yhä tarpeellisempaa. Tunnistuksessa kehityksen odotetaan etenevän kemiallisten tekijöiden detektiosta (vaikuttimien selvittämisestä) biologisten tekijöiden havainnointiin ja tunnistukseen, analyysijärjestelmien kehittämiseen ja siitä edelleen detektion soveltaminen käytäntöön. Anturiteknologian, määritysmenetelmien ja tiedonsiirron on oltava nopeaa. Tietoturvassa korostuvat usealla sovellusalueella tietoturvamonitorointi sekä tietoverkkojen ja -järjestelmien suojaus.

Tietoturvan hallinnassa on tärkeää tietoturvariskien, -uhkien ja haavoittuvuuksien ymmärtäminen yritysten liiketoiminnassa, sen tuotteissa ja palveluissa. Haasteita tietoturvatyöhön luo erityisesti tietoverkkojen, laitteiden ja palveluiden tasolla tapahtuva digitaalinen konvergenssi. Konvergenssikehitys aiheuttaa myös yleisen turvallisuuden kannalta uhkaa, kun kriittisten perusrakenteiden ohjausjärjestelmiin rakennetaan rajapintoja avoimiin verkkoihin. Turvallisuuden kannalta on tärkeää, että pystytään kehittämään proaktiivisia monitorointi- ja suojausmenetelmiä reaktiivisten sijaan.

Taulukko 1. Yhteiskunnan järjestelmien turvallisuuden varmistamisen tavoitteet valituissa sovelluskohteissa lyhyellä (alle 5 v.) ja keskipitkällä–pitkällä (10 v.) aikavälillä.

Toiminnallisuus	**Tavoitteet & visio (lyhyt)**	**(keskipitkä–pitkä)**
Energia-verkostot	Analysoida verkostoihin kohdistuvia uhkia sekä mahdollisuuksia parantaa turvallisuutta tämän päivän teknologioilla.	Kehittää tarvittavia teknologioita suojaamaan verkostoja odotettavissa olevia uhkia vastaan sekä parantaa verkostojen omistajien ja käyttäjien turvallisuusajattelua.
Tietoliikenne-verkot	Palvelujen toimivuuden ja saatavuuden varmistaminen, ts. tietoturvallinen palvelu on saatavissa, kun sitä tarvitaan, ja se myös toimii. Tietoturvatavoitteiden määrittely ja arvoverkkoanalyysi mobiilipalveluissa.	Varsinaiset ja kattavat tietoliikenteen perustietoturvapalvelut. Proaktiivnen ja läpinäkyvä tietoturva. Älykäs tietoturvamonitorointi.
Vesihuolto	Analysoida vesihuollon kriittiset kohdat ja niihin liittyvät riskit ja uhat sekä mahdollisuudet parantaa turvallisuutta uusilla monitorointi-, mittaus- ja analysointitekniikoilla.	Kehittää tarvittavia teknologioita juomavesiverkoston kriittisten pisteiden suojaamiseksi niihin kohdistuvia uhkia vastaan ja tarvittavan päätöksenteon tukemiseksi. Kehittää vesihuollon käytettävyyttä ja vikasietoisuutta kaikissa oloissa.
Kuljetukset	Liikenteen ja logistiikan security-alueen määrittely. Riskien tunnistamismenetelmien ja arviointimallien kehittäminen. Security-ajattelun liittäminen tutkimusmenetelmiin.	Riskienhallinnan mallien soveltaminen. Varmistaa liikenne- ja logistiikkaverkostojen käytettävyys, toimivuus ja turvallisuus.
Ihmisten suojaaminen	Uhkakuvien riskinarvioinnin työstäminen. Kemiallisten ja biologisten agenssien detektiomenetelmien kartoittaminen. Pelastusjoukkojen suojautumisen yhtenäistäminen, nopeasti pystytettävien suoja- ja sisätilojen dekontaminaatioratkaisujen kehittäminen.	Mikrobiologisen riskinarviointiosaamisen ja -mallien hyödyntäminen, biologisten agenssien detektiomenetelmien soveltaminen. Ilmanäytteiden luotettavan määrityskonseptin luominen sekä CBR-aineiden hallinta (suodatus, suojaus, dekontaminaatio).

Turvallisuuden parantamiseen tähtäävät tuotteet ja järjestelmät tuottavat monia taloudellisesti merkittäviä hyötyjä. Nämä liittyvät kriittisten kohteiden varmistamiseen ja esimerkiksi tuotantokatkosten estymiseen. Luotettavuus ja saatavuus edistävät käytettävyyttä. Esimerkiksi vesihuolto liittyy moneen muuhun järjestelmään. Samoin kuljetuksien (elintarvikkeiden, polttoaineen, sähkön jne.) turvaaminen palvelee yhteiskunnalle kriittisten toimintojen ylläpitoa. Ihmisten suojaamiseen kehitettävät ratkaisut voivat parantaa sisäilmanlaatua yleisestikin.

Taulukko 2. Elinkeinoelämän turvallisuuden varmistamisen tavoitteet valituissa sovelluskohteissa lyhyellä (alle 5 v.) ja keskipitkällä–pitkällä (10 v.) aikavälillä.

Toiminnallisuus	**Tavoitteet ja visio (lyhyt)**	**(keskipitkä–pitkä)**
Tuotannon ja toiminnan turvallisuus	Security-näkökulman integroiminen haavoittuvuusanalyyseihin, HACCP-vaara-analyyseihin sekä muihin riskianalyysivälineisiin. Riskianalyysi- ja riskienhallintamenetelmien tietoteknisten työvälineiden kehittäminen ja soveltaminen security-alueelle. Turvallisuuden mittarien ja riski-indikaattoreiden kehittäminen. Tietoturvariskien hallinnan menetelmien kehittäminen.	Security-riskienhallinnan liittäminen osaksi yritysten johtamista. Turvallisuusjohtamisen ja riskienhallinnan integrointi tuotannon elinkaaren eri vaiheisiin sekä selkeämmin osaksi yritystoimintaa. Tietoturvajohtamisen menettelytavat (arviointi, suunnittelu, toteutus, seuranta).
Kiinteistö- ja toimitila-turvallisuus	Toimitilojen riskianalyysit, referenssirakennusten riskianalyysit. Toimitilojen riskien hallintamenetelmien kehittäminen: automaatio-, hälytys- ja valvontajärjestelmien IP-verkkojen käyttöön liittyvät tietoturvariskit selvitetty. Pelastusajoneuvoon raportoiva kiinteistö (PARK)-järjestelmä.	Riskikäyttäytymisen tunnistaminen, ennaltaehkäisy ja hallinta. RF-anturiverkkoja hyödyntävät hälytysjärjestelmät. Automaatio-, hälytys ja valvontajärjestelmien IP-verkkojen käyttöön liittyvät turvalliset tietoturvaratkaisut. Kiinteistön turvallisuusjohtamisen informaatiojärjestelmä.
Tuotteiden ja järjestelmien tietoturva	Mobiililaitteiden ja sulautettujen järjestelmien state-of-the-art-tietoturvateknologian hallitseminen. Digi-TV:n sovellusalustan ja IP-pohjaisen paluukanavan tietoturva-analyysi. Sisällönsuojaus (DRM) -menetelmien hallinta ja soveltaminen.	Uusien tietoturva-arkkitehtuuriratkaisujen kehittäminen mobiililaitteisiin ja sulautettuihin järjestelmiin. Tietoturvan hallinta päätelaitteessa (mm. massamuistin ja paluukanavan suojaaminen). Sisällönsuojausmenetelmien testaus, menetelmäkehitys.

2. Security tutkimusalueena

Luvussa esitellään, mitä tutkimus- ja kehitysmahdollisuuksia security voisi teknologisista lähtökohdista käsin tarkasteltuna tarjota. Kohta Security tutkimusalueena (1.1) esittelee raportin lähtökohtia ja valittua security-näkökulmaa. Kohdat 2.2 ja 2.3 tarkastelevat turvallisuuden varmistamisen tarjoamia hyötyjä (2.2) sekä uusia tuotteita ja palveluja (2.3). Sekä hyötyjä että uusia tuotteita ja palveluja pohditaan raportin kahden keskeisen näkökulman kautta: miten ne turvaavat toisaalta yhteiskunnan järjestelmiä ja toisaalta varmistavat elinkeinoelämän turvallisuutta. Eri turvateollisuuden teknologioita, niiden mahdollistamia palveluja ja yhteyttä eri sovellusalueille esitellään kohdassa Turvateollisuuden teknologiat ja palvelut (2.4).

2.1 Taustaa

Lähtökohta

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaaminen on noussut Euroopassa merkittäväksi haasteeksi. EU:n toimesta aloitettaneen vuoden 2007 alusta Security-ohjelma, jonka vuotuiseksi rahoitukseksi on esitetty miljardi euroa. Ohjelman perusteluissa todetaan, että ”teknologia ei voi taata turvallisuutta, mutta turvallisuutta ei voida saavuttaa ilman teknologian tukea”. Edelleen perusteluissa korostetaan sitä, että turvallisuus- ja puolustustutkimus lähestyvät yhä enemmän toisiaan. Täten vanha erottelu siviili- ja sotilastutkimukseen on pienenemässä, koska on todettu, että molemmat hyödyntävät samaa osaamista. Tätä on korostettu myös Suomessa Puolustusvoimien vuonna 2005 käynnistyneissä teknologiahankkeissa.

Koska Security-tutkimus tulee olemaan laajuudeltaan hyvin merkittävä, on EU käynnistänyt valmistelevan hankkeen, jonka ensimmäiset projektit alkoivat vuoden 2004 aikana. Niiden tavoitteena on avustaa Komissiota suuntaamaan Security-tutkimusta. Tähän liittyen VTT on, yhdessä yritysten ja muiden tutkimusorganisaatioiden kanssa, mukana IMPACT- ja SeNTRE-hankkeissa. SeNTRE on verkostohanke, jonka työhön osallistumalla VTT:n asiantuntijat pääsevät vaikuttamaan tulevan EU:n Security-ohjelman suuntaamiseen ja samalla voivat muodostaa tarvittavia verkostoja.

VTT:n security roadmap

VTT:llä on monialaisena, luottamukselliseen ja puolueettomaan tutkimukseen erikoistuneena tutkimuslaitoksena hyvät mahdollisuudet ja resurssit ottaa vetovastuu suurista turvallisuusalan hankkeista. VTT:llä on myös yhteistyöverkostot, mm. EUROTECHin kautta Euroopan parhaisiin osaajiin. Samoin esimerkiksi puolustusvälinetutkimuksen

kautta VTT on luonut toimivat linkit alan teollisuuteen Suomessa. Monipuolinen osaaminen ja verkostot mahdollistavat aktiivisen osallistumisen kansainvälisiin verkostoihin ja teollisuuden kehitystyöhön.

VTT:n Security-tutkimuksen roadmap tarkastelee security-aluetta seuraavilta näkökulmilta (mahdollisilta tutkimus- ja kehitysalueilta):

- yhteiskunnan järjestelmien turvaaminen
- elinkeinoelämän turvallisuuden varmistaminen
- turvateollisuuden teknologiat ja palvelut.

Alueella on suuri tutkimuspotentiaali, koska turvallisuuden parantamiseen tähtäävien tuotteiden ja järjestelmien kehittäminen on vasta käynnistynyt. Uusille innovaatioille on vielä tilaa ja niitä tarvitaan. Tuotteiden ja järjestelmien parantaminen edellyttää teknologioiden kehittämistä ja yhdistämistä sekä laaja-alaista soveltamista. Tavoitteena on luoda uusia tuotteita ja liiketoimintaa. Myös teollisuus, erityisesti puolustusvälineteollisuuden yritykset, suuntaa tulevaa toimintaansa yhä enemmän security-alueelle. Tutkimuksen yhteiskunnallinen vaikuttavuus on suuri.

Security-tutkimussuunnitelman osa-alueet

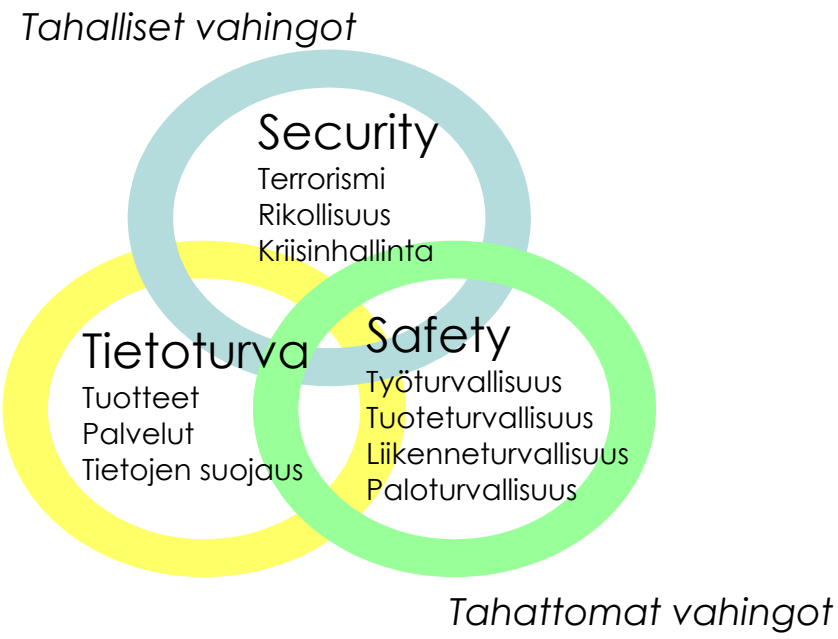
Suomen kielen käsite ”turvallisuus” kattaa englannin kielen käsitteet ”safety” ja ”security”. ”Safety”-käsite liittyy yleensä tahattomiin onnettomuuksiin ja tapaturmiin, jotka viittaavat esimerkiksi työ-, liikenne-, koti-, palo- ja tuoteturvallisuuteen. ”Security”-käsite liittyy yleensä tahalliseen vahingontekoon ja viittaa esimerkiksi rikollisuuteen, terroriin ja yritysturvallisuuteen. Tähän on poikkeuksena muun muassa tietoturvallisuus, jossa tietoturvariskeiksi luetaan sekä tahalliset että tahattomat riskit. On huomattava, että tietoliikenteen ammattikielessä ”security” tarkoittaa lähinnä tietoturvaa. VTT:llä käytetään tietoturvaa kuvaamaan englanninkielistä termiä ”network and information security” sekaannusten välttämiseksi. Tämä nimeämiskäytäntö perustuu Euroopan tietoturvaviraston ENISAn (European Network and Information Security Agency) esimerkkiin.

Juuri ilmestyneessä EU:n CORDIS-julkaisussa *The Foreign Affairs Committee* esittää EU:n Security-ohjelmaan liittyen, että security- ja safety-tutkimusalueiden välille ei pitäisi tehdä mitään eroa. Tähän julkaisuun onkin yritetty hahmottaa kokonaisuuksia, jotka tukevat näitä molempia elementtejä. VTT:n Security roadmap -hankkeessa ei tarkkoihin termimäärittelyihin ole edes pyritty.

Tekesillä on käynnissä ”TURVA 2003 Turvatuotteet, -teknologiat ja -palvelut” -ohjelma. Sen aihealueet ovat:

- älykkäät turvatuotteet ja -järjestelmät seuraaville turvallisuuden osa-alueille: henkilöturvallisuus, omaisuuden turvaaminen, kiinteistö- ja toimitilaturvallisuus sekä tietoturvallisuus
- turvallisuusjohtamisen menetelmät
- turvallisuusalan osaamisintensiivinen palveluliiketoiminta.

Turvallisuus-tutkimusta tehdään kuitenkin monissa muissakin ohjelmissa. Usein turvallisuuden katsotaan olevan niin kiinteä osa tuotteita ja palveluja, että kyseinen tutkimus liittyy siten näiden kehittämiseen. Turvallisuuteen liittyvät asiat ovat varsin horisontaalisia – ne ovat sovellettavissa erityyppisillä vertikaalisilla sovellusalueilla.



Kuva 1. Security-tutkimuksen roadmapissa huomioidut tutkimuksen osa-alueet. VTT:n perinteisesti vahvoja safety-osaamisalueita on käsitelty tässä roadmapissa vain, jos ne tuovat uusia näkökulmia myös Security-tutkimukseen.

Julkaisussa käsiteltäviä osa-alueita on hahmoteltu kuvassa 1. Roadmap kattaa EU:n Security-ohjelman aihepiirin sekä safety- ja tietoturvallisuustutkimuksen (kuten esimerkiksi turvallisuuden johtamisen, ihmisen toiminnan sekä erityisesti tuotteisiin ja palveluihin liittyvän tietoturvan). VTT:n osaaminen perustuu aiempiin tahattomien ja tietoturvallisuuden osalta myös tahallisten riskien tarkasteluihin. Tahattomiin riskeihin tahallisuuden lisääminen on suhteellisen suoraviivaista, joskin yksityiskohdissaan hyvinkin haastavaa. VTT:llä tehdään paljon muutakin turvallisuuteen liittyvää tutkimusta, jota tämä roadmap ei kata, kuten

esimerkiksi ydinturvallisuustutkimusta. Security roadmap -työn yhtenä tavoitteena on myös kehittää yhteistyötä tietoturvatutkimuksen ja muun turvallisuustutkimuksen välillä.

VTT:llä on tietoturvatutkimusta useassa osaamiskeskuksessa. Tietoturvatutkimusta koordinoi horisontaalisesti toimiva tietoturvatutkimuksen koordinointityhmä (NIS). Tietoturvallisuutta käsitellään teknologia-alueena *Tietoverkkojen ja -järjestelmien suojaus*-kappaleessa sekä sovellusalueena mm. *Tuotannon ja toiminnan turvallisuus* (mukana palvelut ja niiden tietoturva) ja *Tuotteiden ja järjestelmien tietoturva -kohdissa*. Tietoturvallisuus on myös sisällä monissa muissa sovellusalueissa.

2.2 Turvallisuuden varmistamisen hyödyt

Kriittisten kohteiden varmistaminen tuottaa taloudellisia hyötyjä esimerkiksi tuotantokatkosten estymisenä. Luotettavuus ja saatavuus edistävät käytettävyyttä. Esimerkiksi vesihuolto liittyy moneen muuhun järjestelmään. Samoin kuljetuksien turvaaminen palvelee yhteiskunnalle kriittisten toimintojen ylläpitoa (elintarvike, polttoaine, sähkö jne.). Ihmisten suojaamiseen kehitettävät ratkaisut voivat parantaa sisäilmanlaatua yleisestikin. Turvallisuuden varmistamisen hyötyjä sovellusalueittain esitetään taulukossa 3.

Taulukko 3. Turvallisuuden varmistamisen hyödyt.

Sovellusalue	Hyöty
Yhteiskunnan järjestelmien turvaaminen	
Energia	Verkkoyhtiöille parantunut tuote (sähkö), imago ja yhteiskuntavastuu, yhteiskunnalle välttämättömän hyödykkeen saatavuuden varmistaminen, yleisen turvallisuuden lisääntyminen (sähköriippuvaiset toiminnot, mm. lukitukset). Keskinäisten riippuvuussuhteiden ymmärtäminen ja analysointi on oleellista. Varajärjestelmän mitoitus. Verkon turvallisuuden optimointi Euroopan kannalta.
Tietoverkot	Tietoturva voidaan tehdä kattavammaksi, varmemmaksi, tehokkaammaksi tai helpommaksi hallinnoida ja käyttää. Parempi tietoturva mahdollistaa edistyneen verkon hallinnan. Pitkällä tähtäimellä voidaan tehdä tietoliikenteen osalta jopa käyttäjille näkymättömäksi. Tietoverkkojen toimintavarmuus paranee. Varajärjestelmien mitoitus ja valinta.
Vesihuolto	Vesihuollon turvallisuus ja käyttövarmuus lisääntyy valuma-alueiden, yhdyskuntien ja teollisuuslaitosten tasolla. Tärkeitä ovat seurausvaikutukset: Yhdyskuntien (asukkaat ja yritykset) ja teollisuuslaitosten turvallisuus ja käyttövarmuus lisääntyvät. Samat menetelmät varoittavat sekä tahallisesta että järjestelmän ikääntymisen tai luonnononnettomuuden aiheuttamista poikkeamista normaalitilanteeseen verrattuna.
Liikenne ja kuljetukset	Riskien ja uhkien karsiminen, parempi logistiikan hallinta. Toimitusvarmuuden parantaminen. Liiketoiminnalle kriittisten toimitusten turvaaminen (arvokuljetukset, elektroniikka yms.). Liikenne- ja kuljetuselinkeinojen toimintaedellytykset. Kuljetusvälineet, kuljetusverkko, verkon käyttötapa, tarkastelu näiden kannalta.
Ihmisten suojaaminen terrori-iskujen seurauksilta	Varhainen varoitusjärjestelmä (biologiset ja kemialliset agenssit), parempi suojavaatetus ja varustus. Nopea reagointi ja hälyttäminen, ennaltaehkäiseminen. Muiden järjestelmien liittymäkohdat terveydenhuollon järjestelmiin, esimerkiksi sairaaloihin. Erityisvaatimukset suojauksessa. Väestösuojarakenteen taloudellinen optimointi. Voidaan estää tilojen saastuminen.
Elinkeinoelämän turvallisuuden varmistaminen	
Tuotannon ja palvelutoiminnan turvallisuus	Kokonaisvaltainen riskienhallinta, synergiaedut ja laajempi näkökulma kehittämisen tueksi, tietoriskien hallinta, riskienhallinnan kohdentaminen kustannustehokkaasti, nopea reagointi uhkatilanteessa. Sähköinen maksuliikenne. Digitaalinen tuotannon ja logistiikan ohjaus. Digitaalisten ja mobiilien palvelujen turvallisuuden varmistaminen. Automaatiojärjestelmien turvallisuuden varmistaminen. Prosessien kehittäminen.
Kiinteistö- ja toimitila-turvallisuus	Yksintyöskentelyn (mm. terveyskeskuksissa, vartioinnissa, teollisuuden valvontatehtävissä) turvallisuus lisääntyy. Korvausvelvollisuudet selkiytyvät, rikosten selvittäminen helpottuu. Ihmisen toimintakyvyn varmentaminen. Henkilökohtaiset turvalaitteet integroitu kiinteistön turvajärjestelmiin.
Tuotteiden ja järjestelmien tietoturva	Tuotteiden tietoturvan hallinta on ehkä suurin ja merkittävin yksittäinen tietoturvan sovellusalue. Laitteiden ja sulautettujen järjestelmien turvallisuus ja käyttövarmuus paranevat.

2.3 Uudet tuotteet ja palvelut

Panostaminen turvallisuuden varmistamiseen synnyttää lukuisan joukon uusia tuotteita ja palveluja. Tällaisia yhteiskunnan järjestelmiä turvaavia tuotteita ja palveluja luetellaan taulukossa 4. Elinkeinoelämän turvallisuuden varmistamiseen liittyviä uusia tuotteita ja palveluja esitetään vastaavasti taulukossa 5.

Taulukko 4. Yhteiskunnan järjestelmien turvaamisen synnyttämiä uusia tuotteita ja palveluja.

Sovellusalue	**Uudet tuotteet ja palvelut**
Energia	• Uudet tuotteet: energiavarastot • Suojatut tietoliikenneratkaisut • Mahdollisesti uudet rakenneratkaisut • Uudet palvelut: häiriön selvitysratkaisut • Mittaustekniikan kehittäminen • Haavoittuvuusanalyysit
Tietoverkot	• Kattavampi, varmempi, tehokkaampi tai helpommin hallinnoitava tietoturva, pitkällä tähtäimellä tietoliikenteen osalta jopa käyttäjille näkymätöntä • Tietoturvan T&K- ja konsulttipalvelut: tavoitteiden määrittely, protokollat, tunnistaminen, kontekstiriippuva tietoturvanhallinta (digitaalinen konvergenssi), arviointi, validointi, integrointi, ”best practices” -sääntöjen ylläpito, organisaatioiden tietoturvanhallinta ja kansainväliset arvoverkostot • Yhteiskunnan palvelutoiminnan tietoturva; hallinnon tietoturva (tiedon saatavuus, säilyvyys, eheys, luottamuksellisuus, kiistämättömyys, todennus) • Terveydenhuollon ja automaatioteollisuuden tietojärjestelmien toimintavarmuus
Vesihuolto	• Monitorointimenetelmät verkostojen laajuiseen kunnonvalvontaan • Veden laadun ja turvallisuuden uudet analysointijärjestelmät • Järjestelmän laajuiset liikkumisen valvontajärjestelmät • Uudet mallinnus-, simulointi- ja visualisointijärjestelmät monitoroinnin tukena • Riskianalyysi-, arviointi- ja hallintamenetelmät ja -työkalut
Liikenne ja kuljetukset	• Kuljetusten seurantajärjestelmät • Henkilöliikenteen turvaaminen (lentoturvallisuus, biometrinen passi) • Securityn hallinta palveluna liikenne ja logistiikka -toimialalla • Security-työkalut liikenne ja logistiikka -toimialalla
Ihmisten suojaaminen terrori-iskujen seurauksilta	• Biodetektioteknologiat, vaarallisten agenssien ilmaisimet • Riskinarviointimenetelmät • Paremmat ja yhteensopivat kemialliset hälytysjärjestelmät • Suojamateriaalit ja -rakenteet • Yhteiskunnan (alueelliset) hälytys- ja varoitusjärjestelmät

Taulukko 5. Elinkeinoelämän järjestelmien turvaamisen synnyttämiä uusia tuotteita ja palveluja.

Sovellusalue	Uudet tuotteet ja palvelut
Tuotannon ja palvelu-toiminnan turvallisuus	• Maksu- ja rahoituspalveluiden tietoturva • Riskianalyysi-, arviointi- ja hallintamenetelmät ja -työkalut • Toiminnan suunnittelukonseptit, johtamis- ja toimintajärjestelmät, taloudellisten vaikutusten arviointi, riskin muuttaminen liiketoimintamittareilla mitattavaksi (due diligence) • Ulkoistamisen ja verkostoitumisen riskien hallinta • Diagnostiikka- ja analysointimenetelmien kehittäminen ja mittarit • Tilannetietoisuus, havainnollistaminen, viestintä • Tietoturvan T&K- ja konsulttipalvelut: tavoitteiden määrittely, protokollat, tunnistaminen, kontekstiriippuva tietoturvanhallinta (digitaalinen konvergenssi), arviointi
Kiinteistö- ja toimitila-turvallisuus	• Suojaamisrakenteet ja -teknologiat, suodattimet • Detektorit ja hälytysjärjestelmät (hälytysajoneuvoon raportoiva järjestelmä) • Riskien hallintakonseptit • Taloudellisten vaikutusten arviointi, riskin muuttaminen liiketoimintamittareilla mitattavaksi (due diligence)
Tuotteiden ja järjestelmien tietoturva	• Päätelaitteiden tietoturvaominaisuuksien kehittäminen • Palveluntarjoajien laitteiden tietoturvaominaisuuksien kehittäminen • Tietoturvatestaus ja -monitorointi • Tietoturvan hallintaprosessi koko tuotteen elinkaaren ajan

Osa edellä kuvatuista tuotteista ja palveluista on toteutettavissa nopealla aikataululla, osa vasta pidemmän ajan kuluttua. Turvallisuuden parantamiseen tähtäävät tuotteet edellyttävät usein teknologioiden yhdistämistä sekä järjestelmien kokoamista. Tämä on hidasta ja aikaa vievää työtä.

2.4 Turvateollisuuden teknologiat ja palvelut

2.4.1 Teknologiat sovelluskohteissa

Roadmapissa tarkasteltavat turvateollisuuden teknologiat on jaettu neljään pääluokkaan. Näitä ovat kokonaisturvallisuuden hallinta; tunnistus, paikannus ja tiedonsiirto; tietoverkkojen ja -järjestelmien suojaus sekä fyysinen suojaus.

Kokonaisturvallisuuden hallinnassa käsitellään riskianalyysimenetelmiin, yleiseen turvallisuuden hallintaan sekä hälytys- ja monitorointijärjestelmiin liittyviä teknologioita. Tunnistus, paikannus ja tiedonsiirto -nimikkeen alla käsitellään laajaa joukkoa teknologioita, esimerkiksi RFID:tä, anturiverkkoja (aktiivitageja), ilmaisuteknologioita, kuten esimerkiksi millimetriaaltokuvannusta, immunologisia tekniikoita sekä hahmontunnistuksen ja biometrisen henkilöntunnistuksen tekniikoita. Tietoverkkojen ja -järjestelmien suojaus käsittää mm. tunkeilunestoon, ohjelmistoalustoihin ja -arkkitehtuureihin, verkko- ja Internet-tietoturvaan sekä tietoturvatestaukseen liittyviä teknologioita. Fyysinen suojaus sisältää sekä rakenteellinen suojauksen että ilman mukana kulkeutuvien CBR-agenssien suojauksen teknologioita.

Taulukossa 6 arvioidaan turvallisuutta parantavien teknologioiden merkittävyyttä eri sovelluskohteiden kannalta. Merkittävyyttä tarkastellaan sekä yleisesti että teknologian kasvupotentiaalin kannalta käyttäen kolmiportaista luokittelua. Asteikko on:

1. ei kovin merkittävä, suhteellisen pieni kasvupotentiaali
2. merkittävä, merkittävä kasvupotentiaali
3. erittäin merkittävä, erittäin merkittävä kasvupotentiaali.

Taulukko 6. Turvateollisuuden teknologiat sovelluskohteittain. Taulukossa on roadmap-työryhmän näkemys sovelluskohteista, joilla tutkimuksella olisi suurimmat kehityspotentiaalit. Kaikissa sovelluskohteissa ei ole merkittävyysarviota, mutta arvion puuttuminen ei osoita kohdealueen merkityksen vähäisyyttä. Merkittävyysarvioiden asteikko on seuraava: 1 – ei kovin merkittävä, 2 – merkittävä, 3 – erittäin merkittävä.

Teknologiat / **Sovellusalueet**	Energiaverkostot	Tietoliikenneverkot	Vesihuolto, kaukolämpö	Liikenne ja kuljetukset	Ihmisten suojaaminen	Tuotannon ja palvelutoiminnan turvallisuus	Kiinteistö- ja toimitilaturvallisuus	Sulautettujen järjestelmien tietoturva
Kokonaisturvallisuuden hallinta								
Riskianalyysimenetelmät	3	1	3	2	2	3	3	1
Tietoturvan hallinta	2	3	1	1		3		3
Hälytysjärjestelmät (+ monitorointi)	1	1	2	1	3	1	2	
Ilmaisu, tunnistus, paikannus ja tiedonsiirto								
RFID				3		3	2	1
Anturiverkot (aktiivitagit)		2	2	3		3	2	
Ilmaisu (detektio)	2		3		3	2	1	
Hahmontunnistus			2	3	3	3	3	1
Biometrinen henkilöntunnistus		3		2	1	3	3	
Tietoverkkojen ja -järjestelmien suojaus								
Tietoverkkojen ja -järjestelmien suojaus	2	3		2	2	3	2	3
Tietoturvamonitorointi	3	3		3		3	2	3
Ohjelmistoalustat ja -arkkitehtuurit		3				3	2	3
Verkko- ja Internet-tietoturva	3	3		2	2	3	2	3
Tietoturvatestaus	2	3		2	1	3	2	3
Fyysinen suojaus								
Rakenteellinen suojaus			1		3	1	3	
Suojaus ilman mukana kulkeutuvilta CBR-agensseilta					3	1	3	

2.4.2 Kokonaisturvallisuuden hallinta

Riskianalyysimenetelmät[1]

Riskianalyysimenetelmillä ymmärretään tässä yhteydessä

- riskianalyysimenetelmien soveltamista ja kehittämistä security-riskien arvioimiseen
- kriittisten suojattavien kohteiden tunnistamista, uhkien tunnistamista (skenaariot)
- haavoittuvuuden analysointia, riskien kvantifiointia, riskienhallintaa
- mikrobiologisia riskinhallintastrategioita teollisuudessa, mikrobiologista kvalitatiivista ja kvantitatiivista riskinarviointia
- teollisuuden omavalvontaa ja HACCP-vaara-analyysejä.

Riskianalyysit luovat pohjan systemaattiselle riskien hallinnalle. Siihen liittyy muun muassa riskien eliminointi, pienentäminen ja tilanteen seuranta. Tähän on kehitetty uusia tekniikoita, kuten esimerkiksi heikkojen signaalien analysoiminen.

Hyödyt ja mahdollisuudet: Uusia riskianalyysimenetelmiin perustuvia tuotteita ja palveluja voivat olla esimerkiksi riski- ja haavoittuvuusanalyysimenetelmät, riskien arviointiin pohjautuvat päätöksentekomallit, riskianalyyseihin liittyvät tietotekniset apuvälineet, mikrobiologiset kvalitatiiviset sekä kvantitatiiviset riskinarviointi- ja hallintamenetelmät ja työkalut.

Yritysten ja organisaatioiden tietoturvanhallinta[2]

Yritysten ja organisaatioiden tietoturvanhallinnalla ymmärretään tässä yhteydessä

- prosesseja, käytäntöjä ja teknisiä ratkaisuja, miten tietoturvaa hallitaan organisaatioissa
- tietoturvanhallintaprosessien ja -käytäntöjen kehittämistä
- tietoturvan hallintaa osana yritysten liiketoimintaprosesseja
- tietoturvan tavoitteiden ja vaatimusten määrittelyä (esimerkiksi Common Criteria-tyyppisellä lähestymistavalla)
- riski-, uhka- ja haavoittuvuusanalyysiä
- jatkuvaa tietoturvan hallintaa yli tarkasteltavan järjestelmän elinkaaren.

[1] Teuvo Uusitalo ja Marinka Lanne, Laura Raaska & Gun Wirtanen kommentoineet
[2] Reijo Savola ja Anni Sademies

Hyödyt ja mahdollisuudet: Yritysten ja organisaatioiden tietoturvanhallintaan perustuvat palvelut voivat olla auditointi- ja määrittelypalveluja sekä ”standardointia”. Tuotteita voivat olla tietoturvamonitorointijärjestelmät, auditointi- ja monitorointimetriikkakehitys, ja riski-, uhka- ja haavoittuvuusanalyysit.

2.4.3 Ilmaisu, tunnistus, paikannus ja tiedonsiirto

RFID (Radio Frequency Identification)[3]

RFID (Radio Frequency Identification) on halpa radioteknologia, jolla voidaan identifioida jokin objekti, tyypillisesti kulutustavara. RFID:n käyttö on lisääntymässä teollisuudessa vaihtoehtona viivakoodille, sillä RFID ei vaadi näköyhteyttä. RFID-lukijassa on antenni ja lähetinvastaanotin sekä objektissa on passiivinen RFID-tunniste, joka ilmoittaa tunniste- ja muut tietonsa lukijalle, kun lukija niitä pyytää.

Esimerkki RFID:n käytöstä on Prosec Tietoturvapalvelun kehittämä RFID-saattomuisteihin perustuva tietojärjestelmä lukittujen keräyssäiliöiden käsittelyn entistä täsmällisemmäksi seuraamiseksi. Jokaisessa turvasäiliössä on yksilöity RFID-tunnistetarra. Tarran avulla kirjataan säiliöiden viennit, tarkastukset ja noudot, rekisteröidään tapahtuma-ajat ja tekijät sekä tunnistetaan säiliöt niiden punnituksen yhteydessä. Kuljettajilla on käsipäätteet, joilla rekisteröidään säiliöihin kohdistuvat palvelutapahtumat.

Hyödyt ja mahdollisuudet: Voidaan sähköisesti tunnistaa henkilöitä tai tavaroita nopeasti tai tosiaikaisesti ilman kontaktia tai näköyhteyttä. Suhteellisen halpa ja automatisoitu tunnistus. Mahdollistaa uusien yritysten syntymisen. Mahdollistaa toimintojen automatisoinnin. Kulunvalvonta automaattista. Kuljetusten ja tavaroiden reaaliaikainen seuranta.

Aktiivitagit[4]

Aktiivitagi on halpa yksinkertainen tagi, joka passiivisesta RFID:stä poiketen voi suorittaa esimerkiksi mittaus- tai radiokommunikointitoimenpiteitä itsenäisesti. Tagi sisältää energialähteen tai se kehittää itse energiaa ympäristöstään. Aktiivitagit mahdollistavat sen, että tagi mittaa jatkuvasti tilaansa tai ympäristöään ja tarvittaessa lähettää tiedon eteenpäin.

Hyödyt ja mahdollisuudet: Aktiivitagien verkostolla voidaan toteuttaa esimerkiksi erilaisia valvonta- ja tunnistusjärjestelmiä. Mahdollisia uusia tuotteita ovat muun muassa anturiverkot ja aistivat ilmaisimet.

---

[3] Pasi Ahonen ja Antti Permala
[4] Henrik Huovila

Ilmaisu (detektio)[5]

Anturi tunnustelee fysikaalista tai kemiallista suuretta ja muodostaa sitä kuvaavan signaalin. Esimerkiksi sulkuventtiilien vuodot ja laakerien kulumat voidaan tunnistaa aiempaa paremmin mikromekaanisella piianturilla. Molemmat viat aiheuttavat rakenteissa värähtelyä ultraäänialueella. Toimilaitteen vikaantuminen, kuluminen ja huoltotarve saadaan selville, kun anturi sulautetaan laitteeseen mittaamaan värähtelyä.[6]

Uudet tekniikat voivat tarjota monia hyötyjä ja mahdollisuuksia. Esimerkiksi ilmaisevalla pakkauksella voi olla kyky monitoroida omaa tilaansa (lämpötila, kosteus, korroosio, ESD, happi jne.) ja mahdollisesti myös olla yhteydessä operaattoriin. Mittaus voi tapahtua antureilla tai muilla tekniikoilla. Myös ihmisen toimintakykyä voidaan seurata.

Kemiallisten ja biologisten tekijöiden havainnointi [7]

Laajan kansainvälisen tutkimus- ja kehitystyön kohteena on hyvän, toimivan ja nopean biodetektorin kehittäminen tärkeimmille bioagensseille. Esimerkiksi Yhdysvallat panostaa tälle alueelle n. 1 mrd. dollaria/v.[8] B-detektiossa käytetään yleisimmin mm. massaspektrometriaa PCR-tekniikkaa ja immunologisia tekniikoita. C-detektio perustuu perinteisiin analyyttisiin kemiallisiin tekniikoihin tai ioniliikkuvuusdetektoriin.

VTT:lla on vuosikymmenien perinne väestönsuojarakentamisesta, jossa myös CBNR-suojaus on aina ollut mukana – suodatintekniikat mukaan lukien. Nykyisten C- ja B-detektioon käytettävien tekniikoiden läpikäyminen sekä SWOT-analyysi ovat tekeillä IMPACT-projektissa, samoin kuin uusien bioteknisten menetelmien etujen evaluointi seuraavan sukupolven monianalyytti B- ja C-detektiomenetelmien kehittämisessä. PCR-pohjaisten määritysmenetelmien kehitystyössä teollisuusnäytteiden haittamikrobeille on tavoitteena mm: [9]

- elintarvike- ja paperiteollisuuden prosessi- ja lopputuotenäytteiden epätoivottujen mikrobien määrittäminen
- nopeiden molekyylibiologisten menetelmien soveltaminen uusille näytematriiseille
- keskittyminen valittuihin teollisuusprosesseissa epätoivottuihin avainmikrobilajeihin ja -ryhmiin.

---

5 Pasi Ahonen, Antti Permala ja Laura Raaska
6 Aarne Oja
7 Kristiina Takkinen
8 Veikko Komppa ja IMPACT WP400, D400.1
9 Outi Priha, Laura Raaska, Kirsi Kujanpää, Hanna Miettinen

Hyödyt ja mahdollisuudet: Uusilla mikrobiologisilla ja kemiallisilla menetelmillä tulokset voidaan saada paljon nopeammin, mikä mahdollistaa teollisuuden nopean reagoinnin ongelmatapauksissa (esimerkiksi saastuneen elintarvikkeen takaisinveto ennen jakelua, paperitehtaan prosessin säätö ennen mikrobien aiheuttamien ongelmien esiintymistä)

Millimetriaaltokuvannustekniikka[10]

Millimetriaaltokuvannustekniikalla ymmärretään millimetri- ja alimillimetrialueella tapahtuvaa kuvan muodostusta käyttäen erittäin herkkiä radiometrejä. Suhteellisen lyhyt aallonpituus yhdistettynä hyvään läpäisevyyteen esimerkiksi tyypillisissä vaatemateriaaleissa mahdollistaa vaatteiden alle kätkettyjen aseiden ym. esineiden ja räjähteiden etätunnistamisen jopa sadan metrin päästä.

Millimetriaaltokuvannustekniikan lyhyen ajanjakson tavoitteena on demonstroida käytännöllinen, hinnaltaan järkevä sekä riittävän herkkä kuvauslaitteisto. Demonstraatio käsittäisi muutamia pikselielementtejä yhdistettynä mekaaniseen skannaukseen. Keskipitkällä aikajänteellä pikselielementtien lukumäärää kasvatettaisiin kymmeniin pikseleihin yhdistettynä mekaaniseen tai mekaanis-elektroniseen skannaukseen, jolloin kuvanmuodostusaika putoaa muutamaan sekuntiin. Vaihtoehtoisesti demonstroitaisiin apertuurisynteesiin perustuvaa kuvauslaitteistoa. Pitkällä ajanjaksolla tavoitteena ovat: täydellinen elektroninen skannaus, videotaajuinen kamera (mm-alue); fokaalitaso, jossa useita tuhansia pikselielementtejä, videotaajuinen ”CCD”-kamera (alimm-alue); pidemmille etäisyyksille (esim. sotilassovellutukset) apertuurisynteesiin perustuva videotaajuuskuvaa tuottava kamera. Millimetriaaltokuvannustekniikkaa kehittävät VTT, NIST, DARPA, HSARPA, University of Delaware sekä monet yritykset.

Hyödyt ja mahdollisuudet: Monet uhkat jäävät nykyisillä lentokenttäturvajärjestelyillä huomaamatta: Metallinpaljastimet eivät ilmaise esimerkiksi keraamisia keittiöveitsiä. Ohuiden levyräjähteiden havaitseminen on nykyisillä röntgenlaitteistoilla hyvin haastavaa. Millimetrikameroilla on mahdollista havaita molemmat näistä esimerkkiuhista. Pitkällä tähtäimellä myös millimetri- ja alimillimetrialueelle lankeavat makromolekyylien resonanssit voivat mahdollistaa esimerkiksi biologisten uhkien etätunnistuksen. Lentokenttien maaliikenteen seuranta mahdollistuu lähes kaikissa olosuhteissa, koska mm-aallot etenevät mm. sumun läpi. Uhkien etätunnistaminen mahdollistaa uhkan lievittämisen ennen sen lokalisoitumista turvattavaan kohteeseen. Myös sotilaallisia sovelluksia.

[10] Markku Jenu

Hahmontunnistus[11]

Hahmontunnistuksen (pattern recognition) avulla pyritään tunnistamaan, luokittelemaan tai mallittamaan tarkasteltavia kohteita niiden ominaisuuksien tai niistä tehtyjen havaintojen perusteella. Hahmontunnistus käyttää mm. signaalinkäsittelyn, neurolaskennan, tilastotieteen ja tekoälyn menetelmiä. Näiden avulla voidaan käsitellä monentyyppistä informaatiota, kuten kuvia, puhetta, tekstiä, teollisuusprosessin mittauksia, tiedusteluinformaatiota, tilastoaineistoja ja muuta tietoa. Menetelmien mahdollisia tarkkailukohteita voisivat olla esimerkiksi metroasemat, rekisterikilvet ja epäilyttävä ”käytös”.

VTT:llä on noin 25 vuoden aikana tehty paljon hankkeita lähes kaikille hahmontunnistuksen osa-alueille. Teollisuuden aloja ovat mm. teollisuusautomaatio, prosessiautomaatio, robotiikka, mobiletekniikka, kierrätysteollisuus, lääketiede, biotekniikka, logistiikka, laboratorioautomaatio, kaukokartoitus, turvallisuustekniikka, kiinteistönhallinta, liikennevalvonta, elektroniikka, mikroelektroniikka, jne.

Hyödyt ja mahdollisuudet: Turvallisuustilanteen hahmottaminen, hälytykset, muutoksen havaitseminen; ihmisen ja koneen vuorovaikutuksen yksinkertaistaminen; digitaaliset kuva-arkistot, haku, ym.; lääketiede: automaattinen potilaskuvien läpikäynti; robotiikka: liikkuminen, automaattinen työskentely; teollisuusautomaatio: valmistus, liikkuminen; henkilön identiteetin varmistaminen (maahantulo, lentoliikenne, muut kriittiset kohteet). Uusia tuotteita ja palveluja ovat esimerkiksi

- tietokoneen ja matkapuhelimen käyttöliittymään liittyvät keksinnöt
- ohjelmistotuotteet tunnistusjärjestelmien kehitystyön ja käyttöönoton nopeuttamiseksi
- erikoissovelluksiin räätälöidyt anturit (esimerkiksi laajaspektrinen havainnointi).

Biometrinen henkilöntunnistus[12]

Henkilön tunnistaminen fyysisen ominaisuuden (esimerkiksi sormenjäljen) tai käyttäytymispiirteen perusteella (esimerkiksi kävelytyylin). Tyypillisesti järjestelmän käyttäjä ensin rekisteröidään (opetetaan, enrollataan) järjestelmään, esimerkiksi antamalla mallisormenjälki, jonka jälkeen normaalissa toiminnassa annettua tunnistetietoa verrataan opetettuun mallineeseen (template). Biometrinen tunnistus voidaan jakaa yksi-yhteen-tunnistukseen (verifiointi) tai yksi-moneen-tunnistukseen (identifiointi). Erikseen on vielä ns. watch-list-toiminta, jossa vain tietyt henkilöt halutaan tunnistaa.

[11] Pasi Ahonen, Heikki Ailisto ja Jouko Viitanen
[12] Pasi Ahonen, Heikki Ailisto

Tyypillisiä tuotteita ja palveluja ovat:

- tietoturva: PC:t, tietoverkot
- pankkiautomaatit, muu pankkitoiminta
- biometriset lukot ja kulunvalvonta: lentokentän suljetut alueet, toimistot, tehtaat, sairaalat, virastot, kodit
- turvallisuus: puolustusvoimat
- avustusten jako katastrofialueella
- maahantulo: passintarkastus
- viranomaistoiminta ja asiapaperit.

Tulevaisuuden sovelluksia voisivat olla:

- sähköinen kauppa
- mobiilit päätelaitteet, tulevaisuuden internet kännykät, mobiilimaksaminen
- laitteiden ja palveluiden personointi käyttäjälle: autot, kodinkoneet, kuntosalilaitteet
- kotielektroniikka tunnistaa, kuka tuli huoneeseen ja valitsee suosikkikanavan ja äänenvoimakkuuden jne.
- seniorikansalaisten turvallisuus ja mukavuus.

2.4.4 Tietoverkkojen ja -järjestelmien suojaus

Yhteensopivuus tietoturvamielessä[13]

Eri organisaatioiden, yritysten, ja julkishallinnon, verkkoja joudutaan erilaisissa arvoverkoissa liittämään yhteen esimerkiksi tietyn palvelukokonaisuuden mahdollistamiseksi tai yritysten yhteistyön parantamiseksi. Näillä organisaatioilla voi olla hyvinkin erilaisia tietoturvapolitiikkoja (policies), ja tietoturvan taso verkoissa saattaa vaihdella. Jos verkkojen yhteen liittämisessä hyödynnetään julkista Internetiä, on mukana myös komponentti, jolle tietoturvapolitiikkaa ei ole määritelty ja tietoturvan taso on vaihteleva tai tuntematon. Jatkossa on kiinnitettävä erityistä huomiota tietoturvan riittävän tason varmistamiseen, kun palvelut, laitteet ja verkot yhdentyvät tulevaisuudessa yhä enemmän ja enemmän. Varsinkin suljettujen vanhojen järjestelmien kytkeminen avoimiin järjestelmiin asettaa kovia haasteita tietoturvaratkaisuille.

[13] Jarkko Holappa

Hyödyt ja mahdollisuudet: Turvallinen eri organisaatioiden, yritysten ja julkishallinnon verkkojen liittäminen yhteen esimerkiksi tietyn palvelukokonaisuuden mahdollistamiseksi tai yritysten yhteistyön parantamiseksi. Tietoturvan liittäminen osaksi yrityksen liiketoimintaprosessia.

Tunkeutumisen esto, havainnointi- ja torjuntajärjestelmät sekä tietoturvan mittaus verkoissa[14]

Tunkeutumisen havaitsemisjärjestelmät (IDS) ja tunkeutumisen estojärjestelmät (IPS) monitoroivat verkkoliikennettä ja sen ominaisuuksia. IDS-järjestelmän tarkoituksena on havaita tunkeutumisyritykset ja toimia niin, että mahdolliset vahingot saadaan minimoitua. Mitä aiemmin hyökkäys todetaan, sitä vähemmän tuhoa siitä aiheutuu. Tällaiset järjestelmät mahdollistavat myös tiedon keräämisen hyökkäystekniikoista. Tätä tietoa voidaan käyttää kehitettäessä tehokkaampia tunkeutumiseneston menetelmiä ja mittausjärjestelmiä.

Hyödyt ja mahdollisuudet: Järjestelmä havaitsee tunkeutumisyritykset ja toimii niin, että mahdolliset vahingot saadaan minimoitua estämällä tai hidastamalla tunkeutumisen tai rajaamalla sen vaikutuksia. IDS-/IPS-järjestelmiä pitää kehittää kokonaisvaltaisempaan ja älykkäämpään suuntaan, ”Beyond IDS”.

Ohjelmistoalustat ja -arkkitehtuurit[15]

Ohjelmistoalustoilla ja -arkkitehtuureilla ymmärretään tässä yhteydessä

- tietoturvanhallintamekanismeja sulautetuissa ohjelmistotuotteissa lähtien arkkitehtuuri- tai alustanäkökulmasta
- erityisesti välitason ohjelmiston (middleware) ratkaisut ovat merkittäviä.

Hyödyt ja mahdollisuudet: Tietoturvan hallintaratkaisut, sisällönsuojaus. Ohjelmistoalustojen ja -arkkitehtuurien tietoturvatestaustekniikoiden kehittäminen on tärkeää, jotta ne tarjoaisivat riittävän laadukkaan pohjan laitteille ja sulautetuille järjestelmille.

[14] Jarkko Holappa ja Reijo Savola
[15] Reijo Savola

Verkko- ja Internet-tietoturva[16]

Verkko- ja Internet-tietoturvalla ymmärretään tässä yhteydessä:

- verkottuneen ympäristön mahdollistamien uhkien tunnistamista, torjuntaa ja estoa sekä valvontaa ja hallintaa
- Internetiin ja sen tarjoamien palvelujen käyttöön liittyvää kokonaisvaltaista tietoturvanhallintaa ja IP-verkkojen tietoturvaratkaisuja
- verkon itsensä ja sen hallinnan turvaamista
- verkon tukemien overlay-verkkojen turvaamista
- tietoturvanhallintaratkaisuja Internet-sovellusympäristössä. On nähtävissä, että IP-verkkoteknologia tulee olemaan hallitseva lähes kaikissa verkkoratkaisuissa. Muita teknologioita käytetään vain erikoissovelluksissa (mm. hyvin yksinkertaisten laitteiden, kuten antureiden, liittämisessä laajempiin verkkoihin).
- IP-verkkojen erityisongelmia.

Hyödyt ja mahdollisuudet: Autonomisuus ja hallittavuus; tietoturva läpinäkyvästi osaksi sekä verkkoa että sen palveluja. Hallittavuudesta seuraa jäljitettävyys. Voidaan vaikuttaa siihen, kuka tekee ja mitä tekee. Mahdollistaa käytön vaativissa sovelluksissa. Uusia tuotteita ja palveluja voivat olla esimerkiksi verkon tietoturvan tukipalvelut, jotka sisältävät dynamiikan ja kattavat mobiilisuuden, aktiivisen häiriöihin puuttumisen ja overlay-verkot.

Tietoturvatestaus[17]

Tietoturvatestauksella tarkoitetaan tuotteen tai järjestelmän testausta tai kelpoistamista niin, että tietoturvatavoitteet toteutuvat. Jos tietoturvatavoitteita ei ole määritelty riittävällä tasolla, kuuluu tietoturvatestaukseen myös niiden määritteleminen. Tietoturvatestaus koostuu robustness-testauksesta ja tietoturva-analyysistä (= vertailu tietoturvatavoitteisiin).

Hyödyt ja mahdollisuudet: Testausosaamisen vahvistaminen. Tietoturvailmiöiden parempi ymmärtäminen. Synergia tietoturvamonitorointipuolelle (erityisesti metriikat). Varmuus siitä, että tuote on vaatimusten mukainen. Lisäksi tietoturvatestaus tarjoaa materiaalia tutkimustyöhön.

[16] Reijo Savola, Arto Juhola ja Juuso Pesola
[17] Reijo Savola

2.4.5 Fyysinen suojaus

Rakenteellinen suojaus[18]

Rakenteellisella suojauksella ymmärretään tässä yhteydessä

- ihmisten ja rakennuksessa sijaitsevien toimintojen suojaamista mekaaniselta iskulta, kuten
  - paineaallolta (räjähdykseltä)
  - kineettiseltä kuormitukselta (ajoneuvon törmäykseltä, sirpaleilta)
- ihmisten ja rakennuksessa sijaitsevien toimintojen suojaamista tulipalotilanteessa
- rakennuksessa sijaitsevien sähkölaitteiden sekä sähköisten piirien suojaamista
  - sähkömagneettiselta pulssilta (EMP)
  - suuritehoisilta mikroaaltoaseilta (HPM).

Hyödyt ja mahdollisuudet: Tunkeutumisen estäminen ja hidastaminen. Poikkeustilanteissa ihmisiin kohdistuu lievempiä vaikutuksia. Sähkömagneettinen suojaus. Uusia tuotteita ovat kestävämmät ja turvallisemmat materiaalit (esimerkiksi ikkunalasi, joka rikkoutuessaan ei sirpaloidu) sekä palvelut (esimerkiksi testausmenetelmä paineiskun vaikutuksen todentamiseen seinä- ja välipohjarakenteissa).

Suojaus ilman mukana kulkeutuvilta CBR-agensseilta[19]

Suojauksella ilman mukana kulkeutuvilta CBR-agensseilta ymmärretään

- CBR-agenssien detektointia ilmasta
- tulo- ja hengitysilman puhdistamista CBR-agensseista
- hajautettua ilmanvaihtojärjestelmää, rakenteiden tiiviyttä yms.
- kontrolloidun tilan ilman laatua ja sen edellyttämiä suodatusmenetelmiä
- ilmamikrobiologiaa ja biologisten agenssien tunnistamista ilmasta.

[18] Auli Lastunen
[19] Auli Lastunen, Laura Raaska ja Gun Wirtanen kommentoineet

Hyödyt ja mahdollisuudet: Normaalioloissa tehostettu tuloilman suodatus poistaa myös muut terveydelle haitalliset epäpuhtaudet (ulkoilman saasteet) ja tiiviimmät seinärakenteet säästävät lämmitysenergiaa. Poikkeustilanteissa ihmisiin kohdistuu lievempiä vaikutuksia. Tilojen puhdistustarve mahdollisen iskun jälkeen on vähäisempi. Uusia tuotteita ovat esimerkiksi tehokkaammat, monipuolisemmat, älykkäämmät, halvemmat, pitkäikäisemmät ja huoltovapaammat suodattimet ja analyysijärjestelmät. Alan kehitystä hidastaa se, että sille ei ole perusteita, ellei turvallisuusasioista ole viranomaisten antamaa ohjeistusta tai uhkaa koeta yleisesti niin suureksi, että asialle on jotain tehtävä. Rakennuttajilla on merkittävä rooli uusien tuotteiden käyttöönotossa. Varsinaisia käyttöönottajia ovat suodatin- ja detektorivalmistajat.

3. Yhteiskunnan järjestelmien turvaaminen

Tässä luvussa käsitellään yhteiskunnan järjestelmien turvaamista. Tarkasteltaviksi kohteiksi on valittu energiaverkot (3.1), tietoliikenneverkot (3.2), vesihuolto (3.3), liikenne ja kuljetukset (3.4) sekä ihmisten suojaaminen (3.5). Jokaisesta tarkastelukohteesta käydään läpi teknologiaperusta ja VTT:n nykyinen osaaminen sekä tavoite alueella.

3.1 Energiaverkostot[20]

Energiaverkostoilla ymmärretään tässä yhteydessä kaikkien yhteiskuntaa palvelevien ja yhteiskunnan keskellä sijaitsevien energiaverkostojen turvallisuutta. Näitä verkostoja ovat sähkö- ja kaukolämpö sekä kaasuverkko, laajimpana sähköverkko. Turvallisuudella tarkoitetaan sekä verkostojen käyttövarmuutta fyysistä uhkaa ja tietojärjestelmän kautta tapahtuvaa uhkaa vastaan että sen varmistamista, että järjestelmä ei aiheuta terveys- tms. vaaraa yhteiskunnalle (esimerkiksi sähköiskuvaara tai kaukolämpö- ja kaasuvuotoja). Fyysinen uhka on esimerkiksi verkon tai sen osan tuhoaminen; tietojärjestelmäuhka on esimerkiksi verkon käytettävyyden eliminointi.

3.1.1 Teknologiaperusta

Merkittäviä energiaverkostojen toiminnan varmistamiseen liittyviä teknologioita ovat kokonaisturvallisuuteen liittyvät erilaiset varautumissuunnitelmat sekä yleisesti hajautetun energiantuotannon lisääminen ja uudet rakenneratkaisut (taulukko 7).

[20] Osmo Auvinen, Reijo Savola kommentoinut

Taulukko 7. Energiaverkostojen turvaamisen teknologioiden kehitys.

Käytettävä teknologia	Lyhyt	Keskipitkä	Pitkä
Kokonaisturvallisuuden hallinta			
Riskianalyysi-menetelmät	Varautumis-suunnitelmat Security-näkökulman integroiminen haavoittuvuusanalyyseihin sekä muihin riskianalyysivälineisiin Riski- ja haavoittuvuusanalyysimenetelmien tarvekartoitus	Riski- ja haavoittuvuusanalyysimenetelmien kehittäminen Päätöksentekomallien kehittäminen Riskien kvantifioinnin kehittäminen Tilanteen reaaliaikainen seuranta	Hajautetun energiantuotannon lisääminen, uudet rakenneratkaisut Tietotekniset apuvälineet riski- ja haavoittuvuusanalyysien tekoon ja riskien kvantifiointiin
Ilmaisu (detektio)	Langaton sensoriteknologia, kuvankäsittely		Biologiset anturijärjestelmät
Tietoverkkojen ja -järjestelmien suojaus			
Tietoturva-monitorointi	Suojatut tietoliikenneyhteydet nykytekniikalla. Olemassa olevat QoS-, verkon liikenne- ja IDS/IPS-toteutukset.	Omat prototyypit (Beyond IDS)	Omat prototyypit (Beyond IDS)
Verkko- ja Internet-tietoturva	Verkkoriippumaton AAA/IDM, IPv4:ään pohjautuvia ratkaisuja IDS/IPS, ohj. verkot (mobiilisuustuki, verkkokonteksti)	Verkon ja kommunikoivien systeemien tietoturvayhteistyö (ohjelmoitavat verkot, IDS/IPS), IPv6, IPsec rajoitetusti	Avainhallinta (hyvä ja yleiskäyttöinen) Autonominen tietoturvan hallinta, oppivat systeemit
Tietoturvatestaus	Robustness-testaustyökalut, verkon monitorointityökalut ja yleiset testaustyökalut	Todennettu tietoturvatestausprosessi, joka käyttää työkaluja	Jatkuvasti kehittyvä ja monipuolinen tietoturvatestausprosessi ja työkaluvalikoima

3.1.2 VTT:n toiminta

Energiaverkostojen turvaamisen keskeisin osaaminen liittyy riskianalyysimenetelmien ja tietoturvan hallintaan (taulukko 8). Lisäksi esimerkiksi ilmaisuun (detektioon) liittyvä teknologinen osaaminen on merkittävää energiaverkostojen toiminnan turvaamisen kannalta. Tietoturvassa korostuvat tietoturvamonitorointi sekä tietoverkkojen ja -järjestelmien suojaus. Ohjauksen ja tietoliikenteen verkottuminen tuovat tietoturvauhkia jo nykyään. Keskinäisten riippuvuussuhteiden ymmärtäminen ja analysointi on oleellista.

Taulukko 8. VTT:n nykyinen osaaminen energiaverkostojen turvaamisessa.

Fokusalue	Vahvuudet, mikä osataan
Kokonaisturvallisuuden hallinta	
Riskianalyysi-menetelmät	Sähköverkostosta hallitaan tämän päivän tekniikat ja teknologiat, joilla voidaan vaikuttaa sähköverkon käytettävyyteen (tietojärjestelmät, materiaalit, rakenteet, ym.). Tunnetaan sähköjärjestelmän toiminta osana yhteiskuntaa sekä yrityselämää. Kaukolämpö- ja kaasuverkoston teknologiat ovat vähemmällä painoarvolla VTT:ssä. Perinteinen riskianalyysiosaaminen Todennäköisyyspohjaiset riskianalyysit
Tietoverkkojen ja -järjestelmien suojaus	
Monitorointi	Käynnissä EU-projekti (IST FP6, C4) IRRIIS (sähköverkostojen ja liittyvien järjestelmien riippuvuuksia analysointi).
Verkko- ja Internet -tietoturva	Sähköntoimituksen kaukoluentaan ja siihen liittyvien konfigurointi- ja maksupalvelujen tietoturvaan liittyen menossa Eureka-ITEA-projekti SHOPS.

VTT:n tavoitteena on luoda itselleen merkittävä rooli teknologioiden kehittäjänä (mm. energiavarastot) sekä yhteiskunnan ja julkisen sektorin suuntaan päätöksenteon tukena turvallisuuspoliittisissa ratkaisuissa.

3.2 Tietoliikenneverkot[21]

Kriittisiin infrastruktuureihin kuuluvat esimerkiksi turvallisuusviranomaisten tietoliikenne (poliisi, rajavartiolaitos, pelastuslaitos, puolustusvoimat) sekä kaikki ne ohjaus- ja tietoliikennejärjestelmät, jotka kuuluvat muihin kriittisiin infrastruktuureihin. Tietoliikenneverkoilla ymmärretään tässä yhteydessä:

- tietoliikenne ja puhelinverkkojen (kiinteän, matkapuhelimien) varmentamista ja suojausta
- kiinteitä verkkoja, VIRVEä yms., matkapuhelinverkkoa, Internetiä

[21] Arto Juhola, Reijo Savola, Pasi Ahonen; Julkaisu: Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka and Wiander Timo. *Information Security Threats and Solutions in the Mobile World – the Service Developer's Perspective.* Espoo 2005. VTT Tiedotteita – Research Notes 2308. ISBN 951-38-6737-4; 951-38-6738-2. 95 s. + liitt. 4 s. http://virtual.vtt.fi/inf/pdf/tiedotteet/2005/T2308.pdf

- Overlay-verkkojen (mm. dns, e-mail) tietoturvaa, varmuutta ja suojausta ts. Internetin p2p, mobility-, multicast-, content distribution ja grid-verkot, joilla omat, verkkokerroksen topologiasta eriytyneet solmut, myös e-mail
- verkkopalvelujen saatavuutta (availability)
- verkkojen toimintakykyä
- valtakunnallisia, alueellisia ja lokaalisia verkkoja, yritysverkkoja.

Mobiilipalveluilla tarkoitetaan palveluja, joita käytetään mobiililla päätelaitteella, usein verkkoyhteyden kautta. Palveluesimerkkejä ovat verkkopelaaminen ja musiikin kuuntelu. Mobiilipalvelujen tietoturvalla tarkoitetaan tietoturvan hallintaa infrastruktuurissa ja päätelaitteissa, joita tarvitaan mobiilipalvelujen toteuttamiseen. Kehittyneet mobiilipalvelut yleistyvät tulevaisuudessa, kun mobiililaitteet ja -verkot nykyaikaistuvat. Myös turvallisuuden kannalta kriittisiä palveluja, kuten esimerkiksi sähköistä maksamista, toteutetaan langattomasti (taulukko 9).

Taulukko 9. Tietoliikenneverkkojen turvaamisen teknologioiden kehitys.

Käytettävä teknologia	**Lyhyt**	**Keskipitkä**	**Pitkä**
Kokonaisturvallisuuden hallinta			
Tietoturvan hallinta	Auditointi- ja tietoturvavaatimusmäärittelypalvelut State-of-the-art-firewall, antivirus, IDS/IPS, verkkomonitorointi (liikenne, QoS), tekninen tuki, standardit	Teknisten logien yhdistäminen (firewall, antivirus, IDS) Tietokannat, sääntölogiikat, riskianalyysimenetelmät	Kehittynyt verkkomonitorointi (”beyond IDS”), proaktiivinen mittaus Pattern recognition, sumea logiikka, oppivat algoritmit, Semantic Web, työkalut analyysiin
Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
Anturiverkot (aktiivitagit)	Langattomat anturit, mikroanturit, bioanturit, antureiden sovellukset.	Anturiverkkotekniikat, mikroenergian generointitekniikat	Laajojen tagiverkkojen hallintamenetelmät, uudet kommunikointitekniikat
Biometrinen henkilöntunnistus	Sormenjälkitunnistus, puhujan tunnistus, kasvojen tunnistus, tunnistus iiriksestä, käden tunnistus, allekirjoituksen tarkastus		

Taulukko 9. Jatkuu ...

Tietoverkkojen ja -järjestelmien suojaus			
Tietoverkkojen ja -järjestelmien suojaus	IP-teknologiat	Mobile-IP (v4 ja v6)	
Tietoturva-monitorointi	Olemassa olevat QoS-, verkon liikenne- ja IDS/IPS-toteutukset	Omat prototyypit (Beyond IDS)	Omat prototyypit (Beyond IDS)
Ohjelmisto-alustat ja -arkkitehtuurit	Välitason ohjelmistokomponenttien hallintamekanismien kehittäminen Ohjelmistokomponenttimallit	Välitason ohjelmistokomponenttien hallintamekanismien kelpoistaminen Ohjelmistokomponentit, tietoturvatestaus	Turvalliset ja yksiselitteisesti tietoturvahallittavat välitason komponenttiarkkitehtuurit Ohjelmistokomponentit ja menetelmät
Verkko- ja Internet-tietoturva	Turvallinen välitason ohjelmistokerros, yksinkertaistettu ja robusti avaintenhallinta, ohjelmoitavat verkot tietoturvan ”liikkuvien osien” tarpeisiin (mobiilit verkkopalomuurit, mobiilit VPN:t yms.) Verkkoriippumaton AAA/IDM, IPv4:ään pohjautuvia ratkaisuja.(Mobiili X, esimerkiksi VPN, FW...) IDS/IPS, ohjatut verkot (mobiilisuustuki, verkkokonteksti)	Vaativaan käyttöön kelpaavat Internetit: automaattinen ja autonominen, politiikkapohjainen verkkotietoturvahallinta, ohjelmoitavien verkkojen mahdollistama, skaalautuva operaattorien ja kansainväliseen ympäristöön IPv6, IPsec rajoitetusti. Koodigeneraattoreita yms. reaaliaikaisessa operoinnissa hyödyntävä verkonhallinta	Proaktiivinen tietoturva, anonyymi ja digitaalinen kolikkopussi Avainhallinta (hyvä ja yleiskäyttöinen) Autonominen tietoturvan hallinta, oppivat systeemit, mahdolliset biologiset anturijärjestelmät
Tietoturva-testaus	Robustness-testaustyökalut, verkon monitorointi-työkalut sekä yleiset testaustyökalut	Overlay-tietoturva Tietoturvan mittaaminen (monitorointi) Todennettu tietoturvatestausprosessi, joka käyttää työkaluja	Tietoturvan mittaaminen, vahvat metriikat, laajempi valikoima työkaluja Jatkuvasti kehittyvä ja monipuolinen tietoturvatestausprosessi ja työkaluvalikoima

3.2.1 VTT:n toiminta

Tietoliikenneverkkojen turvaamisen keskeisin osaaminen liittyy tietoturvan hallintaan sekä luonnollisesti itse tietoverkkojen ja -järjestelmien suojaukseen. Myös anturiverkkoihin ja biometriseen henkilöntunnistukseen liittyvästä osaamisesta on hyötyä tietoliikenneverkkojen toiminnan turvaamisessa (taulukko 10).

Taulukko 10. VTT:n nykyinen osaaminen tietoliikenneverkkojen turvaamisessa.

Fokusalue	**Vahvuudet, mikä osataan**
Kokonaisturvallisuuden hallinta	
Tietoturvan hallinta	Ymmärrämme tietoturvanhallintaprosesseja Osaamme kehittää metriikoita auditointia ja monitorointia varten, laaja-alainen monitorointi- ja mittausosaaminen, sekä state-of-the-art-näkemys Osaamme tietoturvavaatimusten määrittelyä ja tietoturva-analyysiä, tietoturvamonitorointi- ja -testausympäristö kehitteillä
Biometrinen henkilöntunnistus	VTT soveltanut sormenjälkitunnistusta BioSec (Biometrics and Security) projektissa Finnairin ja sisäministeriön kanssa
Tietoverkkojen ja -järjestelmien suojaus	
Tietoverkkojen ja -järjestelmien suojaus	IP-verkkojen ja Internetin tietoturvanhallinta, tunnistusmenetelmien hallinta, tietoturva-arkkitehtuurien ja -alustojen osaaminen, osaamista kriittisistä palveluista, jotka käyttävät tietoliikenneverkkoja (maksupalvelut) Mobiilialustojen tietoturva PAN-koti ja -sensoriverkkoihin liittyvät minimalistiset mutta tehokkaat ja tietoturvalliset välitason ohjelmistoratkaisut
Tietoturva-monitorointi	Tietoverkko-osaaminen mobiili- ja kiinteiden verkkojen puolella monella kerroksella Tietoturvametriikkaosaaminen Tietokantaosaaminen
Ohjelmistoalustat ja -arkkitehtuurit	Osataan ohjelmistoarkkitehtuureja, ohjelmistoalustoja, tietoturva-ratkaisuja ja niiden arviointia
Verkko- ja Internet-tietoturva	Vahva (Internet-) verkko-osaaminen, myös ”avant-garde”-rintamalla Ohjelmoitaviin verkkoihin perustuvat edistykselliset ratkaisut (äärimmäinen dynaamisuus, reagointikyky ja joustavuus). Mobiilitietoturva, yleinen verkonhallinta Tietoturvaprotokollat (authentication, authorisation, accounting),
Tietoturvatestaus	Tietoturvan mittaaminen: monitorointi (IDS/IPS, beyond IDS/IPS), metriikat Vahvaa osaamista testauksessa ja tietoturvassa VTT:n tietoturvatiimeissä Valmiit kontaktit kaupallisiin testaajiin

Tietoturva on tärkeä osa järjestelmää; se voidaan tehdä kattavammaksi, varmemmaksi, tehokkaammaksi tai helpommaksi hallinnoida, pitkällä tähtäimellä tietoliikenteen osalta jopa käyttäjille näkymättömäksi. Osaa tietoliikenteen tietoturvasta voidaan hoitaa tehokkaammin verkon puolella, sovelluskohtaisesti.

Uusien sovellusten ja innovaatioiden kehitys pakottaa jatkossakin tietoturvan päivittämiseen tuotteilla tai palveluilla, jotka torjuvat esiin tulevia aukkoja. On huomattava erityisesti, että tekniset tietoturvaratkaisut ovat kuitenkin parhaimmillaankin vain tietoturvan hallinnan tuki. Hyviä tietoturvakäytäntöjä ja -prosesseja tarvitaan tuotteiden elinkaaren ja koko yrityksen kattavaan tietoturvanhallintaan. Erityinen haaste ovat tuotteet ja palvelut, jotka syntyvät yrityksen yhteistyönä.

3.3 Vesihuolto[22]

Vesihuollon palveluihin kuuluvat puhdasvesihuolto raakavesivarastoineen ja puhdistus- ja siirtojärjestelmineen, jätevesihuolto siirto- ja käsittelyjärjestelmineen ja sadevesihuolto siirtojärjestelmineen. Turvallisuudella tarkoitetaan em. järjestelmien käyttövarmuutta sekä fyysistä uhkaa vastaan että niiden väärinkäytön aiheuttamaa terveydellistä uhkaa vastaan. Fyysinen uhka on jonkun järjestelmän tai osajärjestelmän, esimerkiksi pumppaamon, tuhoutuminen. Terveydellinen uhka on jonkin kemiallisen, biologisen tai radioaktiivisen vaaratekijän pääseminen erityisesti puhdasvesijärjestelmään. Puhdasvesihuollon katkeaminen lamaannuttaa parissa kolmessa päivässä koko kaupungin ja erityisesti siitä riippuvaisen terveydenhuollon, elintarvikehuollon ja teollisuuden. Myös jätevesihuollon katkeaminen luo lyhyessä ajassa kaaoksen sekä kaupunkitasolla että teollisuuslaitostasolla mahdollisine ympäristökatastrofeineen.

Vesihuollon kriittinen infrastruktuuri käsittää:

- raakavesivarastoihin liittyvät padot (yli 1000 patoa, pääasiassa maarakenteita, joiden pettämiseen liittyy ihmishenkien menetyksen riski)
- raakavesitunnelit (mm. Päijänne-tunneli, josta yli miljoona ihmistä on riippuvaisia)
- muut maanalaiset tunnelit (jätevesi-, sadevesi- ja yhteiskäyttötunnelit energia- ja tietoliikenneverkkojen kanssa)
- maanalaiset järjestelmät (pumppaamot, sähköasemat, vedenpuhdistamot ja jätevedenkäsittelylaitokset sekä runkovesi- ja viemäriverkostot)
- muut yhdyskuntien ja teollisuuslaitosten vesihuoltolaitokset ja niiden ohjauskeskukset sekä kaukovalvontalaitteet ja järjestelmät).

[22] Hannu Maula ja Juhani Korkealaakso + kommentteja Laura Raaskalta ja Gun Wirtaselta

Esimerkiksi Helsingin vesihuollon valvonta on niin pitkälle automatisoitu, että viikonloppuina sitä valvoo yhdessä pisteessä yksi henkilö, jolla on varamies paikalla. Patoja, maanalaisia tiloja ja runkoverkostoja lukuun ottamatta riskit liittyvät vesihuollon kiinteistöihin ja rakennuksiin sekä kunnissa että teollisuuslaitoksissa.

3.3.1 Teknologiaperusta

Merkittäviä vesihuollon toiminnan varmistamiseen liittyviä teknologioita ovat kokonaisturvallisuuteen liittyen vesilaitosten tuoteturvallisuuden kannalta kriittisten prosessivaiheiden arviointi ja hallintajärjestelmän kehittäminen sekä uhkaskenaarioiden laatiminen ja potentiaalisten uhkien selvitys. Keskipitkällä ja pitkällä aikavälillä korostuvat erilaiset mallinnus-, simulointi-, visualisointi- ja paikannustekniikat sekä ohjaus- ja päätöksentekojärjestelmät. Tunnistukseen liittyviä merkittäviä teknologioita ovat kemialliset, biologiset ja radioaktiiviset analyysi- sekä detektiotekniikat. Keskipitkällä aikavälillä kehitetään mikrobiologista diagnostiikkaa kohdemikrobeille. Pitkällä aikavälillä korostuvat mikrobidiagnostiikan nopeus – tulokset alle 2 tunnissa – ja soveltaminen käytäntöön. Anturiteknologian ja tiedonsiirron on oltava nopeaa (taulukko 11).

Taulukko 11. Vesihuollon turvaamisen teknologioiden kehitys.

Käytettävä teknologia	**Lyhyt**	**Keskipitkä**	**Pitkä**
Kokonaisturvallisuuden hallinta			
Riskianalyysimenetelmät	Vesilaitosten tuoteturvallisuuden kannalta kriittisten prosessivaiheiden arviointi ja hallintajärjestelmän kehittäminen Uhkaskenaarioiden laatiminen ja potentiaalisten uhkien selvitys Riski- ja haavoittuvuusanalyysimenetelmien tietoteknisten työvälineiden kehittäminen	Mallinnustekniikat, simulointi, visualisointi, paikannustekniikat Päätöksentekomallien kehittäminen Riski- ja haavoittuvuusanalyysimenetelmien kehittäminen Riskien kvantifioinnin kehittäminen Tilanteen reaaliaikainen seuranta	Paikkatietojärjestelmät Ohjaus- ja päätöksentekojärjestelmät Tietotekniset apuvälineet riski- ja haavoittuvuusanalyysien tekoon ja riskien kvantifiointiin
Hälytysjärjestelmät ja monitorointi	Kulunvalvonta, paikannusteknologiat, ilman puhdistustekniikka, anturiteknologia	Tilannetietoisuus (sumeat teknologiat) + edelliset	Tunnistusteknologiat, anturi- ja ilmaisinteknologiat, uudet ICT- ja mobiiliteknologiat

Taulukko 11. Jatkuu ...

Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
Anturiverkot (aktiivitagit)	Langattomat anturit, mikroanturit, bioanturit, antureiden sovellukset	Tagiverkko-teknologioiden kehittäminen Energiaomavaraiset tagit	Laajojen moniteknologisten tagijärjestelmien suunnittelu- ja hallintamenetelmät
Ilmaisu (detektio)	Langaton sensoriteknologia, CBR-analyysitekniikat, langaton tiedonsiirto, pallorobottiteknologia Selvitys nykyisten markkinoilla olevien immunologisten B-tunnistukseen käytettävien detektiomenetelmien toimivuudesta Rekombinanttivasta-ainetekniikan hyödyntäminen kehitettäessä C- ja B-määritysmenetelmiä Haitallisten mikrobien detektointiin soveltuvien PCR-pohjaisten menetelmien kehittäminen	Mikrobiologisen diagnostiikan kehittäminen kohdemikrobeille Tuottaa tietyille C- ja B-analyyteille rekombinanttivasta-aineet ja kehittää niiden avulla herkkiä ja nopeita pikatestejä Bioanturi ja mikrofluidistiikan hyödyntäminen pikatestikehityksessä Testien laajentaminen mikrobien esiintymisen detektoinnista niiden toimintojen detektointiin (hajuntuotto, toksiinintuotto)	Nopean (tulokset alle 2 tunnissa) ja herkän mikrobidiagnostiikan soveltaminen käytäntöön Integroituun mittajärjestelmään soveltuvan multianalyytti detektioon soveltuvan immunomenetelmän (esimerkiksi sirutekniikkaan perustuvan) kehittäminen Tekniikoiden integrointi multianalyyttimäärityksiin soveltuvan sirutekniikan kehityksessä Bakteeritoimintojen nopeat määritykset käytäntöön
Hahmontunnistus	Valittujen erityissovellusten arkkitehtuurit, SW- ja HW-työkalut Signaalin- ja kuvankäsittely, tiedon louhinta, tilastotiede	Kehittynyt multimodaalinen biometrinen tunnistus, anturitiedon käyttö Oleellisen piirretiedon valitsemista auttavat apuvälineet	Kuvan ja näkymätiedon ymmärtäminen Ubi-antureita

3.3.2 VTT:n toiminta

Vesihuollon turvaamisen keskeisin osaaminen liittyy ilmaisuun (detektioon), anturiverkkoihin ja hahmontunnistukseen. Myös riskianalyysimenetelmien hallinta on olennaista. VTT:lla on laaja kokemus teknisten riskien ja teollisuuden tuotantoon liittyvien riskien analysoinnista ja hallinnasta. Lisäksi tietoturvan hallinta sekä hälytys- ja monitorointijärjestelmiin liittyvä osaaminen auttaa vesihuollon turvaamisessa (taulukko 12).

Taulukko 12. VTT:n nykyinen osaaminen vesihuollon turvaamisessa.

Fokusalue	Vahvuudet, mikä osataan
Kokonaisturvallisuuden hallinta	
Riskianalyysi-menetelmät	Materiaalien ja rakenteiden käyttöikämallit, hydrologiset ja geofyysiset mittausmenetelmät, vesilaitosten tietojärjestelmät. Monitorointi- ja mallinnusjärjestelmien kehitys käynnistynyt laajana kansainvälisenä yhteistyönä Ympäristöriskien ja pohjavesivaroja uhkaavien riskien arviointi
Tietoverkkojen ja -järjestelmien suojaus	Ohjausjärjestelmät ja siihen liittyvä tietoliikenne tietoturvan kannalta
Ilmaisu, tunnistus, paikannus ja tiedonsiirto	
Ilmaisu (detektio)	Veden mikrobiologiset analysointitekniikat, mikrobiologinen diagnostiikka, eri materiaalien vaikutus haittamikrobien tarttumiseen, biofilmin muodostukseen sekä materiaalien puhdistuvuuteen, vesilaitosten tuoteturvallisuusriskien arviointi ja riskinhallintamenetelmien kehittäminen Kemialliset anturit on jo suurelta osin kehitetty

VTT:n tavoitteena on lyhyellä aikavälillä kehittää veden laadun ja turvallisuuden analysointijärjestelmiä sekä monitorointimenetelmiä verkostojen laajuiseen kunnonvalvontaan. Keskipitkällä aikavälillä tavoitteena on immunologisten pikamääritysmenetelmien kehittäminen ja niiden toimintavarmuuden todentaminen sekä integroitujen, miniatyrisoitujen mittausjärjestelmien kehittäminen ja niiden toimintavarmuuden todentaminen.

3.4 Liikenne ja kuljetukset[23]

Liikenteen ja kuljetusten turvallisuus koskee etenkin seuraavia asioita:

- häirikkökäyttäytyminen julkisissa liikennevälineissä (linja-autoissa, junissa, lentokoneissa, takseissa) ja liikenneasemilla
- liikenteen infrastruktuuriin (väyliin laitteineen, terminaaleihin), liikenne- ja kuljetusvälineisiin, niitä käyttäviin ihmisiin ja niillä kuljetettaviin tavaroihin kohdistuva ilkivalta, rikollisuus ja terrorismi. Tämä koskee tavaraliikenteessä kuljetusta, käsittelyä, varastointia ja logistiikan hallintaa

[23] Antti Permala, Veli-Pekka Kallberg ja Jukka Räsänen, kommentit Laura Raaskalta ja Gun Wirtaselta

- liikenteen tietojärjestelmiin kohdistuva rikollisuus ja terrorismi, joka voi aiheuttaa vaaraa tai merkittävää haittaa logistiikkatoimialalle. Tämä koskee erityisesti tavaraliikenteen ohjausjärjestelmiä, henkilöliikenteen henkilötietojärjestelmiä ja maksujärjestelmiä.

Liikenneonnettomuuksiksi luettavista tapahtumista security-käsitteen piiriin kuuluvat tapahtumat poikkeavat tyypillisesti siinä, että ne eivät tule aiheuttajalle yllätyksenä, tapahtuman aiheuttajasta ei ole epäselvyyttä ja teot ovat tahallisia.

Liikenteen ja kuljetusten turvaamisen tavoitteet henkilö- ja tavaraliikenteessä ovat:

Henkilöliikenne: Julkisilla liikennevälineillä matkustavat tai muuten julkisilla liikenneverkoilla liikkuvat ja terminaaleissa asioivat henkilöt ovat turvassa fyysisiltä vammoilta, joita aiheutuu kanssamatkustajien häiriköinnistä (joukkoliikennevälineissä), ilkivallasta, rikollisuudesta tai terrorismista. Liikenteeseen liittyvät henkilötietojärjestelmät on suojattu asiattomalta käytöltä, josta voi aiheutua asianosaisille haittaa.

Tavaraliikenne: Tavarankuljetukset julkisilla ja yksityisillä liikenneverkoilla (ml. silloilla, tunneleissa ja suluilla erityisesti TEN-T-verkolla) ja terminaaleissa (erityisesti satamissa) voidaan ilkivallasta, rikollisuudesta ja terrorismista aiheutuvista vaaroista suojattuna toteuttaa suunnitelluissa aikatauluissa niin, etteivät kuljetettavat tavarat vaurioidu eikä kuljetuksista aiheudu vaaraa tai kohtuutonta haittaa ihmisille tai ympäristölle. Kuljetuksiin liittyvät tietojärjestelmät on suojattu asiattomalta käytöltä, josta voi aiheutua asianosaisille haittaa.

3.4.1 Teknologiaperusta

Liikenteen ja kuljetusten toiminnan varmistamisessa korostuvat tunnistus-, paikannus- ja tiedonsiirtoteknologiat. Näitä ovat lyhyellä tähtäimellä ajoneuvojen ja kuorman seurantateknologiat sekä GIS-sovellukset. Keskipitkällä aikavälillä kehitys kohdistuu järjestelmäkehitykseen, esimerkiksi ohjaus- ja valvontajärjestelmiin, ja pitkällä näiden eri järjestelmien integrointiin (taulukko 13).

Taulukko 13. Liikenteen ja kuljetusten turvaamisen teknologioiden kehitys.

Käytettävä teknologia	Lyhyt	Keskipitkä	Pitkä
Kokonaisturvallisuuden hallinta			
Riski-analyysi-menetelmät	Riskienhallinta sekä riskien kartoittaminen ja kvantifiointi	Päätöksenteko- ja riskienhallintamallien kehittäminen	Tietoteknisten apuvälineiden hyödyntäminen kuljetuksissa
Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
GPS, GALILEO	Ajoneuvojen ja kuorman seurantateknologiat, GIS-sovellukset	Ohjaus- ja valvonta-järjestelmät	Eri järjestelmien integrointi
RFID	RFID-tunnisteista ”nappi” -tyypissä herkkä antenni ja siru on valettu epoksiin. Näin tunniste kestää kovaa kohtelua ja kemikaaleja. Kompakti pakkauskoko kuitenkin rajoittaa lukuetäisyyttä. Aktiivi ja passiivi RFID	Hierarkkiset tunnistusratkaisut, luetaan aina korkein taso (kolli, laatikko, tuotepakkaus, tuote...); toimintatavat, jotka hyötyvät autom. tunnistamisesta Painettavat saattomuistit, muutoin integroidut saattomuistit; NFC-teknologia integroitu matkapuhelimeen	Mukana tuotteiden tekoprosessissa ja edelleen kehittelyssä, Globaalit ratkaisut; saattomuisti tuotteen käyttöliittymänä
Anturiverkot (aktiivitagit)	Energian generointimenetelmien kehittäminen Lyhyen kantaman radiotekniikat Langattomat anturit, mikroanturit, bioanturit, antureiden sovellukset	Tagiverkko-teknologioiden kehittäminen Energiaomavaraiset tagit Anturiverkkotekniikat, mikroenergian generointitekniikat	Laajojen moniteknologisten tagijärjestelmien suunnittelu- ja hallintamenetelmät Laajojen tagiverkkojen hallintamenetelmät, uudet kommunikointitekniikat
Hahmontunnistus	Valittujen erityissovellusten arkkitehtuurit, SW- ja HW-työkalut Signaalin- ja kuvankäsittely, automaattinen henkilöntunnistus, tiedon louhinta, tilastotiede	Kehittynyt multimodaalinen biometrinen tunnistus, anturitiedon käyttö. Oleellisen piirretiedon valitsemista auttavat apuvälineet	Tiedustelutiedon (laajasti ymmärrettynä) analysointi ja uhkatilanteiden tunnistus. Kuvan tai näkymätiedon ymmärtäminen Ubi-antureita
Biometrinen henkilöntunnistus	Sormenjälkitunnistus, puhujan tunnistus, kasvojen tunnistus, tunnistus iiriksestä, käden tunnistus, allekirjoituksen tarkastus		
Tietoverkkojen ja -järjestelmien suojaus			
Tietoverkkojen suojaus	IP-teknologiat	Mobile-IP (v4 ja v6)	
Tunkeilunesto yms.	Olemassa olevat QoS-, verkon liikenne- ja IDS/IPS-toteutukset	Omat prototyypit (Beyond IDS)	Omat prototyypit (Beyond IDS)

3.4.2 VTT:n toiminta

Liikenteen ja kuljetusten turvaamisen keskeisin osaaminen liittyy paikkatietojärjestelmiin (GPS, Galileo), RFID:hen, anturiverkkoihin, hahmontunnistukseen ja biometriseen henkilöntunnistukseen. Lisäksi tietoverkkojen ja -järjestelmien suojauksen sekä riskianalyysimenetelmien osaaminen on merkittävää liikenteen ja kuljetusten turvaamisessa (taulukko 14).

Taulukko 14. VTT:n nykyinen osaaminen liikenteen ja kuljetusten turvaamisessa.

Fokusalue	**Vahvuudet, mikä osataan**
Kokonaisturvallisuuden hallinta	
Riski-analyysi-menetelmät	Logistiikkajärjestelmät, toimitusketjun hallinta Telematiikan arkkitehtuurit ja tietojärjestelmät Simulointi, optimointi yms. matemaattiset menetelmät Ihmisten käyttäytyminen Kuljetusmuotokohtaiset erityispiirteet (tie, rautatie, vesi ainakin, ilmakuljetukset tulevaisuudessa)
Ilmaisu, tunnistus, paikannus ja tiedonsiirto	
GPS, GALILEO	GPS-, GALILEO- ja GIS-sovellukset Logistiikan ja kuljetusten teknologiat (aktiivi ja passiivi RFID, muut langattomat (BT, WLAN, Zigbee jne.)
RFID	Olemassa on RFID-esiselvityksiä ja -pilotteja: langaton ratkaisu, toimivia logistiikkasovelluksia olemassa, kulunvalvonta vahvin alue, bussikortit, tuotannon ohjaus, auton avaimet, RFID-lukija Symbian puhelimessa
Anturiverkot (aktiivitagit)	Laajaa osaamista tagien vaatimissa tekniikoissa: RF-tekniikat, lyhyen kantaman radiotekniikat, mikroenergian generointi, verkkotekniikat, anturitekniikat, liittyminen päätelaitteisiin ja taustajärjestelmiin Tagiverkkojen tutkimus ja kehittäminen käynnissä Energian generointimenetelmiä kehitetty ja kehitteillä
Hahmon-tunnistus	Puhekommunikaatio automaatio- ja tietoliikennesovelluksissa: audio-analyysi, puheen ja muun erottaminen audiosignaalista, puhujan vaihtumisen havaitseminen, puhujan tunnistus Sormenjälkeen perustuva tunnistus, konenäkö
Tietoverkkojen ja -järjestelmien suojaus	
Tietoturva-monitorointi	Tietoliikenne ja ohjaus (tietoturva)

VTT:n tavoitteena on tarjota palveluja ja kehittää teknologisia ratkaisuja teollisuuden hankkeissa, joissa kuljetusten security on tärkeä (EU- ja Tekes-hankkeet). Keskipitkällä aikavälillä tavoitteena on kehittää toimitusketjun hallintaan integroituja innovatiivisia seurantajärjestelmiä ja liikenteen hallinnan menetelmiin integroituja järjestelmiä.

3.5 Ihmisten suojaaminen terrori-iskujen seurauksilta[24]

Ihmisten suojaamisella terrori-iskujen seurauksilta ymmärretään tässä yhteydessä:

- uhkakuvien määrittämistä ja siihen liittyvää riskien arviointia (sen pohjalta myös nopeaa ja oikeaa väestön tiedottamista uhan realistisuudesta)
- uhkakuvien analysointia, teknisiä keinoja uhkien lieventämiseksi
- ensipelastusjoukkojen (first responder) määrittämistä ja yhtenäisen konseptin luomista EU-tasolla
- kemiallisten tekijöiden detektiota (C)
- biologisten tekijöiden detektiota (B)
- suojalaitteiden vaatimuksia ja toimintavarmuutta (CBRN)
- pelastusjoukkojen ja muiden osallistuvien suojaamista (CBRN)
- dekontaminaatiota
- epäilyttävän materiaalin näytteenottoa, kuljetusta ja analysointia.

CBRN (C = kemiallinen, B = biologinen, R = säteily ja N = ydinvoima) terrorismin uhkakuvan ennaltaehkäisyyn ja torjuntaan panostetaan voimakkaasti Euroopassa. Yhdysvalloissa tällaisen terrorismin torjuntaan on jo useamman vuoden panostettu voimakkaasti. Yhteistyön luominen EU:n ja Yhdysvaltojen välillä on käytännössä vaikeata. Myös Euroopan sisällä yhteistyö ontuu, sillä NATOlle tehty tutkimustyö ei ole suoraan NATOn ulkopuolisten maiden käytettävissä.

Suomen kiinteistökanta on suunniteltu vuosikymmenien ajan niin, että ihmiset ja kriittiset toiminnot voidaan siirtää väestönsuojiin suojaan sota-ajan ilmaiskuilta ja jopa lähialueilla tapahtuvilta ydiniskuilta. Suojat suunnitellaan ja rakennetaan niin, että ne kestävät voimakasta ulkopuolelta aiheutettua maaperän tärähtelyä, ilmakehässä leviäviä paineiskuja sekä ilmassa leviäviä terveydelle haitallisia kaasuja ja hiukkasia (CBNR).

VTT:llä on vuosikymmenien perinteet väestönsuojien teknisten vaatimusten sekä suojaustekniikoiden kehittämisessä. Käytännöllisesti katsoen kaikki Suomen väestönsuojissa käytettävä tekniikka on tutkittu VTT:ssä. Uudet terroriin liittyvät uhkakuvat ovat kuitenkin luoneet painetta tekniikoiden edelleen kehittämiseksi, erityisesti kemialliselta ja mikrobiologiselta uhalta suojautumiseksi.

[24] Gun Wirtanen, Laura Raaska, Ilpo Kulmala ja Veikko Komppa

3.5.1 Teknologiaperusta

Merkittäviä ihmisten suojaamiseen liittyviä teknologioita ovat fyysisen suojaamisen teknologiat sekä erilaiset tunnistus-, paikannus- ja tiedonsiirtoteknologiat. Jälkimmäisiä voivat olla esimerkiksi millimetriaaltokuvannustekniikka sekä immunologiset tekniikat C- ja B-detektiossa. Kehityksen odotetaan etenevän kemiallisten agenssien detektiosta biologisten agenssien detektioon, analyysijärjestelmien kehittämiseen ja siitä edelleen detektion soveltamiseen käytäntöön.

Kokonaisturvallisuuden hallinnassa korostuu riski- ja haavoittuvuusanalyysimenetelmien kehittäminen esimerkiksi poikkeavan käytöksen tilastollisen havaitsemisen suuntaan. Tämä edellyttää esimerkiksi riskien kvantifiointiin tarvittavan datan saatavuuden kartoittamista, kysely- ja haastattelututkimusmenetelmien, riskien kvantifioinnin ja päätöksentekomallien kehittämistä sekä tilanteen reaaliaikaista seurantaa, tulkintaa ja ohjausta (taulukko 15).

Taulukko 15. Ihmisten suojaamisen teknologioiden kehitys.

Käytettävä teknologia	**Lyhyt**	**Keskipitkä**	**Pitkä**
Kokonaisturvallisuuden hallinta			
Riskianalyysi-menetelmät	Riski- ja haavoittuvuusanalyysimenetelmien tietoteknisten työvälineiden kehittäminen Riskien kvantifiointiin tarvittavan datan saatavuuden kartoittaminen Kysely- ja haastattelututkimusmenetelmät	Uusien riski- ja haavoittuvuusanalyysimenetelmien kehittäminen Päätöksentekomallien kehittäminen Riskien kvantifioinnin kehittäminen Tilanteen reaaliaikainen seuranta, tulkinta ja toiminnan ohjaus	Tietotekniset apuvälineet riski- ja haavoittuvuusanalyysien tekoon ja riskien kvantifiointiin
Hälytys-järjestelmät ja monitorointi	Kulunvalvonta, paikannusteknologiat, ilman puhdistustekniikka, anturiteknologia Pelastusajoneuvoon tietoa välittävät ja raportoivat kiinteistöt	Tilannetietoisuus (sumeat teknologiat) + edelliset	Tunnistusteknologiat, anturi- tai ilmaisinteknologiat, uudet ICT- ja mobiiliteknologiat
Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
Ilmaisu (Millimetriaaltokuvannustekniikka)	Erittäin matalakohinaiset HEMT-vahvistimet koherentin lähestymistavan tapauksessa (demonstroitu). Suprajohtavat antennikytketyt mikrobolometrit epäkoherentissa lähestymistavassa (demonstroitu).	Kanava- tai pikselimäärän kasvattaminen, elektronisessa skannauksessa RF MEMS -tekniikka. Komponenttien kustannusten minimointi, erityisesti koherenteilla ilmaisimilla. Spektroskooppiset kuvantavat ilmaisimet bolometrien tapauksessa. Bolometrien jäähdytys kryovapaalla jäähdyttimellä	mm-alueen CMOS-tekniikka

Taulukko 15. Jatkuu ...

Ilmaisu (Immunologiset ja DNA-pohjaiset teknologiat sekä näytteenotto- ja esikäsittely)	Kemiallisten agenssien detektio ilmanäytteiden otto ja esikäsittely Selvitys immunologisten C- ja B-detektiomenetelmien toimivuudesta. Rekombinanttivasta-aineteknologian etujen evaluointi ja hyödyntäminen C- ja B-menetelmien kehityksessä. Kehittää näytteenottoa ja PCR-pohjaisia menetelmiä haitallisten B-agenssien detektointiin	Biologisten agenssien detektio ja analyysijärjestelmien kehittäminen Integroida näytteenotto ja esikäsittely osaksi analysointiprosessia Tuottaa tietyille C- ja B-analyyteille rekombinanttivasta-aineet ja kehittää niiden avulla herkkää ja nopeaa pikatestiä. Bioanturi ja mikrofluidistiikan hyödyntäminen pikatesteissä Mikrobitoimintojen detektointi (hajuntuotto, toksiinintuotto) Laajentaminen muihin näytematriiseihin	Biologisten agenssien detektion soveltaminen käytäntöön Integroituun mittajärjestelmään soveltuvan immunomenetelmän (esimerkiksi sirutekniikkaan perustuvan) kehittäminen Molekyylibiologiset menetelmät uhkien kartoittamiseen ja niiden hallintaan Mikrobitoimintojen perusteella toimivien menetelmien kehitys
Fyysinen suojaus			
Rakenteellinen suojaus	Kehittää rakenteellisia ratkaisuja tilojen suojaamiseen EMP- ja HPM-iskuilta	Paineaaltojen simulointi	Järjestelmä, jolla viranomaiset tai rakennuttaja voi helposti ottaa huomioon turvallisuusseikat ja rakennuttaa halutessaan turvallisen rakennuksen
Suojaus ilman mukana kulkeutuvilta CBR-agensseilta	Kehittää CBR-agenssien detektointia Kehittää ulko- ja väliseinäratkaisuja tiiviimmiksi Antimikrobiset sovellukset ilmanvaihtojärjestelmissä Hiukkassuodattimet: sähköisesti tehostettu hiukkassuodatin Kaasusuodattimet: uudet kuitukangasaktiivihiilimateriaalit, aktiivihiilen impregnoinnin vanhenemisreaktioiden parempi hallinta Antimikrobisten ominaisuuksien liittäminen suodatinteknologiaan	Hiukkassuodattimet: nanokuidut Kaasusuodattimet: regeneratiiviset suodatinratkaisut, uudet impregnointitekniikat Mikrobidiagnostiikan kehittäminen ja soveltaminen kohdematriiseihin ja kohdemikrobeihin	Kaasusuodattimet: UV+fotokatalyysi, molekyyliseula, katalyyttinen hapetus, syklinen suodatus Mikrobidiagnostiikan kehittäminen ja soveltaminen kohdematriiseihin ja kohdemikrobeihin

3.5.2 VTT:n toiminta

VTT toimii kansallisesti ja kansainvälisesti eri puolustusorganisaatioiden merkittävänä kumppanina. Ihmisten suojaamisen keskeisin osaaminen liittyy toisaalta fyysisen suojauksen, ts. rakenteellisen suojauksen ja suojauksen ilman mukana kulkeutuvilta CBR-agensseilta, ja toisaalta ilmaisu (detektio) -teknologioiden kehittämiseen. Myös hälytys-

ja monitorointijärjestelmiin liittyvä osaaminen sekä järjestelmien integrointi on olennaista (taulukko 16).

Taulukko 16. VTT:n nykyinen osaaminen ihmisten suojaamisessa.

Fokusalue	**Vahvuudet, mikä osataan**
Ilmaisu, tunnistus, paikannus ja tiedonsiirto	
Ilmaisu (millimetriaalto-kuvannus-tekniikka)	Vankka millimetrialueen sekä mikroaaltotekniikan tuntemus. Koherenttien ja epäkoherenttien ilmaisimien ominaisuuksien tuntemus sekä näiden vahvuuksien sekä heikkouksien tunnistaminen Demonstroidut kuvantamislaitteet sekä millimetri- että alimillimetrialueelle. Kokeellisesti varmennettu ennätyksellinen herkkyys alimillimetrialueen ilmaisimilla Uraauurtavat uudet teknologiset lähestymistavat sekä millimetri- että alimillimetrialueella Antenni- ja RF MEMS -tekniikka mm-alueella Kuvauskohteiden näkyvyyden tarkastelu sähkömagneettisen simulaation keinoin
Ilmaisu (immunologiset ja DNA-pohjaiset teknologiat sekä näytteenotto- ja esikäsittely)	Mikrobiologiset tunnistusmenetelmät, ilmamikrobiologia, riskinarviointi sekä teollisuusprosessien hyvä tuntemus erityisesti mikrobiologisen turvallisuuden kannalta Tietoliikenne, anturiverkostot, terrorismin vastainen monitorointi Rekombinanttivasta-aineisiin perustuvien immunologisten pikamääritysmenetelmien kehittäminen Bioanturi ja mikrofluidistiikkaosaaminen Perusmolekyylibiologian tuntemus, hyvä ilmamikrobiologian osaaminen
Ilmaisu (tulipalon ilmaiseminen)	Paloilmaisimien toimintaperiaatteiden tunteminen Savun leviämisen mallintaminen
Hälytys-järjestelmät	Kiinteistöjen hälytysjärjestelmät, erityisesti kiinteistötiedon hyödyntäminen hälytysjärjestelmissä, pelastusajoneuvoon tietoa välittävät hälytysjärjestelmät
Fyysinen suojaus	
Rakenteellinen suojaus	Suodatusteknologiat ja riskianalyysit Pitkä kokemus paineaaltojen simuloinnissa ja teoreettisessa tarkastelussa Kokemusta myös tärähdyksen ja tärinän kestävyyden arvioinnista Palokokeet ja tulipalon mallinnus
Suojaus ilman mukana kulkeutuvilta CBR-agensseilta	Kemialliset hälytysjärjestelmät Ilmansuodattimien testaus ”normaaleilla” epäpuhtauksilla Uusien suodatinratkaisujen kehittäminen sekä kaasu- että hiukkasmaisia epäpuhtauksia vastaan Ilmansuodattimien ja iv-järjestelmien suojaaminen paineiskulta Mikrobiologinen näytteenotto ja analysointi ilmasta ja suodatinmateriaaleista, mikrobidiagnostiikan soveltaminen eri näytematriiseihin

VTT:n tavoitteena on lyhyellä tähtäimellä syventää valvontajärjestelmien ja -toiminnan tuntemusta sekä hankkia osaamista hälytys- ja vartiointitoiminnasta ja niiden tietojärjestelmistä. Tavoitteena on myös osallistua voimakkaasti EU:n tulevaan Security-ohjelmaan. Keskipitkällä aikavälillä tavoitteena on kehittää security-teknologiaa asiakkaiden ja julkisen vallan tarpeiden mukaisesti samoin kuin kehittää security-alan yritysten ja julkisten toimijoiden teknologioita ja toimintatapoja.

4. Elinkeinoelämän turvallisuuden varmistaminen

Tässä luvussa käsitellään elinkeinoelämän turvallisuuden varmistamista. Tarkasteltaviksi kohteiksi on valittu tuotannon ja palvelutoiminnan turvallisuus (4.1), kiinteistö- ja toimitilaturvallisuus (4.2) sekä sulautettujen järjestelmien tietoturva (4.3). Jokaisesta tarkastelukohteesta käydään läpi teknologiaperusta ja VTT:n nykyinen osaaminen sekä tavoite alueella.

4.1 Tuotannon ja palvelutoiminnan turvallisuus[25]

Aihealue kohdistuu niihin osaamisalueisiin ja teknologioihin, joilla teollisuus ja palvelutuotanto voivat ja pyrkivät varmistamaan oman toimintansa turvallisuuden ja jatkuvuuden tahallisia vahingontekoja vastaan.

Tarkasteltava teollisuus voi olla

- yhteiskunnan kannalta kriittistä (energian tuotanto, elintarviketeollisuus, verkottuneen tuotannon solmukohdat, rahaliikenne), johon kohdistuva vahinko aiheuttaa ongelmaa muualla yhteiskunnassa ja teollisuudessa
- turvallisuuskriittistä (ydinvoima, aseteollisuus, räjähdysaineteollisuus), jolle yhteiskunta on asettanut erityisvaatimuksia
- tavanomaista pääomavaltaista teollisuutta (metsäteollisuus, metalliteollisuus, elektroniikka, tietotekniikka, yms.), jossa mahdolliset taloudelliset menetykset ovat suuret.
- palvelutuotantoa (palvelulaitokset esimerkiksi vanhain- ja päiväkodit, kauppa, pankit, yms.), jolla on yhteiskunnallista merkitystä.

Aihepiiriin sisältyvät

- ihmisen tahallisen toiminnan seurauksena syntyvät turvallisuusriskit, niiden estäminen ja seurausten minimointi. Uhat voivat olla joko ulkoisia tai sisäisiä.
- tärkeiden kohteiden haavoittuvuutta aiheuttavat luonnonkatastrofit (myrskyt, tulvat)
- muualla tapahtuvien häiriöiden heijastusvaikutukset (terrorismi, pandemiat, tsunamit) teollisuuden toimintaan ja huoltovarmuuteen (mm. avainhenkilöriskit)
- tietoturvauhat
- yritysten toimintaan kohdistuvat uudet uhkat, jotka aiheutuvat esimerkiksi teollisuuden omien toimintatapojen ja teknologioiden kehittymisestä. Tällaisia ovat esimerkiksi ohjaus- ja turvallisuusjärjestelmien integroituminen, tuotteiden ja raaka-aineiden jäljitettävyys, tuotannon verkostoituminen ja globalisoituminen sekä uudet teknologiat.

[25] Veikko Rouhiainen, Ismo Ruohomäki, Seppo Enbom, Teuvo Uusitalo, Päivi Mikkonen ja Marinka Lanne, Laura Raaska & Gun Wirtanen kommentoineet

Aihepiiriin eivät liity: perinteinen yritysten liiketoiminnan riskienhallinta, tuotantojärjestelmien tekninen riskienhallinta, haitallisten tapahtumien pitkäaikaisvaikutukset liiketoimintaan ja alkutuotanto.

Teollisuuden nykyinen turvallisuuden hallinta jatkuu normaalisti kehittyen. Sen lisäksi tulevaisuudessa korostuvat security-asiat, jotka hyödyntävät osin samoja menetelmiä ja tekniikoita mitä käytetään tahattomien vahinkojen hallinnassa, mutta myös uusia lähestymistapoja ja teknisiä ratkaisuja tarvitaan. Safety- ja security-asioiden hallinta yhtenäistyy sekä yritysturvallisuuden johtamisen että kokonaisvaltaisen riskienhallinnan näkökulmasta.

4.1.1 Teknologiaperusta

Tuotannon ja palvelutoiminnan turvallisuuden varmistaminen on laaja osa-alue. Siihen liittyvät lähes kaikki julkaisussa käsiteltävät teknologiat. Sovellettavat teknologiat vaihtelevat toimialasta ja yrityksestä toiseen, mutta yleisesti ottaen ainakin seuraavat teknologiat ovat lyhyellä ajanjaksolla merkittäviä: tietoturvallisuus, kiinteistöteknologia (käsitellään tarkemmin seuraavassa luvussa), suojausteknologiat, riskianalyysit sekä riskien arviointi- ja hallintamenetelmät ja mikrobidiagnostiikka. Keskipitkällä ja pitkällä aikavälillä korostuu näiden teknologioiden soveltaminen käytäntöön. Kokonaisturvallisuuden hallinnassa lähtökohtana on safety-osaamisen ja kokemuksen soveltaminen security-alueelle (taulukko 17).

Taulukko 17. Tuotannon ja palvelutoiminnan turvaamisen teknologioiden kehitys.

Käytettävä teknologia	**Lyhyt**	**Keskipitkä**	**Pitkä**
Kokonaisturvallisuuden hallinta			
Riski-analyysi-menetelmät	Safety-osaamisen ja kokemuksen soveltaminen security-alueelle Security-aiheen integroiminen riskianalyysivälineisiin Tietoteknisten työvälineiden kehittäminen ja tarvekartoitus riski- ja haavoittuvuusanalyysimenetelmissä Riskien kvantifiointi ja datan saatavuus	Riski- ja haavoittuvuusanalyysimenetelmien kehittäminen Päätöksentekomallien kehittäminen Riskien kvantifioinnin kehittäminen Tilanteen reaaliaikainen seuranta	Tietotekniset apuvälineet riski- ja haavoittuvuusanalyysien tekoon ja riskien kvantifiointiin

Taulukko 17. Jatkuu ...

Tietoturvan hallinta	Auditointi- ja tietoturvavaatimusmäärittelypalvelut State-of-the-art firewall, antivirus, IDS/IPS, verkkomonitorointi (liikenne, QoS), tekninen tuki, standardit	Teknisten logien yhdistäminen (firewall, antivirus, IDS) Tietokannat, sääntölogiikat, riskianalyysimenetelmät	Kehittynyt verkkomonitorointi (”beyond IDS”), proaktiivinen mittaus Pattern recognition, sumea logiikka, oppivat algoritmit, Semantic Web, työkalut analyysiin
Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
RFID	RFID-tunnisteista ”nappi”-tyypissä on herkkä antenni ja siru on valettu epoksiin. Näin tunniste kestää kovaa kohtelua ja kemikaaleja. Kompakti pakkauskoko kuitenkin rajoittaa lukuetäisyyttä. Aktiivi ja passiivi RFID	Hierarkkiset tunnistusratkaisut, uudet toimintatavat, jotka hyödyntävät automaattista tunnistusta Painettavat saattomuistit, muutoin integroidut saattomuistit; NFC-teknologia integroitu matkapuhelimeen	Mukana tuotteiden tekoprosessissa ja edelleen kehittelyssä, Globaalit ratkaisut; saattomuistit tuotteen käyttöliittymänä
Anturiverkot (aktiivitagit)	Energian generointimenetelmien kehittäminen Lyhyen kantaman radiotekniikat Langattomat anturit, mikroanturit, bioanturit, antureiden sovellukset	Tagiverkko-teknologioiden kehittäminen Energiaomavaraiset tagit Anturiverkkotekniikat, mikroenergian generointitekniikat	Laajojen moniteknologisten tagijärjestelmien suunnittelu- ja hallintamenetelmät Laajojen tagiverkkojen hallintamenetelmät, uudet kommunikointitekniikat
Ilmaisu (detektio)	Kemiallisten agenssien detektio ilmanäytteiden otto ja esikäsittely Selvitys immunologisten C- ja B-detektiomenetelmien toimivuudesta. Rekombinanttivasta-aineteknologian etujen evaluointi ja hyödyntäminen C- ja B-menetelmien kehityksessä. Kehittää näytteenottoa ja PCR-pohjaisia menetelmiä haitallisten B-agenssien detektointiin.	Biologisten agenssien detektio ja analyysijärjestelmien kehittäminen Integroida näytteenotto ja esikäsittely osaksi analysointiprosessia. Tuottaa tietyille C- ja B-analyyteille rekombinanttivasta-aineet ja kehittää niiden avulla herkkää ja nopeaa pikatestiä. Bioanturi ja mikrofluidistiikan hyödyntäminen pikatesteissä. Mikrobitoimintojen detektointi (hajuntuotto, toksiinintuotto). Laajentaminen muihin näytematriiseihin	Biologisten agenssien detektion soveltaminen käytäntöön Integroituun mittajärjestelmään soveltuvan immunomenetelmän (esimerkiksi sirutekniikkaan perustuvan) kehittäminen. Molekyylibiologiset menetelmät uhkien kartoittamiseen ja niiden hallintaan. Mikrobitoimintojen perusteella toimivien menetelmien kehitys.

Taulukko 17. Jatkuu ...

Hahmontunnistus	Valittujen erityissovellusten arkkitehtuurit, SW- ja HW-työkalut Signaalin- ja kuvankäsittely, automaattinen henkilöntunnistus, tiedon louhinta, tilastotiede	Kehittynyt multimodaalinen biometrinen tunnistus, anturitiedon käyttö. Oleellisen piirretiedon valitsemista auttavat apuvälineet	Tiedustelutiedon (laajasti ymmärrettynä) analysointi ja uhkatilanteiden tunnistus. Kuvan tai näkymätiedon ymmärtäminen Ubi-antureita
Biometrinen henkilöntunnistus	Sormenjälkitunnistus, puhujan tunnistus, kasvojen tunnistus, tunnistus iiriksestä, käden tunnistus, allekirjoituksen tarkastus		
Tietoverkkojen ja -järjestelmien suojaus			
Tietoverkkojen suojaus	IP-teknologiat	Mobile-IP (v4 ja v6)	
Tietoturvamonitorointi	Olemassa olevat QoS-, verkon liikenne- ja IDS/IPS-toteutukset	Omat prototyypit (Beyond IDS)	Omat prototyypit (Beyond IDS)
Ohjelmistoalustat ja -arkkitehtuurit	Välitason ohjelmistokomponenttien hallintamekanismien kehittäminen Ohjelmistokomponenttimallit	Välitason ohjelmistokomponenttien hallintamekanismien kelpoistaminen Ohjelmistokomponentit, tietoturvatestaus	Turvalliset ja yksiselitteisesti tietoturvahallittavat välitason komponenttiarkkitehtuurit Ohjelmistokomponentit ja menetelmät
Verkko- ja Internet-tietoturva	Liikkuvuuden huomioonottaminen, verkkoriippumaton AAA/IDM, IPv4 pohjautuvia ratkaisuja. (Mobiili X, esimerkiksi VPN, FW). IDS/IPS, ohj. verkot (mobiilisuustuki, verkkokonteksti)	Verkon ja kommunikoivien systeemien tietoturvayhteistyö (ohjelmoitavat verkot, IDS/IPS), IPv6, IPsec rajoitetusti	Avainhallinta (hyvä ja yleiskäyttöinen) Autonominen tietoturvan hallinta, oppivat systeemit, mahdollisesti biologisista systeemeistä inspiraationsa saavat järjestelmät
Tietoturvatestaus	Codenomiconin robustnesstestaustyökalu	Muut työkalut	Laajempi valikoima työkaluja

4.1.2 VTT:n toiminta

Yrityksillä on tarpeita kokonaisvaltaiseen riskienhallintaan ja turvallisuusjohtamiseen. Yritystoiminta on monimutkaistunut, ja siihen liittyy yhä moninaisempia riskejä, joten myös riskien hallintamenetelmien on palveltava laajemmin yritysturvallisuuden eri osa-alueita. Päällekkäistä työtä on mahdollisuus vähentää integroimalla security- ja tietoturva-asioita nykyisiin hallintamenetelmiin. Ennaltaehkäisevä security-asioiden suunnittelu tulee yrityksille myöhemmässä vaiheessa toteutettavia security-ratkaisuja halvemmaksi. Tuotantoprosessien suojaaminen on oleellista erityisesti elintarviketeollisuudessa.

Suomessa saatetaan olla joissain asioissa yliturvallisia. Toisaalta teollisuuden riskienhallintatoimenpiteet on mahdollisesti kohdennettu riittämättömästi ja niiden ylläpidon kustannusvaikutuksia ei ole perusteellisesti selvitetty. Puutteita on varmasti myös riskienhallintajärjestelmän ylläpidossa. Toiminnan koordinointi yritystasolla on vielä hajallaan, ja yritysturvallisuuden painopistealueet on valittu lähinnä perinteitä noudattaen. Synergiaeduista on vielä vähän kokemusta. Turvallisuustason toteutumista tulisi mitata paremmin, ja painopistealueiden löytämisen tulisi perustua analyyseihin.

Yritysten liiketoiminnan riippuvuus tietoturvallisuuden hallinnasta on merkittävä, ja haavoittuvuus kasvaa esimerkiksi vahingontekojen yleistymisen myötä. Kansainvälistyminen ja verkostoituminen tuovat mukanaan sekä tietoturvallisuuteen liittyviä vaatimuksia että uhkakuvia. Tietotekniikan ja elektroniikan (ICT:n) yleistyminen kaikissa prosesseissa ja järjestelmissä lisää riskien tunnistamisen ja hallinnan tarpeita nimenomaan käyttövarmuuden ja tietoturvallisuuden näkökulmasta.

Tietoturvariskit toteutuessaan voivat viedä dramaattisesti pohjan koko yrityksen liiketoiminnalta. On oleellista, että yritysten johto on sitoutunut tietoturvanhallintaan ja osaa määritellä yritykselle soveltuvat tietoturvapolitiikat. Tietoturvan hallintaprosessin täytyy integroitua muihin yrityksen liiketoimintaprosesseihin kiinteästi. Koko yrityksen ja sen yhteistyökumppaneiden henkilöstön tietoturvatietoisuuden nostamiseen on panostettava.

Tuotannon ja palvelutoiminnan turvallisuuden varmistaminen vaatii laaja-alaista teknologista osaamista. Keskeisiä osaamisalueita VTT:n kannalta ovat esimerkiksi kokonaisturvallisuuden hallinta sekä tietoverkkojen ja -järjestelmien suojaus. Lisäksi erilaiset tunnistukseen, paikannukseen ja tiedonsiirtoon liittyvät osaamiset ovat merkittäviä. Tulipaloista yli 30 % on tahallisesti sytytettyjä, joten ne on otettava huomioon myös security-asiana (taulukko 18).

Taulukko 18. VTT:n nykyinen osaaminen tuotannon ja palvelutoiminnan turvaamisessa.

Fokusalue	Vahvuudet, mikä osataan
Kokonaisturvallisuuden hallinta	
Riski-analyysi-menetelmät	Pitkäaikainen osaaminen ja kokemus riskianalyysistä, riskinarvioinnista ja riskienhallintakeinoista PK-yritysten riskienhallintaosaaminen Kvalitatiivinen riskien arviointi Uhkien ja vaarojen tunnistaminen. Vahva mikrobiologinen osaaminen teollisuusprosessien ja tuotteiden turvallisuuden analysoinnista ja hallinnasta
Tieto-turvan hallinta	Tietoturvanhallintaprosessien ymmärtäminen Laaja-alainen monitorointi- ja mittausosaaminen sekä state-of-the-art-näkemys Tietoturvavaatimusten määrittely Tietoturvamonitorointi; testausympäristö kehitteillä
Paloturval-lisuus	Palon leviämisen simulointi ja rajoittaminen, sammutustekniikat, palonilmaisu, tuotteiden ja järjestelmien palonkestävyyden arviointi
Ilmaisu, tunnistus, paikannus ja tiedonsiirto	
RFID	Tietoturvaosaaminen, turvauhkien tunnistus ja ennaltaehkäisy. Osataan erilaisten tagien printtausta ja tuotantoympäristöjä Olemassa on RFID-esiselvityksiä ja -pilotteja: aktiivi ja passiivi RFID, langaton ratkaisu, toimivia logistiikkasovelluksia olemassa, kulunvalvonta vahvin alue, bussikortit, tuotannon ohjaus, auton avaimet, RFID-lukija Symbian puhelimessa
Anturi-verkot (aktiivi-tagit)	Laajaa osaamista tagien vaatimissa tekniikoissa: RF-tekniikat, lyhyen kantaman radiotekniikat, mikroenergian generointi, verkkotekniikat, anturitekniikat, liittyminen päätelaitteisiin ja taustajärjestelmiin Tagiverkkojen tutkimus ja kehittäminen käynnissä. Energian generointimenetelmiä kehitetty tai kehitteillä
Ilmaisu (immunologiset ja DNA-pohjaiset teknologiat sekä näyt-teenotto- ja esikäsittely)	Mikrobiologiset tunnistusmenetelmät, ilmamikrobiologia, riskinarviointi sekä teollisuusprosessien hyvä tuntemus erityisesti mikrobiologisen turvallisuuden kannalta Tietoliikenne, anturiverkostot, terrorismin vastainen monitorointi Rekombinanttivasta-aineisiin perustuvien immunologisten pikamääritysmenetelmien kehittäminen Bioanturi ja mikrofluidistiikkaosaaminen Perusmolekyylibiologian tuntemus, hyvä ilmamikrobiologian osaaminen

Taulukko 18. jatkuu ...

Hahmontunnistus	Kunnonvalvonnan tehostaminen kulumishiukkasten tietokoneavusteisella tunnistamisella neuro-sumeita menetelmiä käyttäen Tietokonenäön käyttö 3D-mittaukseen ja -ohjaukseen: senkan ja konvertterin kulumisen mittaus, laivanrakennuksen sovellukset Lääketieteellinen hahmontunnistus, konenäkö
Biometrinen henkilöntunnistus	Puhekommunikaatio automaatio- ja tietoliikennesovelluksissa: audioanalyysi, puheen ja muun erottaminen audiosignaalista, puhujan vaihtumisen havaitseminen, puhujan tunnistus, sormenjälkeen perustuva tunnistus, kävelijän tunnistaminen kännykkään lisätyillä kiihtyvyysantureilla VTT on vetänyt kansallisen projektin (hyvinvointi, terveydenhuolto, sähköinen kaupankäynti)
Tietoverkkojen ja -järjestelmien suojaus	
Tietoturvamonitorointi	Ohjelmoitujen verkkojen soveltaminen mobiilitietoturvaan Mobiilisovellusten käyttäjäntunnistusmenetelmät sekä sovellustason tietoliikenteen tietoturvamonitorointi Maksupalvelutietämys (operaattoripohjaiset maksupalvelut)
Tunkeilunesto yms.	Identiteetti-informaation hallinta Tietoverkko-osaaminen mobiili ja kiinteiden verkkojen puolella monella kerroksella Tietoturvametriikkaosaaminen Tietokantaosaaminen
Ohjelmistoalustat ja -arkkitehtuurit	Content protection/copyright osaamista Osataan ohjelmistoarkkitehtuureja, ohjelmistoalustoja, tietoturvaratkaisuja ja niiden arviointia
Verkko- ja Internet-tietoturva	Tietoturvaprotokollat (authentication, authorisation, accounting) Vahva (Internet-) verkko-osaaminen, myös ”avant-garde”-rintamalla Mobiilitietoturva, yleinen verkonhallinta
Tietoturvatestaus	Tietoturvatavoitteiden määrittely Laaja kokemus mobiilimaailman päätelaitteiden, palvelujen ja verkkojen tietoturvasta Testausosaaminen (tietoturvatestaus) Valmiit kontaktit kaupallisiin testaajiin

VTT:n tavoitteena on toimia Suomessa ja kansainvälisesti toimivien yritysten kumppanina, tarjoten palveluja ja teknisiä ratkaisuja, jotka perustuvat vahvaan osaamiseen esimerkiksi riskienarvioinnin ja -hallinnan, elintarvike- ja pakkausteollisuuden tuoteturvallisuuden varmistavan mikrobidiagnostiikan ja tietoturvallisuuden alueilla. Tavoitteena

on olla security-aihepiiriin liittyvien perusteknologioiden ennakoija, sovellusten ja toimintatapojen kehittäjä ja security-alan perustutkimuksen koordinoija Suomessa.

4.2 Kiinteistö- ja toimitilaturvallisuus[26]

Kiinteistö- ja toimitilaturvallisuudessa tarkastellaan lähinnä normaalioloista poikkeavia tilanteita. Aihealueeseen katsotaan kuuluvaksi seuraavat osa-alueet:

1. Passiiviset tai rakenteelliset turvallisuusratkaisut
   - rakenteiden turvallisuus (rakenteiden kesto)
   - rakenteelliset estot (mm. autopommit, EMP- ja EMC-suojaus), paloturvallisuus (palokaasut).

2. Aktiivinen turvallisuus (turvallisuuden hallinta toiminnallisilla laitteilla)
   - hälytysjärjestelmät (kulunvalvonta-, rikosilmoitus-, videovalvonta-, turvapuhelin-, hälytysten siirto sekä yhdistetyt ja sulautetut hälytysjärjestelmät), savu-, kaasu- ym. ilmaisimet ja hälyttimet (myös mikrobiologiset), automaattisesti toimivat suojalaitteet (sammutusjärjestelmät, suodattimet, palopellit, paineistusjärjestelmät, paineovet, sulut, etc.), valvomojärjestelmät, pelastus- ja turvahenkilöiden tukijärjestelmät sekä niiden yhteensovittaminen
   - turvallisuusjärjestelmien integrointi ja yhteys kiinteistöjärjestelmiin sekä vartiointiliikkeiden hälytysvalvomoihin ja julkishallinnon hätäkeskusjärjestelmiin
   - normaalioloista poikkeavien tilanteiden havainnointi ja indikointi (mm. terrorismi).

3. Kiinteistön elinkaaren turvallisuus (suunnittelu, rakentaminen, käyttö, ylläpito, kehittäminen ja turvallisuusjohtaminen)
   - organisaation käytännön toiminta turvaratkaisujen käytössä ja ylläpidossa
   - tiedonhallinta
   - strateginen, taktinen ja operatiivinen turvallisuussuunnittelu ja -johtaminen (luokitukset otetaan huomioon suunnitteluvaiheessa).

[26] Veijo Lappalainen, Veikko Rouhiainen, Ismo Ruohomäki, Teuvo Uusitalo, Päivi Mikkonen, Seppo Engblom ja Marinka Lanne, Laura Raaska & Gun Wirtanen kommentoineet

4. Turvallisuuden hallinnan ja johtamisen menetelmät

- riskien analysointi, arviointi ja hallinta sekä katselmoinnit, todentaminen, skenaariot
- turvallisuustiedon hallinta ja eri toimijoiden yhteistyö
- palokunnan toiminta
- turvallisuusjohtamisen menetelmät ja mallit.

Yritysten tietoturvanhallintaan liittyy olennaisesti myös kriittisten informaatiojärjestelmien fyysinen suojaus. IT-järjestelmän keskeiset osat sekä varmuuskopiointilaitteistojen sijaintipaikka, huolto ja hallinta täytyy suunnitella tarkasti. Liiketoiminnan jatkuvuussuunnitelma ja katastrofista toipumissuunnitelma pureutuvat myös fyysisen turvallisuuden tekijöihin osana tietoturvallisuutta. Tässä raportissa ei käsitellä tätä tietoturvan ulottuvuutta tarkemmin.

Kiinteistö- ja toimitilaturvallisuuden ulkopuolelle on rajattu olosuhteiden terveellisyys (mm. sisäilma) sekä rakennusten normaali turvallisuus (liikkumisen turvallisuus, kone- ja sähköturvallisuus, räjähdysvaaralliset tilat, kaasuvuodot, tulvat tai suuret vesivuodot erityisesti maanalaisissa tiloissa).

Security-asiat on otettu huomioon teollisuusrakennusten ja tilojen suunnittelussa, rakentamisessa ja käytössä. Tilannetietoisuutta ja ennakoivuutta kehitetään esimerkiksi erilaisten mittarien ja indikaattorien avulla (mm. älytalot). Erityiskohteet, kuten sairaalat, vanhainkodit, kauppakeskukset, yms., toimivat edelläkävijäalueina. Kiinteistöjen hälytysjärjestelmiä ja kiinteistötietojärjestelmiä integroidaan erillisverkoissa toimiviin hätäkeskus-, pelastuslaitos- ja poliisitoimen järjestelmiin. Näiden integroituja reaaliaikaisia mobiileja käyttöliittymiä kehitetään operatiiviselle henkilöstölle. Esimerkkinä voisi olla hälytysajoneuvoon raportoiva (ihmiset, vaaralliset aineet) kiinteistö.

4.2.1 Teknologiaperusta

Merkittäviä kiinteistö- ja toimitilaturvallisuuteen liittyviä teknologioita ovat passiiviset tai rakenteelliset turvallisuusratkaisut sekä erilaiset hälytys- ja monitorointijärjestelmät ja näiden integrointi ja yhteys kiinteistöjärjestelmiin, hälytysvalvomoihin ja julkishallinnon hätäkeskusjärjestelmiin. Kiinteistön kokonaisturvallisuuden hallinnassa ja johtamisessa korostuvat riskien analysointi, arviointi ja hallinta sekä katselmoinnit, todentaminen, skenaariot, turvallisuustiedon hallinta ja eri toimijoiden yhteistyö sekä turvallisuusjohtamisen menetelmät ja mallit. Turvallisuuden kehittämisen lähtökohtana on kiinteistön koko elinkaaren kattaminen (suunnittelu, rakentaminen, käyttö, ylläpito, kehittäminen ja turvallisuusjohtaminen) (taulukko 19).

Taulukko 19. Kiinteistö- ja toimitilaturvallisuuden teknologioiden kehitys.

Käytettävä teknologia	Lyhyt	Keskipitkä	Pitkä
Kokonaisturvallisuuden hallinta			
Riski-analyysi-menetelmät	Riski- ja haavoittuvuusanalyysimenetelmien kehittäminen ja tarvekartoitus Riskien kvantifiointiin tarvittavan datan saatavuuden kehittäminen	Riski- ja haavoittuvuus-analyysimenetelmien tietoteknisten työvälineiden kehittäminen Päätöksentekomallien kehittäminen Riskien kvantifioinnin kehittäminen Tilanteen reaaliaikainen seuranta	Tietotekniset apuvälineet riski- ja haavoittuvuusanalyysien tekoon ja riskien kvantifiointiin
Hälytys-järjestelmät ja monitorointi	Kulunvalvonta, paikannus-teknologiat, ilman puhdistustekniikka, anturi-teknologia	Tilannetietoisuus (sumeat teknologiat) + edelliset	Tunnistusteknologiat, anturi- tai ilmaisinteknologiat, uudet ICT- ja mobiiliteknologiat
Ilmaisu, tunnistus, paikannus ja tiedonsiirto			
RFID	Aktiivi ja passiivi RFID	Hierarkkiset tunnistus-ratkaisut Painettavat saattomuistit, muutoin integroidut saattomuistit	Globaalit ratkaisut; saattomuistin tuotteen käyttöliittymänä
Anturi-verkot (aktiivi-tagit)	Lyhyen kantaman radio-tekniikat Langattomat anturit, mikroanturit, bioanturit, antureiden sovellukset	Anturiverkkotekniikat, mikroenergian generointitekniikat, energia-omavaraiset tagit	Laajojen moniteknologisten tagijärjestelmien suunnittelu- ja hallintamenetelmät Laajojen tagiverkkojen hallintamenetelmät, uudet kommunikointitekniikat
Hahmon-tunnistus	Parannetaan opetettavien luokittelu- ja tunnistus-järjestelmien helppo-käyttöisyyttä ja havainnollisuutta Signaalin- ja kuvankäsittely, automaattinen henkilön-tunnistus, tiedon louhinta, tilastotiede	Kehittynyt multimodaalinen biometrinen tunnistus, anturitiedon käyttö Oleellisen piirretiedon valitsemista auttavat apuvälineet	Tiedustelutiedon (laajasti ymmärrettynä) analysointi ja uhkatilanteiden tunnistus. Kuvan tai näkymätiedon ymmärtäminen Ubi-antureita
Biometrinen henkilöntunnistus	Sormenjälkitunnistus, puhujan tunnistus, kasvojen tunnistus, tunnistus iiriksestä, käden tunnistus	Mobiilimaksaminen ja muut transaktiot	Älykoti ja -toimisto

Taulukko 19. Jatkuu ...

Tietoverkkojen ja -järjestelmien suojaus			
Tieto-verkkojen suojaus	IP-teknologiat	Mobile-IP (v4 ja v6)	
Fyysinen suojaus			
Raken-teellinen suojaus	Kehittää rakenteellisia ratkaisuja tilojen suojaamiseen EMP- ja HPM-iskuilta	Paineaaltojen simulointi	Luoda järjestelmä, jolla viranomaiset tai rakennuttaja voi halutessaan helposti ottaa huomioon turvallisuusseikat ja rakennuttaa niin halutessaan turvallisen rakennuksen
Suojaus ilman mukana kulkeutu-vilta CBR-agensseilta	CBR-agenssien detektointi Ulko- ja väliseinäratkaisujen tiivistäminen Antimikrobisten ominai-suuksien liittäminen suodatinteknologiaan ja ilmanvaihtojärjestelmiin Hiukkassuodattimet: sähköisesti tehostettu hiukkassuodatin Kaasusuodattimet: uudet kuitukangasaktiivihiili-materiaalit, aktiivihiilen impregnoinnin vanhenemisreaktioiden parempi hallinta	Hiukkassuodattimet: nanokuidut Kaasusuodattimet: regeneratiiviset suodatinratkaisut, uudet impregnointitekniikat Mikrobidiagnostiikan kehittäminen ja soveltaminen kohdematriiseihin ja kohdemikrobeihin	Kaasusuodattimet: UV+fotokatalyysi, molekyyliseula, katalyyttinen hapetus, syklinen suodatus Mikrobidiagnostiikan kehittäminen ja soveltaminen kohdematriiseihin ja kohdemikrobeihin

4.2.2 VTT:n toiminta

Toimitilaturvallisuuden hallinta on oleellista mm. rikosturvallisuuden ja tietoturvallisuuden varmistamiseksi. Tietyissä kohteissa myös varautuminen terrorismin uhkaan on tullut tärkeäksi. Nykyiset valvontajärjestelmät ovat integroitumassa. Yritykset toimivat entistä useammin teollisuusalueilla, joissa toimii useita yrityksiä. Teollisuutta myös keskitetään tietyille alueille.

Yksintyöskentely lisääntyy (mm. terveyskeskukset, vartiointi, teollisuuden valvontatehtävät). Henkilökohtaiset turvalaitteet on integroitu kiinteistön turvajärjestelmiin.

Tulevaisuuden turvallisuusvaatimusten toteuttaminen edellyttää turvallisuuden kokonaishallintaa eri hierarkiatasoilla kiinteistön koko elinkaaren ajan. Turvallisuusjohtamisesta kehittyy yritysten ydintoiminta. Riskienhallintaa yritysten kesken tarvitaan mm. teollisuuspuistoissa.

Kiinteistö- ja toimitilaturvallisuuden keskeisin osaaminen liittyy toisaalta fyysiseen suojaukseen, toisin sanoen rakenteelliseen suojaukseen ja suojaukseen ilman mukana kulkeutuvilta CBR-agensseilta, ja toisaalta hahmontunnistukseen ja biometriseen henkilöntunnistukseen. Lisäksi riskianalyysimenetelmien hallinta ja hälytys- ja monitorointijärjestelmiin liittyvä osaaminen sekä tietoverkkojen ja -järjestelmien suojaus ovat olennaisia osaamisalueita kiinteistö- ja toimitilaturvallisuuden kannalta (taulukko 20).

Tietoturvallisuuden hallinnan kannalta toimitilaturvallisuudella on suuri merkitys. VTT:llä on aihepiiriin liittyvää osaamista, jota voidaan soveltaa esimerkiksi tietoturvaauditoinneissa.

Taulukko 20. VTT:n nykyinen osaaminen kiinteistö- ja toimitilaturvallisuuden kehittämisessä.

Fokusalue	Vahvuudet, mikä osataan
Kokonaisturvallisuuden hallinta	
Riskianalyysi-menetelmät	Perinteinen riskianalyysiosaaminen Kvalitatiivinen riskien arviointi Uhkien ja vaarojen tunnistaminen Vahva mikrobiologinen osaaminen teollisuusprosessien ja tuotteiden turvallisuuden analysoinnista ja hallinnasta
Hälytys-järjestelmät ja monitorointi	Rakenteiden kestävyys, turvajärjestelmät, ilmaisin- ja hälytysjärjestelmät, rakennusautomaatio- ja kiinteistötietojärjestelmät, rakennusten tietojärjestelmien integrointi, pelastusautoon raportoivan kiinteistön teknologiat Paikannusmetodiikat ja -teknologiat Henkilöstölogistiikka
Ilmaisu, tunnistus, paikannus ja tiedonsiirto	
Hahmon-tunnistus	Kunnonvalvonnan tehostaminen kulumishiukkasten tietokoneavusteisella tunnistamisella neuro-sumeita menetelmiä käyttäen Tietokonenäön käyttö 3D-mittaukseen ja ohjaukseen: senkan ja konvertterin kulumisen mittaus, laivanrakennuksen sovellukset Lääketieteellinen hahmontunnistus, konenäkö
Biometrinen henkilön-tunnistus	VTT soveltanut sormenjälkitunnistusta BioSec (Biometrics and Security) -projektissa Finnairin ja sisäasiainministeriön kanssa Puhekommunikaatio automaatio- ja tietoliikennesovelluksissa: audioanalyysi, puheen ja muun erottaminen audiosignaalista, puhujan vaihtumisen havaitseminen, puhujan tunnistus, sormenjälkeen perustuva tunnistus, kävelijän tunnistaminen kännykkään lisätyillä kiihtyvyysantureilla
Fyysinen suojaus	
Rakenteellinen suojaus	Pitkä kokemus paineaaltojen simuloinnissa ja teoreettisessa tarkastelussa Kokemusta myös tärähdyksen ja tärinän kestävyyden arvioinnista Palokokeet ja tulipalon mallinnus
Suojaus ilman mukana kulkeutuvilta CBR-agensseilta	Kiinteistöjärjestelmien tuntemus (mm. ilmastointi) Kemikaalien tuntemus (antimikrobiaaliset pinnoitteet ja materiaalit, terveellinen sisäilma) Ilmansuodattimien testaus ”normaaleilla” epäpuhtauksilla ja simulanteilla, uusien suodatinratkaisujen kehittäminen sekä kaasu- että hiukkasmaisia epäpuhtauksia vastaan Ilmansuodattimien ja iv-järjestelmien suojaaminen paineiskuilta Mikrobiologinen näytteenotto ja analysointi ilmasta ja suodatinmateriaaleista, mikrobidiagnostiikan soveltaminen eri näytematriiseihin

VTT:n tavoitteena on kehittää toimitilojen riskianalyysi- ja turvallisuusjohtamisen menetelmiä sekä uusia suojaus- ja torjuntateknologioita. Näitä ovat esimerkiksi suojaamisrakenteet ja -teknologiat, suodattimet ja detektorit. Lisäksi tavoitteena on kehittää riskien hallintakonsepteja ja taloudellisten vaikutusten arviointia, esimerkiksi riskin muuttamista liiketoimintamittareilla mitattavaksi (due diligence), sekä hälytysjärjestelmiä, esimerkiksi hälytysajoneuvoon raportoivia järjestelmiä.

4.3 Tuotteiden ja järjestelmien tietoturva

Tuotteiden tietoturvan hallinta on ehkä suurin ja merkittävin yksittäinen tietoturvan sovellusalue VTT:n tietoturvatutkimuksen kannalta. Tuotteiden ja järjestelmien tietoturva- ja ohjelmistoarkkitehtuuriratkaisut ovat keskeisessä roolissa. Sulautetuilla järjestelmillä tarkoitetaan tuotteita, joiden ohjelmisto-osa on sulautettu itse laitteeseen.

Tässä esityksessä keskitytään esimerkkinä erityisesti kahden sulautetun järjestelmän tietoturvaan: mobiililaitteisiin ja digi-TV:n palveluihin. Mobiililaitteilla tarkoitetaan kännyköitä, PDA-laitteita ja muita päätelaitteita, joihin liittyy mobiilioperaattorin tarjoama yhteys. Mobiililaitteiden tietoturva-arkkitehtuureilla tarkoitetaan niitä ohjelmistoarkkitehtuuri-, ohjelmistokomponentti-, protokolla- ja ohjelmistoalustaratkaisuja, joiden avulla toteutetaan tietoturvan hallinta mobiililaitteissa.

Digi-TV:n palveluilla tarkoitetaan (1) broadcast-tyyppisiä sisällöntuotannon tuotteita, (2) interaktiivisia palveluja jotka käyttävät järjestelmän paluukanavaa. Digi-TV:n tietoturvalla tarkoitetaan (1) digi-TV:n tuotteisiin liittyvää sisällönsuojausta, (2) Vastaanottimen paikallisten resurssien ja sovellusalustan (esimerkiksi MHP) tietoturvan hallintaa, (3) paluukanavaan liittyvää (pääasiassa IP-maailman) tietoturvan hallintaa ja (4) Lähetyspään ja -verkon tietoturvan hallintaa.[27]

4.3.1 Teknologiaperusta

Tuotteiden ja järjestelmien tietoturvan hallinta perustuu usein tietoturvaratkaisuihin jotka ovat sisäänrakennettuja tietoturva-arkkitehtuureihin, mm. välitason ohjelmistokomponentteihin ja -alustoihin. Tällaisia ohjelmistoalustoja ja -arkkitehtuureja ovat lyhyellä aikavälillä mm. Symbian + IP (mobiilit päätelaitteet), Java (sulautetut järjestelmät) ja MHP1.0.x-ympäristö (digi-TV). Keskipitkällä ja pitkällä aikavälillä mobiileissa päätelaitteissa ja sulautetuissa järjestelmissä korostuu edellisten lisäksi myös Linux. Digi-

[27] Reijo Savola, Jarkko Holappa; aiheeseen liittyy selvitys Jarkko Holappa et al. Digi-TV:n tietoturvauhat ja ratkaisut palvelunkehittäjän näkökulmasta). Tilaaja on liikenne- ja viestintäministeriö. 83 s. 2005.

TV-teknologioissa uusi tietoturvan haaste keskipitkällä aikavälillä ovat paluukanavan kautta ladattavat ja paluukanavaa hyödyntävät sovellukset (taulukko 21).

Taulukko 21. Sulautettujen järjestelmien tietoturvan kehitys.

Käytettävä teknologia	**Lyhyt**	**Keskipitkä**	**Pitkä**
Kokonaisturvallisuuden hallinta			
Tietoturvan hallinta	Auditointi- ja tietoturva-määrittelypalvelut State-of-the-art firewall, antivirus, IDS/IPS, verkkomonitorointi (liikenne, QoS), tekninen tuki, standardit	Teknisten logien yhdistäminen (firewall, antivirus, IDS) Tietokannat, sääntölogiikat, riskianalyysimenetelmät	Kehittynyt verkko-monitorointi (”beyond IDS”), proaktiivinen mittaus Pattern recognition, sumea logiikka, oppivat algoritmit, Semantic Web, työkalut analyysiin
Tietoverkkojen ja -järjestelmien suojaus			
Tieto-verkkojen suojaus	IP-teknologiat	Mobile-IP (v4 ja v6)	
Ohjelmisto-alustat ja -arkki-tehtuurit	Symbian + IP (mobiilit päätelaitteet), Java (sulautetut järjestelmät) MHP1.0.x-ympäristö, DVB-(C/S/T/H/IP)	Symbian + Linux + IP (mobiilit päätelaitteet), Java + Linux (sulautetut järjestelmät) MHP1.1, paluukanavan kautta ladattavat ja paluu-kanavaa hyödyntävät sovellukset, lähetyspään teknologiat	Symbian + Linux + IP + muut (mobiilit päätelaitteet ja sulautetut järjestelmät) Koko Digi-TV-ketju
Verkko- ja Internet-tietoturva	Best Practices, liikkuvuuden huomioonottaminen, verkkoriippumaton AAA/IDM, IPv4:ään poh-jautuvia ratkaisuja. (Mobiili X, esimerkiksi VPN, FW). IDS/IPS, ohjelmoitavat verkot (mobiilisuustuki, verkkokonteksti)	Verkon ja kommunikoi-vien systeemien tietotur-vayhteistyö (ohjelmoitavat verkot, IDS/IPS), IPv6, IPsec rajoitetusti Ohjelmoitavat verkot (”Mark II”): hallinnan joustava reagoiminen eri tilanteisiin	Avainhallinta (hyvä ja yleiskäyttöinen) Autonominen tieto-turvan hallinta, oppivat systeemit, mahdolliset biologisista systeemeistä inspiraationsa saavat järjestelmät
Tietoturva-testaus	Robustness-testaustyökalut, tietoturva-testaustyökalut ja yleiset testaustyökalut	Todennettu tietoturva-testausprosessi, joka käyttää työkaluja	Jatkuvasti kehittyvä ja monipuolinen tietoturva-testausprosessi ja työkaluvalikoima

4.3.2 VTT:n toiminta

Sulautettujen järjestelmien tietoturvan keskeisin osaaminen liittyy ohjelmistoalustoihin ja -arkkitehtuureihin sekä tietoturvatestaukseen. Myös yleisempi verkko- ja Internet-tietoturvan osaaminen on merkittävää sulautettujen järjestelmien toiminnan turvaamisessa (taulukko 22).

Taulukko 22. VTT:n nykyinen osaaminen sulautettujen järjestelmien tietoturvassa.

Fokusalue	**Vahvuudet, mikä osataan**
Kokonaisturvallisuuden hallinta	
Tietoturvan hallinta	Tietoturvanhallintaprosessien osaaminen, metriikoiden kehittäminen auditointia ja monitorointia varten, uhka-analyysit, tietoturvavaatimusten määrittely Tietoturvamonitorointitestausympäristö kehitteillä
Tietoverkkojen ja -järjestelmien suojaus	
Tietoverkkojen ja -järjestelmien suojaus	Sulautettujen tietoliikennejärjestelmien toteuttaminen sekä sulautettujen järjestelmien tietoturvallinen välitason ohjelmistokerros Riippuvuussuhdeanalyysi Tietoturvatavoitteiden määrittely
Ohjelmistoalustat ja -arkkitehtuurit	Sulautettujen järjestelmien tietoturva-arkkitehtuurien ja alustojen toteutusosaaminen Digi-TV-laiteosaaminen Mobiililaitteiden arkkitehtuurien ja alustojen toteutusosaaminen. sisällönsuojausosaaminen
Verkko- ja Internet-tietoturva	Tietoturvaprotokollat (authentication, authorisation, accounting) Vahva (Internet-) verkko-osaaminen, myös ”Avant-garde”-rintamalla, ohjelmoidut verkot Mobiilitietoturva, yleinen verkonhallinta Identiteetti-informaation hallinta
Tietoturvatestaus	Vahvaa osaamista testauksessa ja tietoturvassa VTT:n tietoturvatiimeissä, valmiit kontaktit kaupallisiin testaajiin

VTT:n tavoitteena on olla vahva osaaja tietoturva-arkkitehtuuriasioissa. Digi-TV:n osalta tavoitteena on hallita tietoturva koko arvoverkon osalta (päätelaite, lähetysverkko, head-end). Pidemmällä ajanjaksolla tavoitteena on lisätä osaamista tietoturvatestauksessa.

5. Yhteenveto

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaaminen on noussut Euroopassa merkittäväksi haasteeksi. EU:n asiantuntijaryhmä on todennut, että teknologia yksin ei voi taata turvallisuutta, mutta turvallisuus ilman teknologian tukea on mahdotonta. Alueella on suuri tutkimuspotentiaali, koska turvallisuuden parantamiseen tähtäävien tuotteiden ja järjestelmien kehittäminen on vasta käynnistynyt. Uusille innovaatioille on vielä tilaa ja niitä tarvitaan.

Turvallisuutta takaavien tuotteiden ja järjestelmien parantaminen edellyttää teknologioiden kehittämistä ja yhdistämistä sekä laaja-alaista soveltamista. Tämä Security-tutkimuksen roadmap on syntynyt tästä lähtökohdasta. Roadmap keskittyy erityisesti seuraaviin panostusalueisiin: yhteiskunnan järjestelmien turvaaminen, elinkeinoelämän turvallisuuden varmistaminen sekä turvateollisuuden teknologiat ja palvelut. Julkaisussa tunnistetaan yhteiskunnan ja elinkeinoelämän lähivuosien kehitysnäkymistä lähtien VTT:n ja EU:n Security-tutkimuksen kannalta keskeiset VTT:n osaamisalueet ja niiden antamat mahdollisuudet sekä tehdään suunnitelmat uuden osaamisen kehittämiseksi. Työn yhtenä tavoitteena on antaa lähtökohta tietoturvatutkimuksen koordinoinnille ja yhteistyön kehittämiselle VTT:n muun turvallisuustutkimuksen kanssa.

VTT:n kannalta keskeisiä turvateollisuuden teknologioiden sovellusalueita ovat energiaverkostot, tietoliikenneverkot, vesihuolto, liikenne ja kuljetukset, ihmisten suojaaminen, tuotannon ja palvelutoiminnan turvallisuus, kiinteistö- ja toimitilaturvallisuus sekä tuotteiden ja järjestelmien tietoturva. Sovellusalueittain jaoteltuna raportin keskeisiä havaintoja esitellään seuraavassa.

Energiaverkostot

Merkittäviä energiaverkostojen toiminnan varmistamiseen liittyviä teknologioita ovat erilaiset kokonaisturvallisuuteen liittyvät varautumissuunnitelmat sekä yleisesti hajautetun energiantuotannon lisääminen ja uudet rakenneratkaisut.

Energiaverkostojen turvaamisen keskeisin osaaminen liittyy riskianalyysimenetelmien ja tietoturvan hallintaan. Lisäksi esimerkiksi uhkien ja häiriöiden ilmaisuun (detektioon) liittyvä teknologinen osaaminen on merkittävää energiaverkostojen toiminnan turvaamisen kannalta. Tietoturvassa korostuvat tunkeilunesto sekä tietoverkkojen ja -järjestelmien suojaus.

Tietoliikenneverkot

Merkittäviä tietoliikenneverkkojen toiminnan varmistamiseen liittyviä teknologioita ovat lyhyellä tähtäimellä turvallinen välitason ohjelmistokerros, yksinkertaistettu ja robusti avaintenhallinta sekä ohjelmoitavat verkot. Keskipitkällä aikavälillä Internetin toimivuuden vaatimukset korostuvat ja sen kehittämiseen tarvitaan useita teknologioita: mm. automaattinen ja autonominen, politiikkapohjainen verkkotietoturvahallinta, ohjelmoitavat verkot, luotettavat komponentit, kontekstin hyväksikäyttö ja overlay-tietoturva. Tietoturvan mittaamisen ja monitoroinnin merkitys korostuu.

Tietoliikenneverkkojen turvaamisen keskeisin osaaminen liittyy tietoturvan hallintaan sekä luonnollisesti itse tietoverkkojen ja -järjestelmien suojaukseen. Myös anturiverkkoihin ja biometriseen henkilöntunnistukseen liittyvästä osaamisesta on hyötyä tietoliikenneverkkojen toiminnan turvaamisessa.

Vesihuolto

Merkittäviä vesihuollon toiminnan varmistamiseen liittyviä teknologioita ovat kokonaisturvallisuuteen liittyvänä vesilaitosten tuoteturvallisuuden kannalta kriittisten prosessivaiheiden arviointi ja hallintajärjestelmän kehittäminen sekä uhkaskenaarioiden laatiminen ja potentiaalisten riskien analysointi. Keskipitkällä ja pitkällä aikavälillä korostuvat erilaiset mallinnus-, simulointi-, visualisointi- ja paikannustekniikat sekä ohjaus- ja päätöksentekojärjestelmät. Mahdollisten ongelmien tunnistukseen ja monitorointiin liittyviä merkittäviä teknologioita ovat kemialliset, biologiset ja radioaktiiviset analyysi- sekä detektiotekniikat. Keskipitkällä aikavälillä kehitetään mikrobiologista diagnostiikkaa kohdemikrobeille. Pitkällä aikavälillä korostuvat mikrobidiagnostiikan nopeus – tulokset alle kahdessa tunnissa – ja soveltaminen käytäntöön. Anturiteknologian ja tiedonsiirron on oltava nopeaa.

Liikenne ja kuljetukset

Liikenteen ja kuljetusten toiminnan varmistamisessa korostuvat tunnistus-, paikannus- ja tiedonsiirtoteknologiat. Näitä ovat lyhyellä tähtäimellä ajoneuvojen ja kuorman seurantateknologiat sekä GIS-sovellukset. Kehitys kohdistuu keskipitkällä aikavälillä järjestelmäkehitykseen, esimerkiksi ohjaus- ja valvontajärjestelmiin ja pitkällä aikavälillä näiden eri järjestelmien integrointiin.

Liikenteen ja kuljetusten turvaamisen keskeisin osaaminen liittyy paikkatietojärjestelmiin (GPS, Galileo), RFID:hen, anturiverkkoihin, hahmontunnistukseen ja biometriseen henkilöntunnistukseen. Lisäksi tietoverkkojen ja -järjestelmien suojauksen sekä riskianalyysimenetelmien osaaminen on merkittävää liikenteen ja kuljetusten turvaamisessa.

Ihmisten suojaaminen

Merkittäviä ihmisten suojaamiseen liittyviä teknologioita ovat fyysisen suojaamisen teknologiat sekä erilaiset tunnistus-, paikannus- ja tiedonsiirtoteknologiat. Jälkimmäisiä voivat olla esimerkiksi millimetriaaltokuvannustekniikka sekä immunologiset tekniikat C- ja B-detektiossa. Kehityksen odotetaan etenevän kemiallisten agenssien detektiosta biologisten agenssien detektioon, analyysijärjestelmien kehittämiseen ja siitä edelleen detektion soveltamiseen käytäntöön.

Kokonaisturvallisuuden hallinnassa korostuu riski- ja haavoittuvuusanalyysimenetelmien kehittäminen sekä tilanteen monitorointi esimerkiksi havaitsemalla ihmisen poikkeava käytös tilastollisesti. Tämä edellyttää esimerkiksi riskien kvantifiointiin tarvittavan datan saatavuuden kartoittamista, kysely- ja haastattelututkimusmenetelmien sekä riskien kvantifioinnin ja päätöksentekomallien kehittämistä sekä tilanteen reaaliaikaista seurantaa, tulkintaa ja ohjausta.

Ihmisten suojaamisen keskeisin osaaminen liittyy toisaalta fyysisen suojauksen, ts. rakenteellisen suojauksen ja suojauksen ilman mukana kulkeutuvilta CBR-agensseilta, ja toisaalta ilmaisu- (detektio-) teknologioiden kehittämiseen. Myös hälytys- ja monitorointijärjestelmiin liittyvä osaaminen sekä järjestelmien integrointi on olennaista.

Tuotannon ja palvelutoiminnan turvallisuus

Tuotannon ja palvelutoiminnan turvallisuuden varmistaminen on laaja osa-alue. Siihen liittyvät lähes kaikki julkaisussa käsiteltävät teknologiat. Sovellettavat teknologiat vaihtelevat toimialasta ja yrityksestä toiseen, mutta yleisesti ottaen lyhyellä ajanjaksolla merkittäviä ovat esimerkiksi tietoturvallisuus, kiinteistöteknologia, suojausteknologiat, riskianalyysi sekä riskien arviointi- ja hallintamenetelmät sekä mikrobidiagnostiikka. Keskipitkällä ja pitkällä aikavälillä korostuu näiden teknologioiden soveltaminen käytäntöön. Kokonaisturvallisuuden hallinnassa lähtökohtana on safety- ja tietoturvaosaamisen ja -kokemuksen soveltaminen security-alueelle.

Suomessa saatetaan olla joissain asioissa yliturvallisia. Toisaalta teollisuuden riskienhallintatoimenpiteet on mahdollisesti kohdennettu riittämättömästi ja niiden ylläpidon kustannusvaikutuksia ei ole perusteellisesti selvitetty. Puutteita on varmasti myös riskienhallintajärjestelmän ylläpidossa. Toiminnan koordinointi yritystasolla on vielä hajallaan ja yritysturvallisuuden painopistealueet on valittu lähinnä perinteitä noudattaen. Turvallisuuden eri osa-alueiden synergiaeduista on vielä vähän kokemusta. Turvallisuustason toteutumista tulisi mitata paremmin, ja painopistealueiden löytämisen tulisi perustua analyyseihin.

Yritysten riippuvuus tietoturvallisuuden hallinnasta on merkittävä ja haavoittuvuus kasvaa esimerkiksi vahingontekojen yleistymisen myötä. Kansainvälistyminen ja verkostoituminen tuovat mukanaan sekä tietoturvallisuuteen liittyviä vaatimuksia että uhkakuvia. Tietotekniikan ja elektroniikan (ICT:n) yleistyminen kaikissa prosesseissa ja järjestelmissä lisää riskien tunnistamisen ja hallinnan tarpeita nimenomaan käyttövarmuuden näkökulmasta.

Tuotannon ja palvelutoiminnan turvallisuuden varmistaminen vaatii laaja-alaista teknologista osaamista. Keskeisiä osaamisalueita VTT:n kannalta ovat esimerkiksi kokonaisturvallisuuden hallinta sekä tietoverkkojen ja -järjestelmien suojaus. Lisäksi erilaiset tunnistukseen, paikannukseen ja tiedonsiirtoon liittyvät osaamiset ovat merkittäviä.

Kiinteistö- ja toimitilaturvallisuus

Merkittäviä kiinteistö- ja toimitilaturvallisuuteen liittyviä teknologioita ovat passiiviset tai rakenteelliset turvallisuusratkaisut sekä erilaiset hälytys- ja monitorointijärjestelmät ja näiden integrointi ja yhteys kiinteistöjärjestelmiin, hälytysvalvomoihin ja julkishallinnon hätäkeskusjärjestelmiin. Kiinteistön kokonaisturvallisuuden hallinnassa ja johtamisessa korostuvat riskien analysointi, arviointi ja hallinta sekä katselmoinnit, todentaminen, skenaariot, turvallisuustiedon hallinta ja eri toimijoiden yhteistyö sekä turvallisuusjohtamisen menetelmät ja mallit. Turvallisuuden kehittämisen lähtökohtana on kiinteistön koko elinkaaren kattaminen (suunnittelu, rakentaminen, käyttö, ylläpito, kehittäminen ja turvallisuusjohtaminen).

Toimitilaturvallisuuden hallinta on oleellista mm. rikosturvallisuuden ja tietoturvallisuuden varmistamiseksi. Tietyissä kohteissa myös varautuminen terrorismin uhkaan on tullut oleelliseksi. Nykyiset valvontajärjestelmät ovat integroitumassa. Riskienhallintaa yritysten kesken tarvitaan mm. teollisuuspuistoissa.

Sulautettujen järjestelmien tietoturva

Tuotteiden ja järjestelmien tietoturvan hallinta perustuu pääasiassa tietoturva-arkkitehtuureihin sekä välitason ohjelmistokomponentteihin ja alustoihin. Tällaisia ohjelmistoalustoja ja -arkkitehtuureja ovat lyhyellä aikavälillä mm. Symbian + IP (mobiilit päätelaitteet), Java (sulautetut järjestelmät) ja MHP1.0.x-ympäristö (digi-TV). Keskipitkällä ja pitkällä aikavälillä mobiileissa päätelaitteissa ja sulautetuissa järjestelmissä korostuu edellisten lisäksi myös Linux. Digi-TV-teknologioissa uusi tietoturvan haaste keskipitkällä aikavälillä ovat paluukanavan kautta ladattavat ja paluukanavaa hyödyntävät sovellukset.

Sulautettujen järjestelmien tietoturvan keskeisin osaaminen liittyy ohjelmistoalustoihin ja -arkkitehtuureihin sekä tietoturvatestaukseen. Myös yleisempi verkko- ja Internet-tietoturvan osaaminen on merkittävää sulautettujen järjestelmien toiminnan turvaamisessa.

Geneeriset teknologiat

Turvallisuutta takaavia geneerisiä teknologioita ovat esimerkiksi kokonaisturvallisuuden hallinnan, hälytys- ja monitorointijärjestelmien ja tietoturvan teknologiat. Kokonaisturvallisuuden hallinnassa ja johtamisessa lähtökohtana on safety-osaamisen ja kokemuksen soveltaminen security-alueelle. Toiminnassa korostuvat riskien analysointi, arviointi ja hallinta sekä turvallisuustiedon hallinta ja eri toimijoiden yhteistyö sekä turvallisuusjohtamisen menetelmät ja mallit. Riskin muuttaminen liiketoimintamittareilla mitattavaksi (due diligence) on yhä tarpeellisempaa. Riski- ja haavoittuvuusanalyysimenetelmiä kehitetään. Riskien hallitsemiseksi kehitetään esimerkiksi ihmisen poikkeavan käytöksen tilastollista havaitsemista ja heikkojen signaalien analysointia.

Hälytys- ja monitorointijärjestelmiin liittyvä osaaminen sekä järjestelmien integrointi on olennaista. Uhkatilanteiden tunnistuksessa kehityksen odotetaan etenevän kemiallisten agenssien detektiosta biologisten agenssien detektioon, analyysijärjestelmien kehittämiseen ja siitä edelleen detektion soveltamiseen käytäntöön. Anturiteknologian, määritysmenetelmien ja tiedonsiirron on oltava nopeaa. Tavoitteena on pikamääritysmenetelmien ja integroitujen, miniatyrisoitujen mittausjärjestelmien kehittäminen ja niiden toimintavarmuuden todentaminen.

Tietoturvassa korostuvat usealla sovellusalueella tietoturvamonitorointi, riski- ja uhka-analyysi, tietoturvatestaus sekä tietoverkkojen ja -järjestelmien suojaus. Tietoturvan kehittäminen perustuu tietoturva-arkkitehtuureihin, mm. välitason ohjelmistokomponentteihin ja alustoihin. Merkittäviä tietoliikenneverkkojen toiminnan varmistamiseen liittyviä teknologioita ovat turvallinen välitason ohjelmisto, yksinkertaistettu ja robusti avainhallinta sekä ohjelmoitavat verkot.

Teknologiat eivät kuitenkaan yksin voi varmistaa turvallisuutta. Tämän vuoksi teknologioiden kehittämisen lisäksi panostetaan myös turvallisuutta varmistavien ja edistävien toimintatapojen kehittämiseen.

Julkaisija

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2327
VTT–TIED–2327

Tekijä(t)
Naumanen, Mika & Rouhiainen, Veikko (toim.)

Nimeke

Security-tutkimuksen roadmap

Tiivistelmä

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaaminen on noussut Euroopassa merkittäväksi haasteeksi. EU:n seuraavaan puiteohjelmaan on tulossa aihealue ”Space and security”, jonka laajuus tulee olemaan hyvin merkittävä. Aihealueen perusteluissa todetaan, että ”teknologia ei voi taata turvallisuutta, mutta turvallisuutta ei voida saavuttaa ilman teknologian tukea”. Edelleen perusteluissa korostetaan sitä, että turvallisuus- ja puolustustutkimus lähestyvät yhä enemmän toisiaan. Näin vanha erottelu siviili- ja sotilastutkimukseen on pienenemässä, koska on todettu, että molemmat hyödyntävät samaa osaamista.

Suomessa on jo nyt merkittävää turvallisuuteen liittyvää yritystoimintaa. Osa yrityksistä toimii pelkästään Suomessa, mutta jotkut ovat alallaan kansainvälisesti johtavia. Turvallisuusalan merkitys on kasvamassa. Tutkimuksen kautta voidaan löytää merkittäviä kasvumahdollisuuksia myös uusille liiketoiminnoille.

VTT:llä on käynnissä turvallisuustutkimusta kaikissa nykyisissä osaamiskeskittymissä ja klustereissa. Valtaosa tutkimuksesta kohdistuu yleiseen turvallisuuteen, mutta VTT osallistuu myös useisiin puolustusvälineteollisuutta tukeviin hankkeisiin.

Osaamistensa ja tutkimustarpeiden tarkemmaksi määrittämiseksi VTT:ssä laadittiin vuonna 2005 laajan tutkijajoukon yhteistyönä VTT:n Security-tutkimuksen roadmap. Siinä turvallisuuden kannalta erityisen tärkeiksi nousi kolme aihealuetta. Yhteiskunnan järjestelmien turvaamisessa korostuvat energiaverkostot, tietoliikenneverkot, vesihuolto, liikenne ja kuljetukset sekä ihmisten suojaaminen. Elinkeinoelämän turvallisuuden varmistamisessa tärkeiksi aihealueiksi nousivat tuotannon ja palvelutoiminnan turvallisuus, kiinteistö ja toimitilaturvallisuus sekä sulautettujen järjestelmien tietoturva. Keskeisinä tarvittavina osaamisina ja teknologioina nousivat esiin kokonaisturvallisuuden hallinta, ilmaisu, tunnistus, paikannus ja tiedonsiirto, tietoverkkojen ja järjestelmien suojaus sekä fyysinen suojaus.

Tämä julkaisu tarkastelee yksityiskohtaisesti security-aihealueen osaamis- ja kehitystarpeita sekä tulevaisuuden kehitysnäkymiä.

Avainsanat
energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks

ISBN
951–38–6769–2 (nid.)
951–38–6770–6 (URL: http://www.vtt.fi/publications/index.jsp)

Avainnimeke ja ISSN
VTT Tiedotteita – Research Notes
1235–0605 (nid.)
1455–0865 (URL: http://www.vtt.fi/publications/index.jsp)

Projektinumero

Julkaisuaika	Kieli	Sivuja	Hinta
Helmikuu 2006	Suomi, engl. abstr.	69 s.	B

Projektin nimi
Yhteiskunnan turvallisuuden varmistaminen tutkimuksen ja teknologian avulla (VTT:n strateginen hankealue)

Toimeksiantaja(t)

Yhteystiedot
VTT
Vuorimiehentie 3, PL 1000, 02044 VTT
Puh. vaihde 020 722 111
Faksi 020 722 7090

Myynti
VTT
PL 1000, 02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Published by

Series title, number and report code of publication

VTT Research Notes 2327
VTT–TIED–2327

Author(s)
Naumanen, Mika & Rouhiainen, Veikko (eds.)

Title

Security research roadmap

Abstract

Requirements for increasing security have arisen in Europe after highly visible and tragic events in Madrid and in London. While responsibility for security rests largely with the national activities, the EU has also started planning a research area “Space and security” as a part of the 7th Framework Programme. As the justification for this research area it has been presented that “Technology alone can not assure security, but security can not be assured without the support of technology.” Furthermore, the justification highlights that security and military research are becoming ever closer. The old separation between civil and military research is decreasing, because it has been noticed that both areas are nowadays utilising the same knowledge.

In Finland, there is already now noteworthy entrepreneurship related to security. Although some of the companies are currently only operating in Finland, others are already international leaders in their area. The importance of the security area is increasing and remarkable potential for new growth business areas can already be identified. This however also requires an increase in research efforts.

VTT has a broad range of security research ongoing in many technology areas. The main areas have been concentrating on public safety and security, but VTT is participating also in several research projects related to the defence technology.

For identifying and defining in more detail the expertise and research goals, the Security research roadmap was developed. The roadmap identified three particularly significant areas related to security. The assurance of critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport, and obviously also the citizens. For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for embedded systems. The most important security products and technologies needed are, for example, management of total security, detection, identification, localisation and communication, protection of information networks and systems, and physical protection.

This report presents in more detail the knowledge and development needs as well as future development potentials seen in the security area.

Keywords
energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks

ISBN
951–38–6769–2 (soft back ed.)
951–38–6770–6 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN
VTT Tiedotteita – Research Notes
1235–0605 (soft back edition)
1455–0865 (URL: http://www.vtt.fi/publications/index.jsp)

Project number
G5SU00905

Date	Language	Pages	Price
February 2006	Finnish, Engl. abstr.	69 p.	B

Name of project
Yhteiskunnan turvallisuuden varmistaminen tutkimuksen ja teknologian avulla (VTT:n strateginen hankealue)

Commissioned by

Contact
VTT Technical Research Centre of Finland
Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT, Finland
Phone internat. +358 20 722 111
Fax +358 20 722 7090

Sold by
VTT Technical Research Centre of Finland
P.O.Box 1000, FI-02044 VTT, Finland
Phone internat. +358 20 722 4404
Fax +358 20 722 4374

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaaminen on noussut Euroopassa merkittäväksi haasteeksi. EU:n seuraavaan puiteohjelmaan on suunnitteilla laaja turvallisuuteen kohdistuva tutkimusohjelma. VTT:llä on käynnissä laajaa turvallisuustutkimusta useilla teknologia-alueilla. Valtaosa tutkimuksesta kohdistuu yleiseen turvallisuuteen, mutta VTT osallistuu myös useisiin puolustusvälineteollisuutta tukeviin hankkeisiin.

Osaamistensa ja tutkimustarpeiden tarkemmaksi määrittämiseksi VTT:ssä laadittiin vuonna 2005 Security-tutkimuksen roadmap. Siinä turvallisuuden kannalta erityisen tärkeiksi nousi kolme aihealuetta: yhteiskunnan järjestelmien turvallisuuden varmistaminen, elinkeinoelämän toimintojen turvaaminen sekä turvallisuustuotteet ja teknologiat.

Julkaisu tarkastelee yksityiskohtaisesti Security-tutkimuksen osaamis- ja kehitystarpeita sekä tulevaisuuden kehitysnäkymiä.

Tätä julkaisua myy
VTT
PL 1000
02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Denna publikation säljs av
VTT
PB 1000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

This publication is available from
VTT
P.O. Box 1000
FI-02044 VTT, Finland
Phone internat. + 358 20 722 4404
Fax + 358 20 722 4374

ISBN 951-38-6769-2 (nid.)
ISSN 1235-0605 (nid.)
ISBN 951-38-6770-6 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455-0865 (URL: http://www.vtt.fi/inf/pdf/)