ESPOO 2007 VTT TIEDOTTEITA 2388

Marinka Lanne & Eija Kupi

Miten hahmottaa security-alaa?

Teoreettinen malli Suomen security-liiketoiminta-alueista

VTT TIEDOTTEITA – RESEARCH NOTES 2388

Miten hahmottaa security-alaa?

Teoreettinen malli Suomen security-liiketoiminta-alueista

Marinka Lanne & Eija Kupi

ISBN 978-951-38-6924-3 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

Copyright © VTT 2007

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

VTT, Teknikvägen 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, +358 20 722 3499

Toimitus Leena Ukskoski

Lanne, Marinka & Kupi, Eija. Miten hahmottaa security-alaa? Teoreettinen malli Suomen security-liiketoiminta-alueista [Security as an area of business]. Espoo 2007. VTT Tiedotteita – Research Notes 2388. 52 s. + liitt. 1 s.

Avainsanat business security, Finland, security markets, service providers, government, research communities, educational institutions, financial institutions, defence industry, CBRNE-detection technology providers, guarding and security services, transport security solutions, locking solutions

Tiivistelmä

Turvallisuusala on moniselitteinen ja osin hahmottumatonkin käsite. Termi yhdistetään helposti Suomen virallisissa tilastoissa esiintyvään toimialaluokitukseen vartiointi- ja turvallisuuspalvelut. Turvallisuuteen liittyviä tuotteita, ratkaisuja ja palveluja tarjoavien yritysten joukko on kuitenkin huomattavasti tätä yksittäistä toimialaa laajempi. Tässä julkaisussa pohditaan alustavasti kansallisella tasolla niitä liiketoiminnan alueita, joiden ympärille *security*-liiketoiminta todennäköisimmin voisi kehittyä. Lisäksi pohditaan sitä, miten nämä liiketoiminta-alueet voisivat muodostaa klusterin ja mitkä tekijät vaikuttavat security-markkinoihin. *Security*-termillä turvallisuuden tarkastelu rajataan etenkin tahallisilta vahingonteoilta suojaamiseen.

Markkinatutkimusten, muun kirjallisuuden sekä yrityshaastattelujen pohjalta hankkeessa muodostettiin käsitys *securityyn* liittyvästä toimijakentästä sekä markkinoihin vaikuttavista tekijöistä. Toimijakentän nähtiin muodostuvan turvallisuuteen liittyviä tuotteita ja palveluja tuottavista yrityksistä, tuotteita ja palveluja ostavista yrityksistä, eri viranomaistahoista, eri järjestöistä, tutkimus- ja opetuslaitoksista sekä erilaisista yhteistyöfoorumeista. Keskeisenä kotimaisena julkisena rahoittajana toimii lähinnä Tekes. Käyttäjänä, asiakkaana, tutkimuskohteena ja vaikutusten kohteena myös yksilöllä ja yhteiskunnalla on rooli toimijakentässä.

Tässä hankkeessa *security*-markkinoiden nähtiin muodostuvan erilaisten uhkien kautta. Markkinoihin vaikuttaviksi tekijöiksi tunnistettiin esimerkiksi poliittiset päätökset, lainsäädäntö, standardointi, teknologian kehitys, ihmisten yleinen käsitys turvallisuudesta sekä erilaisten ratkaisujen yleinen hyväksyttävyys ja vaikutukset yksityisyyden suojaan. *Securityyn* liittyvissä markkinatutkimuksissa käsiteltiin hyvinkin hajanaisesti erilaisia teknologioita, tuotteita ja suojattavia kohteita. Yrityshaastattelut tukivat käsitystä siitä, että security-liiketoiminta-aluetta ei mielletä vakiintuneena kokonaisuutena, vaan *securityyn* liittyy useita eri liiketoiminta-alueita. Hankkeessa päädyttiin lopulta kuvaamaan teoreettista *security*-klusteria havaittujen liiketoiminta-alueiden yhdistelmänä (CBRNE-detektointi, vartiointi- ja turvallisuuspalvelut, puolustusvälineteollisuus, kuljetusten turvaaminen ja lukitusratkaisut). Nämä alueet kuitenkin kuvaavat edelleen vain osaa koko turvallisuusalasta. Teoreettinen *security*-klusteri voitiin hahmottaa klusterin ja kilpailukyvyn mallinnuksessa yleisesti käytettyjen kaavioiden avulla. Teoreettista klusteria ei kuitenkaan voi pakottaa toimimaan, vaan klusterin syntyyn on tultava tarve eri liiketoiminta-alueiden sisältä.

Lanne, Marinka & Kupi, Eija. Miten hahmottaa security-alaa? Teoreettinen malli Suomen security-liiketoiminta-alueista [Security as an area of business]. Espoo 2007. VTT Tiedotteita – Research Notes 2388. 52 p. + app. 1 p.

Keywords business security, Finland, security markets, service providers, government, research communities, educational institutions, financial institutions, defence industry, CBRNE-detection technology providers, guarding and security services, transport security solutions, locking solutions

Abstract

As an area of business, the concept of security is quite ambiguous and unclear. Security market research reports categorise the security industry in different ways and into several parts; there is currently no common approach, and even the areas and concepts are not well-defined. Even so, there is mutual consensus that the security industry has been growing. This report considers, at a national level, which areas of business have potential in the security sector, how those areas can constitute a cluster, and which factors affect security markets. Throughout this report, security is considered to be the state of being free from the danger of intentional damage.

The business of security includes companies that provide products and services, the companies buying and using those products and services, the government, the research community, educational institutions, financial institutions, and institutions that promote collaboration. Individuals and society also play an important role: as clients, users of products and services, research subjects, and even as a subject of influence. A diverse range of dangers and the associated perceptions on risk have given rise to an extensive and broad security market. There are several different factors that influence the market, for example, political decisions, legislation, standards, technology trends, public opinions on safety and security, and public acceptability of different solutions and the associated effects on privacy protection.

In this study, a theoretical security cluster was outlined by combining some areas of the security business: the defence industry, providers of CBRNE-detection technologies, guarding and security services, transport security solutions and locking system solutions. These areas of business, however, represent only part of the entire security business. Furthermore, this cluster model is purely theoretical and only a real need, deriving from the desires of the stakeholders (members of theoretical cluster), can make the cluster function.

Alkusanat

Julkaisu on toteutettu osana VTT:n sisäistä Yhteiskunnan ja elinkeinoelämän turvallisuuden varmistaminen (*Security*-VTT) -hanketta. Hankkeesta on aiemmin julkaistu VTT Tiedotteita sarjassa *Security*-tutkimuksen roadmap [Naumanen & Rouhiainen 2006]. *Security*-klusterin hahmottamiseen tähtäävä tutkimuksen osa on toteutettu 2.4.2006–31.12.2006. Hankkeen ohjausryhmänä toimi *Security*-KTA:n ydintiimi, johon kuuluivat Veikko Rouhiainen, Veikko Komppa, Arto Juhola, Markku Jenu, Laura Raaska, Auli Lastunen, Osmo Auvinen ja Reijo Savola.

Sisällysluettelo

1. Johdanto

Turvallisuus on sekä Suomessa että kansainvälisesti kasvattanut merkitystään. Uhkien luonne ja vaikutusten laajuus ovat kasvaneet huomattavasti. Tärkeimpiä turvallisuustoimintaan liittyviä kansainvälisiä kehitystrendejä ovat globalisaatioon, verkottumiseen, teknologiariippuvuuteen ja terrorismin torjuntaan liittyvät toimenpiteet sekä kansainvälisen yhteistoiminnan korostuminen. Suomessa turvallisuuden alueella on käynnissä sisäasianministeriön johtama sisäisen turvallisuuden ohjelmatyö. [Savola 2004]

Yhteiskunnan turvallisuuden ja elintärkeiden toimintojen takaamista turvaavan EU:n *security*-teeman perusteluissa todetaan, että ”teknologia ei voi taata turvallisuutta, mutta turvallisuutta ei voida saavuttaa ilman teknologian tukea”. VTT:lla onkin käynnissä turvallisuustutkimusta kaikissa yksiköissä ja alueella nähdään suuri liiketoimintapotentiaali. Turvallisuuden parantamiseen tähtäävien tuotteiden ja järjestelmien kehittäminen on vasta käynnistynyt ja uusille innovaatioille on vielä tilaa. [Naumanen & Rouhiainen 2006] VTT:n strategisena tavoitteena on olla Suomen *security*-klusterin innovaatiokumppani. Tämä edellyttää *security*-klusterin hahmottamista sekä erilaisten teknologiapalvelujen tarpeen tunnistamista.

Hankkeessa *security*-klusterilla tarkoitetaan security-alan tuotteiden ja palvelujen muodostamaa osaamiskeskittymää. Klusteri on toimialojen ja yritysten muodostama kehityskeskittymä, johon kuuluu samanaikaisesti sekä yhteistyötä että kilpailua. Klusterin toimialoja ja yrityksiä sitovat yhteen vahvat osaamis- ja hyödykekytkennät. [Hernesniemi 2004].

Turvallisuusalan klusteri on sellaisenaan hahmottumaton käsite. Tässä julkaisussa lähdetään alustavasti pohtimaan kansallisella tasolla niitä ydintoimialoja, joiden ympärille *security*-klusteri todennäköisimmin voisi kehittyä. Tärkeää on myös saada käsitys siitä, miten turvallisuusalan markkinat muodostuvat. Keskeisiä kysymyksiä ovat:

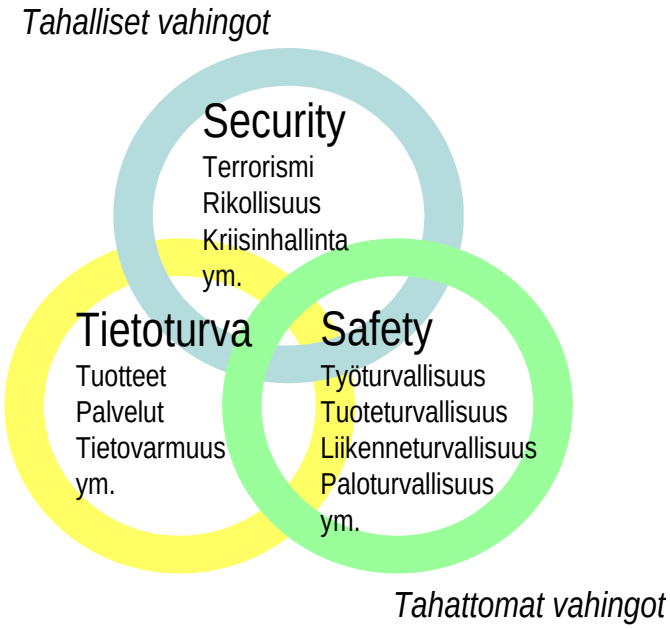
- Millaiset yritykset ovat ydintoimijoita *security*-klusterin muodostamisen kannalta?
- Millaisista kansainvälisen kilpailun kannalta merkittävistä verkostoista klusteri voisi muodostua?
- Miten yksittäisistä toimijoista ja verkostoista voitaisiin muodostaa klusteri?
- Millaiset kilpailukykytekijät vaikuttavat klusterin muodostumiseen?

Koska tietoturvallisuus katsottiin tässä omaksi monitahoiseksi kokonaisuudekseen, jätettiin aihealue tutkimuksessa vähemmälle. Esimerkiksi liikenne- ja viestintäministeriö on tehnyt Tietoturvallisuusklusterin esiselvityksen vuonna 2003. Kyseisessä raportissa on pohdittu tarkemmin juuri tietoturva-alan trendejä ja mahdollisuuksia kehittää tietoturvayritysten klusteria. [Tietoturvaklusterin esiselvitys 2003]

2. Tausta ja viitekehys

2.1 Turvallisuus termeinä

Termiin turvallisuus latautuu useita erilaisia merkityksiä (poliittinen, sotilaallinen, yhteiskunnallinen, sosiaalinen, taloudellinen, psykologinen, tekninen, ympäristöön liittyvä) [Buzan 1983; Laitinen 1999]. Turvallisuutta voidaan tarkastella esimerkiksi maailma-, valtio-, yritys- tai yksilökeskeisesti [Buzan 1983; Hyvärinen 2002]. Usein termi kuitenkin määritellään hatarasti ja sen sisältöä pidetään itsestään selvyytenä [Baldwin 1997]. Tässä tutkimuksessa turvallisuutta tarkastellaan lähinnä vain tahallisten vahingontekojen kannalta. Tällöin vahingontekojen ennaltaehkäisyyn, teoilta suojautumiseen sekä tekoihin varautumiseen viitattaessa käytetään termiä *security*. Tarkastelu keskittyy erityisesti yhteiskunnan sekä elinkeinoelämän turvallisuuteen. Termillä *safety* sen sijaan viitataan tässä tahattomilta onnettomuuksilta, tapaturmilta ja menetyksiltä suojautumiseen. Kuvassa 1 on eräs näkemys turvallisuustermien suhteista.



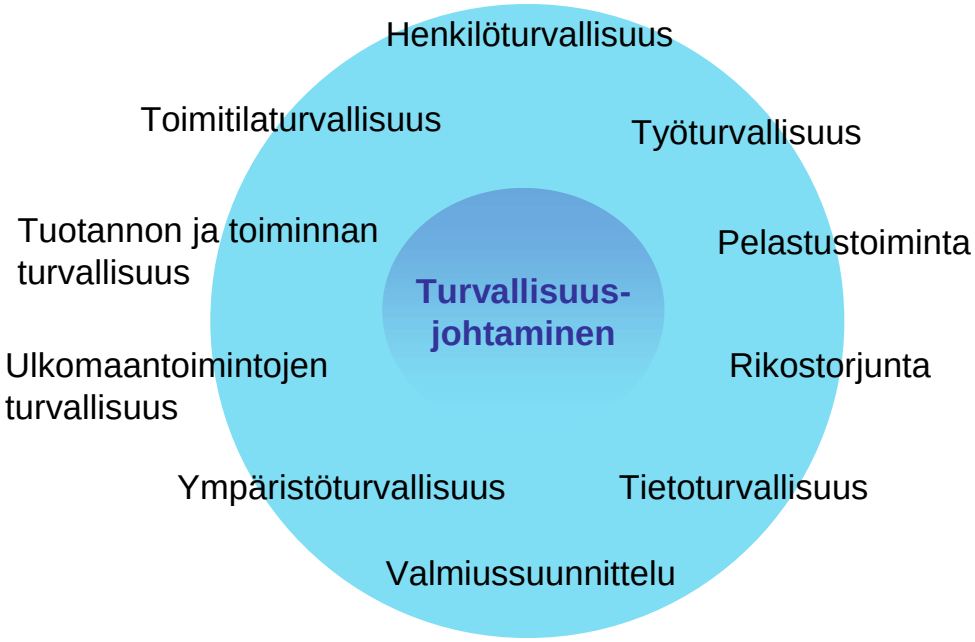
Kuva 1. Turvallisuustermien suhteet [Naumanen & Rouhiainen 2006].

Turvallisuus voidaan määritellä menettelytapoihin sitoen: *jokin on turvallista, kun tietyt toimenpiteet on toteutettu.* Mitattavia kriteerejä turvallisuudelle ei yleensä anneta. Tyypillisesti turvallisuus määritellään riskin kautta: *mitä pienempi riski, sen korkeampi turvallisuus*. Riski puolestaan määritellään seurauksien ja todennäköisyyden funktiona. Seurauksien arvioinnin arvokysymykset ja todennäköisyyden arviointiin liittyvä frekvenssidatan puute vaikeuttavat määrittelyä. [Möller 2005] Levän [2003] mukaan turvallisuus voidaan nähdä ominaisuutena eli toiminnan lopputuloksena sekä käsitteellisenä tavoitteena eli prosessin laatuna. Organisaatioissa eri ihmiset ja yhteisöt voivat määritel-

lä ja nähdä turvallisuuden eri tavoin: esimerkiksi organisaation vastuuna, asenteena tai kulttuurin tuotteena [Gherardi et al. 1998]. Turvallisuus voidaan ajatella myös koettuna turvallisuuden tai turvattomuuden tunteena [Laitinen 1999].

Kun turvallisuutta tarkastellaan erityisesti yrityksen näkökulmasta, käytetään termiä yritysturvallisuus. Suomalaisessa kirjallisuudessa esitetyt erilaiset yritysturvallisuuden osa-aluejaot (Kuva 2) pohjautuvat useimmiten Yritysturvallisuuden neuvottelukunnan (YTNK) jaotteluun (esimerkiksi Kerko 2001; Miettinen 2002). Jokainen osa-alue sisältää erilaisia turvallisuuden hallintaan liittyviä asioita. Alueita on vaikea jakaa täysin *security*- tai *safety*-käsitteiden alle, mutta esimerkiksi yksityisiä turvallisuuspalveluja koskevassa hallituksen esityksessä HE 69/2001 todetaan, että ”*turvallisuuden niin kutsuttu security-näkökulma käsittää muun muassa rikosturvallisuuden, kiinteistö- ja toimitilaturvallisuuden, henkilöturvallisuuden ja tietoturvallisuuden. …safety-näkökulma taas käsittää muun muassa pelastustoiminnan, työsuojelun ja ympäristön suojelun. Käytännössä security- ja safety-näkökulmat usein yhtyvät.*” Yritysturvallisuus (*corporate security*) kattaa organisaatioita koskevat tahattomiin onnettomuuksiin sekä tahallisiin vahingontekoihin liittyvät näkökulmat. [YTNK 1999, 2006; HE 69/2001]. Turvallisuudella suojattavina kohteina ja arvoina nähdään tyypillisesti henkilöt, ympäristö, omaisuus, tieto ja maine.

Kiinteistö- ja toimitilaturvallisuuden tavoitteena on rakenteellisen turvallisuuden ja turvallisuusvalvonnan toteuttaminen yrityksessä [Kerko 2001; Miettinen 2002]. Rakenteelliseen turvallisuuteen kuuluvia kohteita ovat muun muassa aidat ja portit, avainhallinta ja lukitukset, murtosuojaus, turvallisuusrakenteet sekä kiinteistötekniikka. Turvallisuusvalvontaan puolestaan kuuluvat tekninen valvonta ja kulunvalvonta, rikosilmoitusjärjestelmät, henkilöstön, vieraiden ja ajoneuvojen ohjaus sekä vartiointi ja valvomotoiminta. Rikosturvallisuudessa keskitytään yritystä sekä sisä- että ulkopuolelta uhkaavan rikollisen toiminnan ennaltaehkäisyyn ja torjuntaan. Suojattavia kohteita ovat henkilöstö, omaisuus, toiminta ja tiedot. [Kerko 2001; Miettinen 2002; YTNK 1999, 2006] YTNK:n mukaan rikosturvallisuuden hallintaan kuuluvat muun muassa yhteistoiminta viranomaisten kanssa, rikosriskien hallintakeinot ja toiminta rikostapauksessa. Toimitilaturvallisuuden ja rikosturvallisuuden kohdalla on selvä yhteys, sillä hyvä rakenteellinen turvallisuus ja turvallisuusvalvonta muodostavat perustan myös rikosturvallisuuden hallinnalle [Kerko 2001].



Kuva 2. Yritysturvallisuuden osa-alueet [YTNK 1999, 2006; Turvallisuus.net. 2006].

Tietoturvallisuudella tarkoitetaan tietojenkäsittelyn ja tiedonsiirron luottamuksellisuuden, eheyden ja saatavuuden ylläpitämistä, varmistamista ja kehittämistä [Miettinen 2002]. Osa-alueeseen liittyviä yritysturvallisuuden kehittämistoiminnan kohteita ovat muun muassa hallinnollinen tietoturvallisuus, tietoaineistoturvallisuus, luotettavuuslausuntomenettely, tietosuoja ja salassapitosopimukset, tietosodankäynti, tietoteknillinen turvallisuus ja tiedonsiirron suojaus, laitteisto- ja ohjelmistoturvallisuus sekä fyysinen turvallisuus ja käyttötoiminnan turvallisuus [YTNK 1999, 2006]. Henkilöturvallisuudesta huolehtimisen tavoitteena on vähentää ihmisten aiheuttamia tahattomia ja tahallisia riskejä yrityksen toiminnalle [Miettinen 2002]. Osa-alueeseen liittyy YTNK:n [1999, 2006] mukaan asiakkaiden, vierailijoiden, avainhenkilöiden, kodin ja perheen turvallisuus, matkustusturvallisuus, henkilösuojaus erikoistapauksissa, tavoitettavuus- ja hälytysjärjestelmät, varamiesjärjestelyt sekä luotettavuusmenettelyt.

Tieto-, rikos-, henkilö- ja toimitilaturvallisuudella on selkeät liitynnät keskenään. Osa-alueet eivät sinällään erottele yritysturvallisuutta vaan lähinnä tuovat mukaan erilaiset näkökulmat asioiden hallintaan ja turvatoimiin. Edellä mainitut osa-alueet liittyvät kiinteästi myös pelastustoimintaan sekä tuotannon ja toiminnan turvallisuuteen. Pelastustoiminnan ja paloturvallisuuden suunnittelu edellyttää muun muassa toimitilaturvallisuuteen kuuluvien asioiden tiedostamista, rikosten (esim. tuhopoltot) ennaltaehkäisyä ja tietoturvariskien huomioon ottamista. Tuotannon ja toiminnan turvallisuus sisältää muun muassa varastointiin ja kuljetuksiin, arvo-omaisuuden säilyttämiseen, logistiikkaan ja maksuliikenteeseen liittyviä turvatoimia [Miettinen 2002; YTNK 1999, 2006].

2.2 Security-uhat ja kehityshaasteet

Viime vuosina turva-alalle uusia ja ennakoimattomia haasteita ovat luoneet muun muassa yhteiskunnan ja liiketoiminnan kansainvälistyminen sekä ympäristön monikulttuuristuminen. Suomen ulkopuolelta tulevat vaikutukset, kuten globalisaatiokehitys, suurvaltojen vastakkainasettelun murtuminen, Euroopan yhdistyminen, Neuvostoliiton hajoaminen ja rajojen avautuminen, ovat edistäneet uudenlaisen rikollisuuden leviämistä. Tällaisia ovat terrorismi, tehostunut tiedustelu, yritysvakoilu, talousrikollisuus, laajeneva huumerikollisuus ja järjestäytynyt rikollisuus. [Räikkönen & Lanne 2004]

Ympäristöturvallisuuden sektorilla tahallisen vahingonteon uhat on jaoteltu terrorismiin, sotatilaan ja poikkeusoloihin liittyviin asioihin. Terrorismiuhista keskeisiä ovat kemiallisten, biologisten ja radioaktiivisten aineiden, ydinaseiden sekä räjähteiden (CBRNE-aineet) käyttö ihmisten ja ympäristön vahingoittamiseen. Sotatilan ja poikkeustilan uhat liittyvät pelastusorganisaation toimintaan sekä siviilien suojautumiseen. [Turvallisuusohjelman valmistelu 2006]

Sotilaallisten ja ei-sotilaallisten uhkien raja hämärtyy jatkuvasti. Myös kansallista ja kansainvälistä järjestäytynyttä rikollisuutta on vaikea enää erottaa toisistaan. Vaatimukset viranomaisjärjestelmien yhteentoimivuudelle ja yhteensopivuudelle kasvavat koko ajan. Turvallisuus on yhteiskunnallinen ja poliittinen kysymys. Yhteiskunnan toimintatapa ja arvovalinnat, organisaatioiden tarpeet ja osaaminen ratkaisevat turvallisuudessa. Turvallisuutta kehitettäessä on kuitenkin aina otettava huomioon yksityisyyden suoja, eettisyys ja käyttäjien tarpeet. Kansalaisten reaktiot turvallisuutta parantavaan teknologiaan voivat olla erilaisia: tekniset ratkaisut voivat luoda turvallisuuden mutta myös turvattomuuden tunnetta, kun uhkasta tullaan tietoisiksi. Yhteiskunnallisen turvallisuustilanteen muuttuessa muuttuvat myös käsitykset turvallisuudesta [Rintakoski 2006]

Myös kansainvälisillä turvallisuusuhkilla on vaikutusta myös yritysten toimintaan. Oikarisen [2003] mukaan erimerkiksi tavarankuljetusten osalta suurimmat uhat kohdistuvat varastoihin, kuljetusten solmukohtiin sekä logistiikan tietojärjestelmiin. Tavarankuljetuksessa on jo mukana paljon uutta teknologiaa: läpivalaisutekniikat (tunnistetaan räjähteet ja massatuhoaseet), pakkausten luvattoman avaamisen paljastavat sinetit, teipit ja hälytysanturit, räjähdysten vaikutuksia rajoittava teknologia, tavaran seuraamis- ja jäljittämisteknologia sekä lastauksen seurantaan liittyvä teknologia. [Oikarinen 2003] Tavarakuljetusten ohella myös lisääntynyt liikematkailu lisää suojelupalvelujen tarvetta.

Oikarinen [2003] kokoaa kansallisen ja kansainvälisen turvallisuuden kehityshaasteet seuraaviksi teemoiksi:

- henkilöllisyyden varmistaminen (biometriset tunnistustekniikat, luotettavat passit ja ID-tunnisteet, kulunvalvonta ja pääsyn rajoittaminen)

- tietojärjestelmien turvaaminen (tietomurtojen torjunta, Internetin turvaaminen, tietojärjestelmien ja tietokantojen yhteensopivuus, reaaliaikainen tiedonvaihto)
- biologisten, kemiallisten ja ydinaseuhkien torjuminen (ainelistat, lääkkeiden ja vasta-aineiden kehittäminen, aineiden tunnistustekniikat, terveydenhuollon, ruoan ja juomaveden turvaaminen)
- infrastruktuurin, liikenteen ja tavarakuljetusten turvaaminen (energian ja sähkön tuotanto sekä jakelu, lentoliikenne, meriliikenne, maantie- ja rautatieliikenne)
- pelastusorganisaatioiden työn tehostaminen ja turvaaminen (yhteensopivat kommunikaatiojärjestelmät, viranomaisverkot, henkilökohtaiset suojavarusteet ja työvälineet, koulutus- ja valmennusmenetelmät sekä -välineet).

Myös tietoturvallisuudella on yhteys kansalliseen ja kansainväliseen turvallisuuteen. Lukuisat yhteiskunnan perustoiminnot ovat riippuvaisia tietoverkon häiriöttömästä toiminnasta. Näitä ovat esimerkiksi vähittäiskaupan logistiikka, energian jakelu ja pankkitoimiala. [Elinkeinoelämän… 2006] Tietoturvauhat liittyvät kiinteästi myös rikoksiin ja terrorismiin (mm. tietomurrot, identiteetin varastaminen) sekä henkilöiden yksityisyydensuojaan (mm. käyttötiedot). [Liikanen 2004]

Rikoslainsäädäntö huomioi hyvin Internetissä tehdyt rikokset, ja Suomessa poliisin valmiudet tutkia verkkorikoksia ovat hyvät. Ongelma on kuitenkin maailmanlaajuinen, eikä kyky reagoida jälkikäteen riitä yhteiskunnan häiriöttömän toiminnan suojaamiseksi. Internet tarjoaa nykyisellään rikollisuudelle erityisen hyvän kasvualustan. Tietoverkkorikollisuus muodostaa erityisen uhan yritysten tietopääomalle, sillä verkossa rikoksen toteuttaminen on usein helpompaa ja halvempaa kuin reaalimaailmassa. Myös kiinnijäännin riski on verkossa olennaisesti pienempi. Tietojärjestelmiin kohdistuvat yritysten kohtaamat rikosilmiöt voidaan ryhmitellä satunnaisiin hyökkäyksiin, kuten roskapostin ja virusten lähettämiseen, ja kohdistettuihin hyökkäyksiin, jotka uhkaavat yritysten tietopääomaa. Tietoturvallisuuden ylläpitäminen on riskienhallintaa, joka edellyttää oikeaa uhkatietoisuutta, uhan vaikutusten arviointia, turvajärjestelmien toteutuksen säännöllistä tarkastamista ja yritykselle sopivan riskitason hyväksymistä. [Elinkeinoelämän… 2006]

Yritysten riski joutua rikoksen kohteeksi on lisääntynyt huumausaine-, väkivalta-, talous ja tietorikollisuuden kasvun, rikollisuuden kansainvälistymisen sekä ammattimaistumisen seurauksena. Myös yritysten henkilöstön riski joutua väkivallalla uhkailun tai väkivallan kohteeksi on lisääntynyt erityisesti kaupan- ja palvelualan työtehtävissä. Suomalaiset myös suhtautuvat liian avoimesti ja luottavaisesti esimerkiksi tietoverkkojen käyttöön. [Yritysten rikosturvallisuus…2005] Yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi Sisäasiainministeriö on laatinut elinkeinoelämän ja viranomaisten yhteisen strategian [Elinkeinoelämän…2006].

Myös yritysten ja yhteiskunnan verkostoituva ja erikoistuva toimintamalli palvelujen ja tavaroiden tuottamisessa on turvallisuuden kannalta haaste. Toimitusketjut ovat pitkiä ja toisistaan riippuvaisia. Lisäksi aineettomien hyödykkeiden merkitys lisääntyy koko ajan. Eri elinkeinoelämän alojen muuttuvien ominaispiirteiden huomioonottaminen turvallisuustyön kannalta on koko ajan haastavampaa. [Elinkeinoelämän… 2006]

2.3 Security-ohjelmat

Suomen *Sisäisen turvallisuuden ohjelma*n tavoitteena on, että Suomi on Euroopan turvallisin maa vuonna 2015. Ohjelmassa turvallisuutta tarkastellaan ensisijaisesti yksilön näkökulmasta ja tavoitteena on lisätä arjen turvallisuutta. Periaatepäätös ohjelmasta annettiin 23.9.2004. Ohjelma on Suomessa ensimmäinen viranomaisten sektorirajat ylittävä sisäisen turvallisuuden alueen useampivuotinen kehittämissuunnitelma, jolla on myös ylimmän poliittisen johdon tuki. Ohjelma pyrkii ottamaan huomioon keskeiset tulevaisuuden uhkatekijät (Kuva 3).

Kuva 3. Tulevaisuuden uhkatekijät [Arjen turvaa 2004a ja b].

EU:n tutkimusta, teknologian kehittämistä sekä kokeellista toimintaa tukevassa 7. puiteohjelmassa (2007–2013) *security*-aihealue on nostettu yhdeksi teemaksi. Tällä hetkellä EU:n *security*-tutkimus kärsii fragmentoitumisesta sekä laajuuden, päämäärien, yhteyksien ja yhteentoimivuuden puutteellisuudesta. *Security*-tutkimuksessa tarvitaankin nyt kansallisten ja kansainvälisten toimijoiden välistä yhteistyötä ja tiedonkulkua, jolla saadaan nostettua eurooppalaisen *security*-toimialan kilpailukykyä. Puiteohjelmassa tutkimus jaetaan seuraaviin alueisiin [Amended proposal…2006]:

- **Kansalaisten turvallisuus – suojautuminen terrorismia ja rikollisuutta vastaan:** teknologiset ratkaisut siviilien suojeluun
- **Infrastruktuurin ja yleishyödyllisten laitosten turvallisuus:** infrastruktuurijärjestelmien (esim. kuljetus, energia, ICT) ja palvelujen (taloudelliset ja hallinnolliset palvelut) analysointi ja turvaaminen
- **Tiedustelu** (*intelligence surveillance*) **ja rajaturvallisuus:** järjestelmien, kaluston, välineiden ja prosessien vaikuttavuutta ja tehokkuutta parantavat teknologiat sekä nopean identifioinnin menetelmät
- **Kriisienhallinta:** turvallisuuden palauttaminen kriisitilanteessa, monipuoliseen hätätilanteiden hallintaan, organisaatioiden väliseen koordinointiin ja kommunikointiin liittyvät teknologiat.

Aihealueita tukevat myös poikkitieteellisemmät teemat [Amended proposal…2006]:

- **Security-järjestelmien integrointi ja yhteensopivuus**
- **Turvallisuus ja yhteiskunta:** sosioekonomiset analyysit terrorismin ja rikollisuuden seurauksista, arvot, politiikka ja skenaariot liittyen rikollisuuteen, terrorismipsykologiaan ja sosiaaliseen ympäristöön. Systemaattiset riskianalyysit.
- **Security-tutkimuksen koordinointi ja rakenne.**

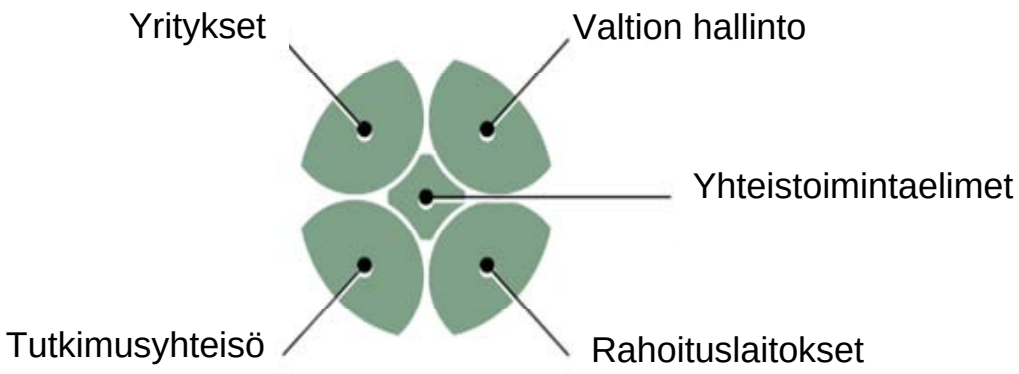
Suomessa myös Tekes on valmistelemassa turvallisuusteknologiaohjelmaa, joka todennäköisesti käynnistyy keväällä 2007. Tällä hetkellä Tekes selvittää suomalaisten yritysten ja tutkijoiden vahvuuksia turvallisuusalan kansainvälisillä markkinoilla. Työn perusteella päätetään, alkaako Tekes rahoittaa alan tutkimus- ja kehitystoimintaa oman teknologiaohjelman kautta. Mahdollisen teknologiaohjelman avulla lisätään turvallisuusalan tutkimusta ja tuotekehitystä sekä kasvatetaan turvallisuusalan liiketoimintaa ja kansainvälistä kilpailukykyä. Tässä vaiheessa Tekes tarkastelee turvallisuutta erittäin laajasti *safety*- ja *security*-näkökulmat huomioon ottaen. [Tekes 2006] Edellä mainittujen ohjelmien lisäksi *security* on sisällä useissa eri tutkimusaloja koskevissa ohjelmissa. Tällöin tutkimuksen hyödyt koskettavat joko suoraan tai välillisesti myös turvallisuuden kehittymistä.

USA:ssa *The Department of Homeland Securityn* (DHS) alainen toimisto *Homeland Security Advanced Research Projects Agency* (HSARPA) käynnisti joulukuussa 2003 ohjelman *Small Business Innovation Research (SBIR)*. Tavoitteena on lisätä innovatiivisten ja luovien pienyritysten osallistumista liittovaltioiden tutkimuksiin sekä T&K-projekteihin. Näin pyritään tuomaan innovatiivisia turvallisuusratkaisuja myös konkreettiselle tasolle. Lisäksi vuoden 2006 alussa alkoi ohjelma *HSARPA Small Business Technology Transfer (STTR),* jossa pienyritykset, yliopistot, tutkimuslaitokset toimivat partnereina tutkimus- ja kehitystyössä. Ohjelma kannustaa älykkäiden konseptien ja tutkimuksissa syntyneiden ideoiden siirtämistä pienyrityksiin. Keskeisiä tutkimusalueita ohjelmissa ovat [Homeland Security Advanced…2006]:

- kemialliset, biologiset ja radioaktiiviset aineet
- ydinaseaineet
- räjähteet
- kyber
- hätätilannevalmius ja -vaste
- rajaturvallisuus ja kuljetusten turvallisuus
- Informaatioanalyysit ja infrastruktuurin suojaaminen.

2.4 Klusterit

Klusterilla tarkoitetaan toisiinsa kytkeytyneiden yritysten ja yhteisöjen muodostamia maantieteellisiä keskittymiä. Klusterit muodostuvat keskenään sidoksissa olevien toimialojen yrityksistä, joiden keskinäinen vuorovaikutus tuottaa selvästi osoitettavissa olevia hyötyjä. Keskittymässä tuulee toimia riittävä määrä ydinyrityksiä ja niille palveluja tuottavia muita yrityksiä sekä T&K-toimintaa. Yritysten ohella klustereihin kuuluu myös muita kilpailun kannalta keskeisiä toimijoita ja yhteisöjä (Kuva 4). [Porter 1998; Viitanen et al. 2003; Virtanen & Hernesniemi 2005] Klusterissa on jatkuvasti muuttuva olotila, johon vaikuttavat myös sosiaaliset suhteet ja luottamus. Näkymättömillä sosiaalisilla suhteilla on usein suurempi merkitys kuin näkyvillä suhteilla. [Virtanen & Hernesniemi 2005]



Kuva 4. Klusterin muodostavat tahot [Sölvell et al. 2003].

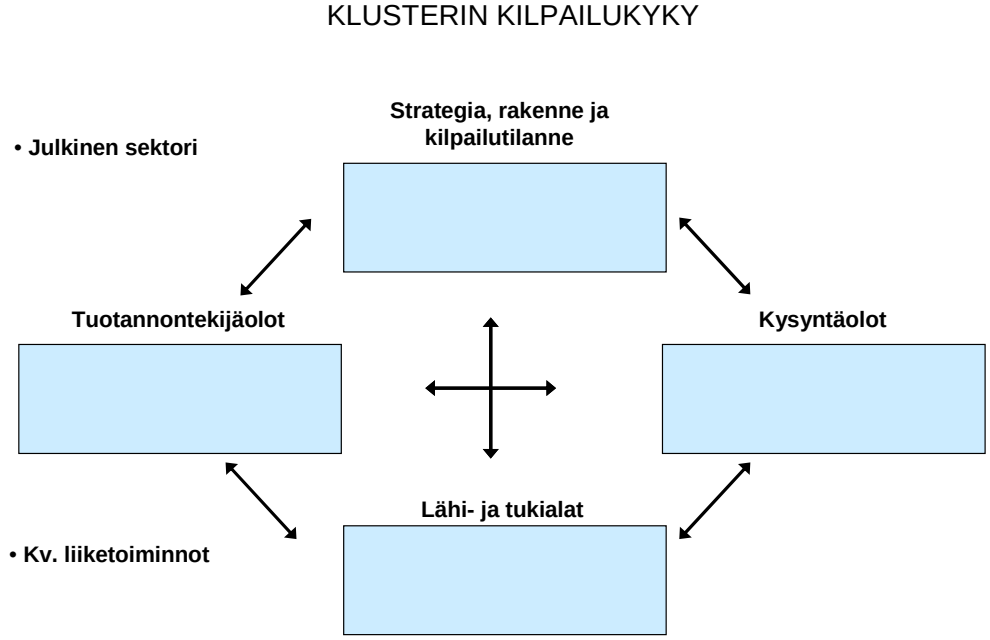
Klusteri toimii siihen kuuluvien tahojen dynaamisena kehitysblokkina. Se tarjoaa synergiaetuja, yhteisiä resursseja, kehittyneen infrastruktuurin, tuotannontekijöitä, erikoistumismahdollisuuden ydinosaamiseen, skaalaetuja, tietoa ja osaamista yli organisaatiorajojen sekä innovaatioita ja tehokkuutta synnyttävää kilpailua. Yritysten kyky luoda yhdessä lisäarvoa tekee klusterit kilpailukykyisiksi. Yritys voi myös kuulua useaan klusteriin samanaikaisesti. [Hernesniemi 2004; Virtanen & Hernesniemi 2005] Klustereiden menestys perustuu vaikeasti jäljiteltävään osaamiseen, innovointiin, verkostomaiseen yhteistoimintaan ja kommunikointiin sekä kovaan ja vapaaseen kilpailuun [Jääskeläinen 2001]. Toimintaan liittyy näin ollen samanaikaista kilpailua ja yhteistyötä [Hernesniemi 2004]. Klustereita on käytetty ennen muuta selvityksissä, joissa on pyritty esittämään, miksi jotkut maat ja niissä toimivat yritykset menestyvät toisia paremmin kansainvälisessä kilpailussa [Virtanen & Hernesniemi 2005]. Klusteritutkimukset Suomessa aloittivat Etla ja sen tytäryhtiö Etlatieto Oy vuonna 1992 [Viitanen et al. 2003].

Klusterin tunnistaminen alkaa yleensä elinkeinoelämän keskittymän tunnistamisesta. Klusterin syntymiseen kuitenkin tarvitaan toimintaympäristön myötävaikutusta, kuten sosiaalista, henkistä ja fyysistä pääomaa sekä toimintaympäristön järjestelmien sopeutumiskykyä. Lisäksi tarvitaan voimakasta erikoistumista, monipuolista tietovarantoa, osaamista sekä asiakaskytkentöjä. Jos keskittymä ja toimintaympäristö epäonnistuvat klusterin yhteisen vision luomisessa tai keskittymästä puuttuu vetovastuun kantava toimija, ei klusteri osaa järjestäytyä. Myös klusterin sisällä tarvitaan kykyä ja motivaatiota jakaa tietoa ja tehdä yhteistyötä, joka tähtää uusiin innovaatioihin ja tuottavuuden parantamiseen. [Virtanen & Hernesniemi 2005] Klustereita analysoitaessa tavoitteena on ensiksi tunnistaa avaintuotteet eli ne tuotteet ja tuoteryhmät, jotka ovat menestyneet kansainvälisessä kilpailussa, sekä toiseksi muodostaa näiden tietojen pohjalta klusterit, joiden yhteydessä kansainvälinen kilpailumenestys on syntynyt. [Viitanen et al. 2003]

Klustereihin liittyy myös kilpailukyvyn mallintaminen. Kilpailukykyä tulee lähestyä kokonaisvaltaisesti – systeemisellä tavalla. Yksittäisen kilpailukyvyn osan tai asian kehittäminen palvelee usein yksittäisen toimijajoukon intressejä mutta on harvoin hyödyksi klusterin muille toimijoille. [Porter 1998] Usein käytetty kilpailukyvyn malli on Porterin timanttimalli (Kuva 5), jossa korostuu neljän perusosan ja kahden ulkoisen tekijän keskinäisen vuorovaikutuksen tärkeys. Porterin timanttimallin neljää perusosaa ovat: kysyntäolot, tuki- ja lähialat, yrityksen strategia, rakenne ja kilpailutilanne sekä tuotannontekijäolot. Timanttimallin ulkoiset tekijät ovat julkinen valta ja sattuma. [Virtanen & Hernesniemi 2005] Porterin malli on osoittautunut toimivaksi ilmestymisensä jälkeen myös käytännössä. Klusterianalyysejä tehdään kymmenissä maissa. Erilaisten mallien ja niitä soveltavien asiantuntijoiden määrä on jatkuvassa kasvussa. [Sölvell et al. 2003]

Klusterin kilpailukyvyn kannalta edullisimpana pidetään tilannetta, jossa kotiseudun kysyntä on suuri suhteessa muiden kilpailevien seutujen paikallisiin markkinoihin. Tämä

heijastuu tuotesuunnitteluun, tuotantomenetelmiin, markkinointiin ja erilaisiin toimijoihin avainyritysten lähialoilla. Usein kotimarkkinoilla esiintyvät potentiaaliset asiakassegmentit kuitenkin laiminlyödään, jos saatavat myyntikatteet jäävät matalalle. Tällöin kotiseudun yritykset ovat haluttomia innovointiin, vaikka ulkomaiset kilpailijat jättävät markkinaosuudet keräämättä. [Porter 1990; Virtanen & Hernesniemi 2005] Asiakkaita voidaan segmentoida muun muassa maantieteen, ilmaston, luonnonvarojen, lainsäädännön, varotusjärjestelmän, viranomaismääräysten, jakelukanavien, sosiaalisten normien ja kansallisten himojen mikaan. Asiakkaita ovat myös arvoverkon muut yritykset. Yksittäisiä asiakassegmenttejä tärkeämpiä ovat kuitenkin segmenttien yhdistelmät. Kun kotimaiset asiakassegmentit edustavat samanaikaisesti kansainvälistä kysyntää, kysyntä-ikkuna kotiseudulla kuvaa myös laajaa segmenttiä vientimarkkinoilla. Kulttuuriin ja tekniikkaan yhdentyneet monikansalliset asiakasvaatimukset vahvistavat mahdollisuuksia. [Porter 1990; Virtanen & Hernesniemi 2005]



Kuva 5. Klusterin kilpailukyvyn timanttimalli [Porter 1990].

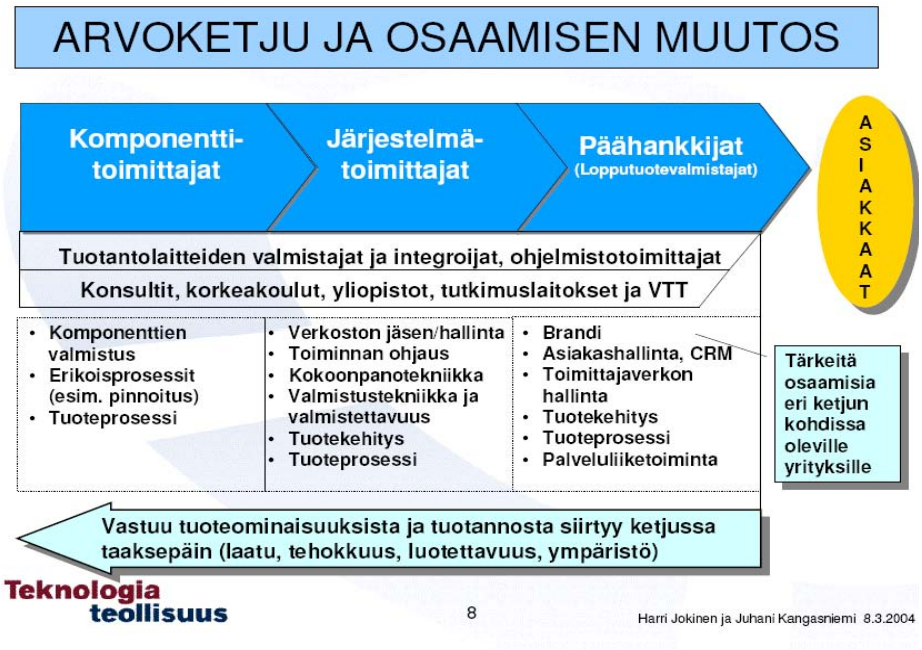
Klusterille suotuisia olosuhteita voidaan luoda esimerkiksi julkisten ja yksityisten koulutusjärjestelmien avulla, kannustusohjelmilla, julkisilla ja yksityisillä tutkimusjärjestelmillä sekä infrastruktuuria kehittämällä. Erityiset olosuhteet vaativat suhteellisesti suurimmat ja pitkäkestoisimmat investoinnit. Kilpailuedun aikaansaamiseksi myös yksityisen sektorin tulee osallistua olosuhteiden luontiin. Tavallisesti julkinen taho panostaa perus- ja yleisolosuhteiden luomiseen. Panostus kuitenkin epäonnistuu, jos yrityspuolella ei ole julkisen tuen vastaanottorakennetta. Parhaana vaihtoehtoehtona pidetään julkisen tahon yritysten, kaupallisten yhdistysten ja yksilöiden yhteistä osallistumista olosuhteiden luontiin. Koska kaikkia otollisia olosuhteita ei voida luoda, arvioidaan tarpeita timanttimallin perusosien keskinäisen vuorovaikutuksen kautta. Arviointi kohdistuu sii-

hen, miten kotimarkkinoiden kysyntä, avainyritysten lähi- ja tukialat, avainyritysten tavoitteenasettelu ja strategia sekä kotimaan kilpailuolosuhteet kykenevät tukemaan tuotannontekijäolosuhteiden luomista. [Porter 1990; Virtanen & Hernesniemi 2005] Innovaatioympäristön tukijärjestelmissä tunnistetaan tyypillisesti kolme erilaista painotusta [Virtanen & Hernesniemi 2005]:

1. teknologian kehittäminen yrityskeskeisinä kehitysprosesseina
2. liiketoimintaosaamisen kehittäminen yrityskeskeisinä kehitysprosesseina
3. systeeminen kehittäminen yritysverkostojen ja innovaatioympäristöjen kehittämisprosesseina – klusteriprojektit/klusteriohjelmat/yhteisöprojektit.

Klusterin järjestäytyminen tapahtuu luonnollisella tavalla ilman vakiintunutta prosessia. Koordinointia tarvitaan kuitenkin useiden erilaisten toimijoiden yhteistyön organisointiin. Klusterin muodostamisen lähtökohtana ovat usein tiettyä avaintuotetta valmistavat yritykset, jotka muodostavat klusterin ytimen. [Viitanen et al. 2003] Tärkeää on käsitys siitä, mitkä tuotteet markkinoilla yhdessä muodostavat liiketoiminta-alueita. Vaihtoehtoinen tapa on toimialakeskeinen lähestymistapa. Tällöin pohditaan, mitkä voisivat olla ne eri klustereiden potentiaaliset ydintoimialat, joiden ympärille klusterit todennäköisimmin ovat kehittyneet tai voivat kehittyä. Tällöin tärkeää on käsitys siitä, mitkä toimialat yhdessä muodostavat liiketoiminta-alueita. [Virtanen & Hernesniemi 2005] Klusteriin muodostuu myös erilaisia lähi- ja tukialojen yrityksiä avaintuotteita tuottavien yritysten kysynnän seurauksena [Viitanen et al. 2003]. Vahvat lähi- ja tukialat tuovat tarjolle täydentäviä tuotteita ja palveluja. Lisäksi kansainvälisesti toimivat vahvat lähi- ja tukialat avaavat myös vientimarkkinoita. [Virtanen & Hernesniemi 2005] Tukialaksi katsotaan yritykset, joiden tuotoksia klusterin ydinyritykset tarvitsevat panoksina omassa toiminnassaan [Porter 1990; Virtanen & Hernesniemi 2005].

Arvoketjun, yhteisten toimintojen ja viestinnän myötä klusterin osapuolet ja ympäristö oppivat tunnistamaan klusterin ominaisuudet. Järjestöt toimivat katalyyttinä kansallisen kilpailukyvyn lisäämisessä sekä auttavat hankealoitteiden jalostamisessa ja keskustelufoorumien muodostamisessa. Arvoketjujen hahmottaminen on välttämätön askel klusterin jäsentelyn aloittamisessa. [Virtanen & Hernesniemi 2005] Kuvassa 6 on TRIO-toimenpideohjelmassa esitetty Harri Jokisen ja Juhani Kangasniemen pohdinta arvoketjusta ja osaamisen muutoksesta. TRIO on suunnattu kansalliselle teknologiateollisuudelle ja tarkoitettu yritysten sekä yritysverkostojen kilpailukyvyn parantamiseen kehittämällä samanaikaisesti ja laaja-alaisesti kansainvälistymistä, liiketoimintaosaamista sekä teknologiaa.



Kuva 6. Arvoketju [Jokinen & Kangasniemi 2004].

Toimittajan ja asiakkaan välinen kontaktipinta klusterissa jäsentyy avaintuotteiden avulla. Asiakkaalla on keskeinen vaikutus innovaation syntymiseen, ja vaativa asiakas on klusterille arvokas. Jalostusarvoa tai osaamisintensiivistä lisäarvoa voi lisätä palveluissa ja tavarahankinnoissa. Asiakas (kuluttajat, yritykset, julkinen taho) voi vaikuttaa omia hankintakäytäntöjään kehittämällä klusterin laajuuteen. Kasvua tukee kansainvälisen kysynnän ennakointi, ja innovaatioprosessia nopeuttaa toimittajayhteistyö. [Virtanen & Hernesniemi 2005]

3. Toteutus

Julkaisu on toteutettu osana VTT:n sisäistä Yhteiskunnan ja elinkeinoelämän turvallisuuden varmistaminen (*Security*-VTT) -hanketta. Hankkeesta on aiemmin julkaistu *Security*-tutkimuksen roadmap [Naumanen & Rouhiainen 2006]. Security-klusterin hahmottamiseen tähtäävä tutkimuksen osa on toteutettu 2.4.–31.12.2006. Hankkeen ohjausryhmänä toimi Security-KTA:n ydintiimi, johon kuuluivat Veikko Rouhiainen, Veikko Komppa, Arto Juhola, Markku Jenu, Laura Raaska, Auli Lastunen, Osmo Auvinen ja Reijo Savola.

Security-klusterin hahmottaminen toteutettiin kirjallisuustarkastelun sekä luottamuksellisten yrityshaastattelujen avulla. Tässä julkaisussa yrityshaastatteluista on hyödynnetty vain yleinen tieto, jonka yritykset ovat hyväksyneet julkisesti julkaistavaksi. Kokonaisuudessaan klusterin hahmottamisen keskeiset osatehtävät olivat:

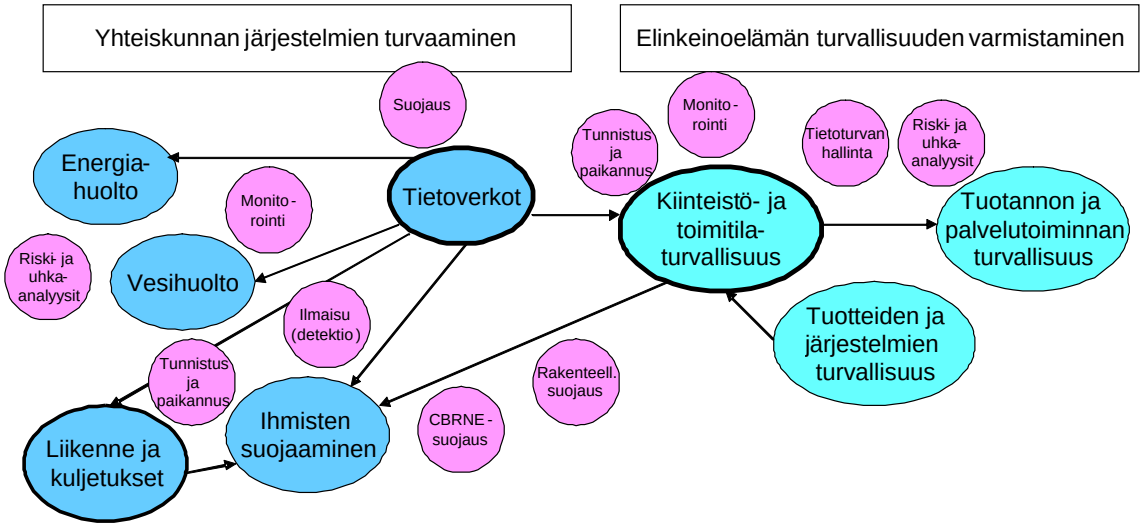
1. Klusterin mallintamistavan valinta
   Tutustuttiin erilaisiin klusterimalleihin ja valittiin sopiva lähestymistapa *security*-klusterin havainnollistamiseen.

2. *Security*-alan toimijoiden hahmottaminen
   Security-alueella toimivien yritysten ja julkisten organisaatioiden kentän hahmottamisessa hyödynnettiin alan järjestöjen luokituksia, kirjallisuutta ja artikkeleita, eri yritysten www-sivuja (yritykset, jotka markkinoivat *security*-tuotteita ja palveluja), VTT:n kontakteja sekä yrityshaastatteluiden aineistoa.

3. *Security*-markkinoiden tunnistaminen
   Turvallisuuteen liittyvien teknologiapalvelujen tuottajaverkostojen muodostumista sekä palvelujen ostajien tarpeita selvitettiin ensisijaisesti yrityshaastatteluilla sekä *security*-alan markkinaraporttien tiivistelmiin tutustumalla.

4. Klusterin hahmottaminen
   Klusterin rakennetta, toimijoita ja vuorovaikutussuhteita kuvattiin karkealla tasolla.

Haastatellut yhdeksän yritystä valittiin VTT:n *Security*-tutkimuksen roadmapin [Naumanen & Rouhiainen 2005] toiminta-alueiden avulla (Kuva 7). Yritykset kuitenkin edustivat yksittäisiä toimintoja ja antoivat näin vain tietyn kuvan turvallisuusalalla toimivista yrityksistä.



Kuva 7. Keskeiset toiminta-alueet (sininen) ja teknologiat (punainen) VTT:n security roadmapin pohjalta.

4. Security toimialana ja markkinoina

4.1 Toimiala ja toimijat Suomessa

Koska turvallisuusala on sisällöltään vakiintumaton käsite, turvallisuusalalla toimivien yritysten määrää voidaan vain arvailla. Suomen virallisissa tilastoissa esiintyy toimialaluokitus ”Vartiointi- ja turvallisuuspalvelut”, mutta tämä toimiala edustaa vain osaa turvallisuuteen liittyviä tuotteita ja palveluja tarjoavista yrityksistä. Finnsecurity ry:n [2006] teettämän selvityksen mukaan kyseisellä toimialalla toimii Suomessa 360 yritystä, joista 80 % työllistää alle viisi henkilöä. Kyseisen selvityksen mukaan yritysten tuottamien turva-alan tuotteiden ja palvelujen arvo (liikevaihto) oli Suomessa noin miljardi euroa vuonna 2005. Alan liikevaihto koostuu hyvin laaja-alaisesta tuote- ja palveluvalikoimasta, josta merkittävimpiä ovat vartiointipalvelut, rakenteelliset turva-alan tuotteet ja sähköiset turvajärjestelmät. Merkitystään kasvattaneita aloja ovat hälytyskeskus- ja etävalvontapalvelut ja erityisesti tietoturvallisuuteen liittyvät tuotteet ja -palvelut. Selvityksen mukaan ulkomailla toimivat turvallisuusalan yritykset harjoittavat lähinnä teollisten tuotteiden valmistusta sekä tukkukauppaa. Alan perinteisillä palveluyrityksillä kansainvälisen toiminnan merkitys on sen sijaan ollut vähäistä. [Finnsecurity 2006] Edellä mainittujen tietojen yleistettävyyttä on kuitenkin vaikea arvioida koko turvallisuuteen liittyvän liiketoiminnan kannalta, sillä selvityksestä julkaistussa tiivistelmässä ei ilmoiteta tarkemmin arvioinnin rajauksia ja yrityskyselyihin osallistuneiden määrää.

Yleisesti kansainväliset suuryritykset ovat varsin riippuvaisia korkeatasoisista turvallisuuspalveluista. Tietoturvallisuuden sekä kiinteistö- ja toimitilaturvallisuuden alueella toimii useita palveluntarjoajia. Yksityinen turvallisuus- ja turva-ala on jo henkilömäärältään poliisia suurempi turvallisuusresurssi. Yritysten liikevaihto on kasvussa, ja suunta on kohti suurempia yrityksiä. Suuri osa järjestyksen valvontaan ja murtohälytyksiin liittyvästä toiminnasta on siirtynyt yksityiselle puolelle. Turvallisuus- ja turva-ala on myös merkittävä tietoyhteiskunnan toimija suurine tuotekehitys- ja teknologiapanostuksineen. Toimitilaturvallisuuden toteuttaminen edellyttää yhä enemmän yhteistyötä eri osapuolten välillä. [Hakala 2004; Leskinen 2004; Savola 2004]

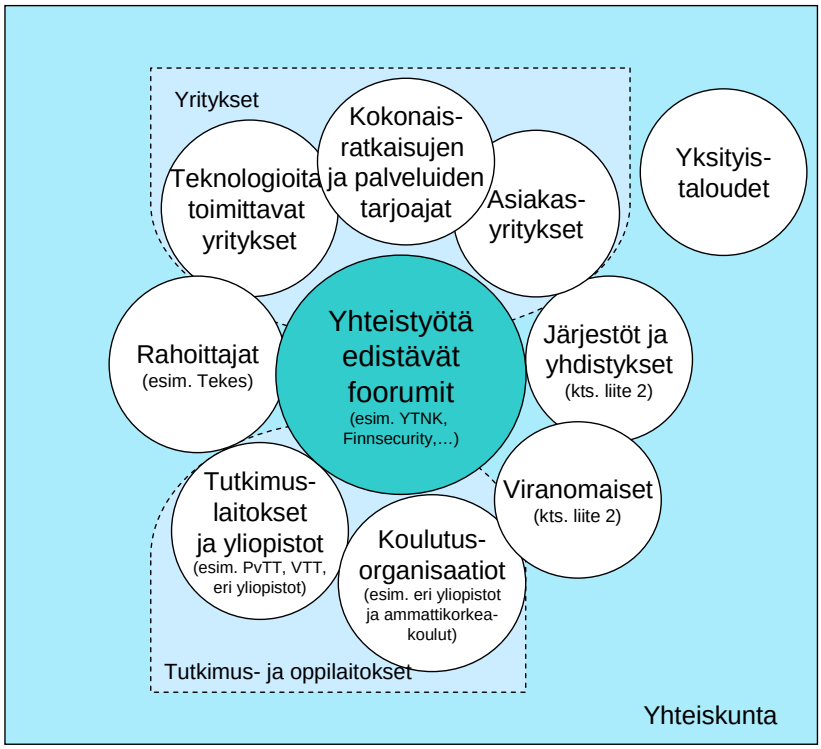
Finnsecurity ry:n Turvallisuusalan vuosikirjan [2004] mukaan turva-alalla toimii noin 550 yritystä ja se kasvaa voimakkaasti. Alalla toimii esimerkiksi vartiointiliikkeitä, lukkoliikkeitä, teknisten järjestelmien toimittajia (mm. kameravalvonta-, rikosilmaisin-, hälytyksensiirto-, paloilmoitin-, kulunvalvonta- ja integroidut järjestelmät), konsultteja ja kouluttajia, yksityisetsiviä, kuriiriyhtiöitä, rakenteellisen turvallisuuden urakoitsijoita ja turvalaitteiden myyjiä (esim. turvakaapit, aseet, radiopuhelimet, viranomaistarvikkeet). Edellä mainitun listan perusteella järjestön jäsenissä painottuu etenkin kiinteistöturvallisuuden näkökulma. Suuria toimijoita ovat muun muassa Abloy, G4S Security Services, Securitas, ISS Security, Fsecure ja SecGo. Alalla kuitenkin toimii paljon myös pieniä yrityksiä.

Turvallisuusalalla toimii useita järjestöjä ja yhdistyksiä, joista löytyy lista esimerkiksi sivustolta http://www.turvallisuus.net. Eräänä yrityslähtöisten turvallisuusnäkemyksen yhdistäjänä toimii Yritysturvallisuuden neuvottelukunta (YTNK), joka on Elinkeinoelämän keskusliiton EK:n sekä sen jäsenliittojen ja -yritysten yhteistyöorganisaatio. Neuvottelukunnan jäsenet edustavat laajasti ja monipuolisesti jäsenyritysten turvallisuusjohtoa ja koko yritysturvallisuuskentän asiantuntemusta. Neuvottelukunnan perustehtävänä on huomion kiinnittäminen yritysten turvallisuusriskeihin ja turvallisuusasioiden kokonaisvaltaiseen toteuttamiseen, turvallisuusjohtamisen kehittäminen yhdessä jäsenyritysten ja sidosryhmien kanssa sekä ajankohtaisen turvallisuustiedon vieminen yrityksiin. Myös Suomen Pelastusalan Keskusjärjestö (SPEK) korostaa yhteistyötä. SPEKillä on merkittävä asema pelastusalan kehittäjänä yhteistoiminnassa alueellisten pelastusliittojen ja alan viranomaisten kanssa. Lisäksi turvallisuuskentällä toimivat vakuutusyhtiöt. Vakuutusyhtiöiden yhteistyötä toteutetaan muun muassa Suomen Vakuutusyhtiöiden Keskusliiton (SVK) kautta.

Viranomaispuolella turvallisuusasioiden hoito on hajaantunut useiden eri ministeriöiden alle (Liite A). Viranomaisten keskinäinen yhteistyö on eräs haaste turvallisuusalan kehittymisessä. Myös tietojen vaihdon merkitys yksityisen ja julkisen sektorin välillä on korostunut erityisesti Euroopan Unionissa. Useiden unionin jäsenmaiden sekä koko unionin tavoitteeksi on asetettu tietoon ja analyysiin perustuvan toiminnan ohjausmallin käyttöönotto sisäisen turvallisuuden alueella. Ohjausmallissa olennaista on ajantasaisen ja kattavan tiedon saaminen päätöksenteon ja toiminnan ohjauksen tueksi. Viranomaisten hallussa oleva tieto ei yksin riitä kattavan kokonaiskuvan muodostamiseksi rikollisuustilanteesta ja sen tulevasta kehityksestä, vaan siihen tarvitaan myös yritysten hallussa olevaa tietoa. Tämä on erityisen tärkeää yrityksiin kohdistuvien uhkien tunnistamiseksi ja niihin kohdistuvien rikosten torjumiseksi. [Elinkeinoelämän… 2006]

Security-alalla toimii myös tutkimuslaitoksia ja yliopistoja. Puolustusvoimien teknillinen tutkimuskeskus (PvTT) on keskittynyt puolustusvoimateollisuuden teknologioiden tutkimiseen. Myös VTT:llä on runsaasti *security*-aihealueella sovellettavissa olevaa osaamista [Naumanen & Rouhiainen 2006]. Eri yliopistot ja oppilaitokset ovat muodostaneet yhteisiä turvallisuuteen liittyviä koulutusohjelmia. Uusi kiinnostava klusteri on syntymässä Kymenlaakson alueelle. Turun yliopisto, Kymenlaakson ammattikorkeakoulu, Teknillinen korkeakoulu, Helsingin yliopisto, Lappeenrannan teknillinen yliopisto sekä kesäyliopisto muodostavat korkeakouluverkoston, joka perustaa ”Kuljetusketjun riskienhallinta” -hankeohjelman. Kyseiseen klusteriin liittyvät myös viranomaiset (mm. tulli ja merenkulkulaitos), alueen yritykset sekä päättäjät. Klusteri tuottaa uutta tietoa ja osaamista päätöksenteon tueksi, tukee viranomaisia muutoksessa, tekee aktiivista yhteistyötä, lisää alueen kasvua palvelemalla yrityksiä, lisää vaikutusalueensa turvallisuutta sekä edistää hyvien käytäntöjen käyttöön ottoa. Yleisesti keskeisenä kotimaisena julkisena rahoittajana *security*-toimijakentässä on lähinnä Tekes. Käyttäjänä, asiakkaana,

tutkimuskohteena ja vaikutusten kohteena myös yksilöllä ja yhteiskunnalla on rooli toimijakentässä.



Kuva 8. Securityyn liittyvät toimijatahot Suomessa.

Suomen vahvuutena *security*-markkinoilla toimimisessa voidaan pitää [Rintakoski 2006]:

- viranomaisten välisen sekä viranomaisten ja yritysten välisen yhteistyön toimivuutta
- sellaista kulttuuria ja arvoja, jotka tukevat turvallisuuden ylläpitämistä,
- luottamusta viranomaisiin
- kansainvälistä ja kansallista kokemusta kriisienhallinnasta
- sekä teknologiaan että toimintatapoihin keskittyvää innovaatiotoimintaa
- turvallisuusteknologiaan liittyviä palveluja (mm. koulutusta), jotka luovat liiketoimintaa,
- toimintamallien ja kokonaisratkaisujen tuottamista yksittäisten teknologioiden sijaan.

4.2 Toimiala ja markkinat kansainvälisesti

Hankkeessa *security*-aihealueen markkinaraportteihin tutustuttiin varsin pinnallisella tasolla ja usein käytiin läpi vain tiivistelmä sekä sisällysluettelo. Lisäksi hyödynnettiin VTT:n tietopalvelun vuonna 2006 laatimaa julkaisematonta markkinointiraporttikoostetta. Markkinaraporttien teemoja tarkasteltaessa tietoturvallisuuteen sekä verkkojen ja Internetin turvallisuuteen liittyvät aihealueet otettiin muusta *security*-kentästä omaksi alueekseen. Tietoturvallisuudesta on tehty runsaasti erillisiä markkinatutkimuksia, joissa kyseistä aihealuetta käsitellään spesifisellä tasolla. Näihin spesifisiin raportteihin ei tässä tutustuttu.

Eri markkinatutkimuksissa ja yhteenvedoissa esiintyy erilaisia toimialaa, markkinoita ja teknologioita eritteleviä jakoja. Tässä julkaisussa osa jaotteluista ja termeistä on päädytty esittämään englanniksi, jotta alkuperäinen ajatus on jokaisen lukijan tulkittavissa. Seuraavassa on listattu joitakin usein esiintyneitä teemoja [mm. Frost & Sullivan 2006; Homeland Security Research 2006; Country industry…2004]:

- CBRN-dekontaminaatio
- *screening*-teknologiat (mm. paketit ja matkatavarat, rahti, ihmiset aseiden ja räjähteiden tunnistamiseksi, jne.)
- ydinmateriaalin ja säteilevän aineen tunnistaminen
- kemiallinen ja biologinen detektointi
- puolustusvälineteollisuus
- biometriikka ja henkilön tunnistaminen (sormenjälki, iiris, kasvot)
- fyysinen (aineellinen) turvallisuus (mm. *intrusion detection, CCTV=closed circuit television, electronic access control*)
- videovalvonta
- RFID-teknologia
- tietoturvallisuus (*information ja data*)
- Internet-järjestelmien turvallisuus
- *networking security*
- palomuurit.

USA:n sisämarkkinoiden tutkimuksessa markkinat on jaettu seuraaviin kategorioihin [Frost & Sullivan 2006]:

- *Port of Entry Markets – Airports and Seaports*

- *Water and Wastewater Treatment Plant Markets*
- *Energy Supply Markets – Nuclear, Hydroelectric (Dams) and Fuel Pipelines*
- *Chemical and Biomedical Facility Markets and Transportation Markets – Bridges and Tunnels.*

Defence & security -teeman alle puolestaan on nostettu seuraavia segmenttejä [Growth Partnership…2006]:

- *Electronic Warfare: World Airborne RF Self Protective Systems and Decoy Market*
- *United States Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Markets*
- *United States Homeland Defence*
- *World Chemical and Biological Warfare Detector Markets*
- *World Military, Civil, and Commercial Unmanned Aerial Vehicle (UAV) System Markets*
- *World Military and Government High Assurance Network and Data Encryptor Market*
- *Other Related Markets.*

Thomson Business Intelligence -tietokannasta, johon on koottu 170 markkinatutkimuslaitoksen tutkimukset, löytyi kahden viime vuoden ajalta useita *security*-toimialan markkinatutkimuksia. Alla on lista julkaistujen markkinatutkimusten määrästä teemoittain.

- *Security Systems & Services* (667 kpl)
- *Information & Data Security* (525 kpl)
- *Internet Security* (450 kpl)
- *Networking Security* (424 kpl)
- *Firewalls* (230 kpl)
- *Physical Security* (89 kpl)
- *Virtual Private Network & Virtual LAN* (85 kpl)
- *Personal Identification & Biometrics (*55 kpl)
- *Homeland Security* (54 kpl)
- *Encryption Technology* (43 kpl)
- *Proxy Server Software* (4 kpl).

Myös kodin automaatio -markkinoilla *security*-teknologiat on tunnistettu yhdeksi osa-alueeksi. *Security*-osakkeet ovat kuitenkin laskeneet ja erityisesti yrityksissä, joissa on panostettu kodin *securityyn*. Esimerkiksi sormenjälkitunnistejärjestelmän kehittäneen yrityksen *Cognent*in osakkeet ovat pudonneet 41 % vuonna 2006. Räjähteitä tunnistavien

röntgenlaitteiden valmistaja *American Science and Engineering*in osakkeet ovat puolestaan laskeneet 24 %. S*ecurity*-alan kysyntä on varsin vaihtelevaa, ja todellisuudentajun pitäminen markkinoilla on tärkeää. [Steinman 2006]

Amerikkalaisissa ja eurooppalaisissa *security*-alan markkinatutkimuksissa on joitakin eroja. Esimerkiksi amerikkalaisissa selvityksessä käsitellään paljon CBRNE-aineiden (kemialliset, biologiset, radioaktiiviset, ydinmateriaalit, räjähteet) detektointia, suojautumista ja puhdistamista, mutta eurooppalaisissa *Industry Forecast* -selvityksissä [Country industry…2004] tämä aihealue jää käsittelemättä. Toisaalta uusimmissa Euroopan markkinoita käsittelevissä raporteissa [European Homeland…2005] on mukana *screening*, joka saattaa pitää sisällään myös detektoinnin. Amerikkalaisten selvitysten tiivistelmissä käytetään myös termiä *Homeland Security* selittämättä tarkemmin tämän alle lukeutuvia teknologioita tai toimintoja. Euroopan teollisia ja kaupallisia *security*-tuotteita ja -järjestelmämarkkinoita käsittelevässä selvityksessä [European Industrial…2005] sen sijaan esiintyy seuraavat teemat: palontorjuntaan, häiriöiden estoon (*Intrusion Detection Equipment),* kulunvalvontaan ja CCTV:n liittyvät välineet. Eurooppalaisessa *Homeland Securityyn* kohdistuvassa *Market Opportunity* -analyysissä on keskitytty erityisesti biometriikkaan, seulontaan (*screening*), RFID:hen ja fyysiseen turvallisuuteen (*physical security*). Taulukossa 1 esitetään joitakin markkinoita kiihdyttäviä ja hidastavia asioita.

Amerikkalaisen *Homeland Security Research*in [2006] tekemän selvityksen mukaan vuosina 2006–2015 maailmanlaajuisen täyden puolustuksen (*total defense*) kustannusten (*military, intelligence community, and Homeland Security/Homeland Defense*) ennustetaan nousevan noin 50 % (1 400 mrd. $:sta 2 054 mrd. $:iin). Maailmanlaajuisen *Homeland Securit*yn (myös yksityinen sektori) kustannusten ennustetaan kasvavan noin 100 % (231 mrd. $:sta 518 mrd. $:iin). Markkinoiden sen sijaan uskotaan kolminkertaistuvan eli kasvavan 60 mrd. $:sta 180 mrd:iin. USA:n *Homeland Security* -liittovaltioiden viraston T&K-rahoitus jakautuu siten, että suurimmat panostukset kohdistuvat aihealueisiin: biopuolus (yli 2,5 mrd. $), *intelligence & warning* (yli 1,5 mrd. $), radioaktiiviset ja ydinmateriaalit (noin 0,75 mrd. $) sekä *agro / food* (noin 0,7 mrd. $). Tarkemmat diagrammit aiheesta löytyvät *Homeland Security Research*in sivustolta: http://homelandsecurityresearch.com. CBRN-dekontaminaatioteknologian osalta rahoituksen on arvioitu kaksinkertaistuvan vuosien 2006 (220 milj. $) ja 2012 välillä [Homeland Security Research 2006].

Taulukko 1. Security-markkinoihin vaikuttavia tekijöitä.

	Kiihdyttävät	Hidastavat
Biometriikka	- lentoturvallisuuden kehittyminen - matkustajamäärien lisääntyminen - uusille ideoille avoin hallinto - suuret mahdollisuudet matkailu- ja kuljetusprojekteista - yleinen tietoisuuden ja hyväksynnän lisääntyminen - älykorttien ja biometrian kehitys - EU-säädökset	- vaikea osoittaa investointien tuottamia tuloja - huoli yksityisyyden suojasta - USA:n kongressin MRTD-takarajan pidennys - toimintakykyyn sidotut asiat - kilpailevat vaihtoehdot - riittävien standardien puute - EU:n talouden hidastuminen
Screening	- uhat ja uhkakuvat - konttien screenauksen osuuden vähäisyys - teknologian kehitys kasvattanee markkinoita - IRAQ - monikäyttöisyys	- teknologian kustannukset - markkinavaatimukset sidottu terroristien määrään
RFID	- tarve lisätä toimitusketjun tehokkuutta - hintojen laskun vahvistuva vaatimus - tulevaisuuden security-aloitteet - security-sovellusten lisääntynyt kehitys - korkean volyymin mahdollisuudet	- markkinarajoitukset - standardoinnin puute - kustannus-hyötysuhdeanalyysien puute - vapaaehtoisuus tai pakko

European Homeland Security - A Market Opportunity Analysis. 2005. Frost & Sullivan.

Homeland Security Research [2006] on tehnyt myös erillisiä markkinaselvityksiä *security*-teemaan kuuluvista aihealueista, kuten konttien ja matkatavaroiden tarkastamisesta, CBRN-dekontaminoinnista, radioaktiivisten aineiden tunnistamisesta ja biodetektoinnista. Esimerkiksi biodetektoinnin ensimmäisen ja toisen sukupolven teknologioiden ennustetaan väistyvän kolmannen sukupolvien teknologian yleistyessä. Teknologia kehittyy etenkin selektiivisyyden, herkkyyden ja nopean vasteen osalta. Myös kalliiden reagenssien tarve vähenee. Kolmannen sukupolven teknologioiden ennustetaan lyövän läpi vuosina 2008–2012, jolloin ensimmäisen ja toisen sukupolven teknologian markkinat romahtavat.

USA:ta koskevia markkina-arvioita löytyy esimerkiksi seuraavilta alueilta [Ratliff 2005]:

- 400 miljoonan $:n *security*-anturimarkkinat 2005
- 800 miljoonan $:n videoanalyysimarkkinat 2009 mennessä
- 10 mrd. $:n biometriikkamarkkinat 2007 mennessä
- 36 mrd. $:n fyysisen turvallisuuden (*physical security)* teknologiamarkkinat (mm. *body armor* ja räjähteiden seulonta) 2007 mennessä
- *security*-kokonaismarkkinoiden arvio vuonna 2005 oli 200 mrd. $.

USA:n *Department of Homeland Security*n budjetti on Civitas Groupin tietojen mukaan lähes 50 mrd. $, ja tästä 9,5 mrd. $ on mahdollista suunnata yksityiselle sektorille (hakumenettely). Näin ollen DHS on suurin yksittäinen *disaster-related*-teknologioiden rahoittaja. Eräs kiintoisa näkökulma on se, että USA:n hallitus käyttää miljardeja tu-

keakseen sekä yksityisyyden suojaa heikentävän (videovalvonta ja datalouhinta) että parantavan (*encryption, network security* ja *anonymization applications*) teknologian tutkimusta ja kehitystä. [Ratliff 2005]

4.3 Esimerkkejä alan yrityksistä ja yritysverkostoista

Tässä esitellään esimerkinomaisesti joitakin yrityksiä, jotka voidaan liittää *security*-alaan. Tiedot ovat peräisin yritysten kotisivuilta, julkisista esitteistä sekä lehtiartikkeleista. Lisäksi selkeästi muilla päätoimialoilla toimivia, turvallisuutta lisäarvona myyviä yrityksiä löytyy useita, esimerkkinä kuljetuspalveluyritykset.

Abloy Oy

Abloy Oy:n kotisivulla yritys kuvaillaan johtavaksi lukko- ja rakennushelavalmistajaksi ja sähköisen lukitusteknologian edelläkävijäksi. Yritys kehittää, valmistaa ja markkinoi mekaanisia ja sähkömekaanisia rakennus-, laite- ja riippulukkoja, ovensulkimia ja ovi-automatiikkaa sekä rakennusheloja. Abloy Oy kuuluu Assa Abloy -konserniin, joka on maailman johtava lukitusratkaisujen valmistaja ja toimittaja. Konkreettisia tuotteita ovat mm. mekaaniset tuotteet, modulaariset alustat, elektromekaaniset tuotteet, automaattiovet, tunnistaminen ja pääsyn hallinta, hotelliturvallisuusratkaisut sekä turvaovet. [http://www.abloy.fi/]

ASAN Security Technologies Oy

ASAN Securityn kotisivulla yritys kuvataan johtavaksi integroitujen visuaalisten valvonta- ja tunnistusratkaisujen toimittajaksi, joka toimii valikoiduilla vertikaalisilla kansainvälisten markkinoiden segmenteillä. Yritys kehittää standardipohjaisia ohjelmisto-teknologia-alustoja ja -tuotteita, jotka mahdollistavat integroitujen visuaalisten valvontaratkaisujen luomisen ja toimittamisen. [http://www.asansecurity. com/] ASANin videovalvontajärjestelmässä kuvaus, tallennus, seuranta ja hallinta suoritetaan olemassa olevan tietoliikenneverkon ja tavallisen Internet-selaimen kautta. ASAN-videovalvontajärjestelmään voidaan kytkeä joko kiinteästi tai langattomasti sekä analogisia että digitaalisia valvontakameroita, IP-kameroita. [Suomen Teollisuussijoitus Oy 2006]

ASANilla on *Integration and Technology Partner Program*, joka on mahdollistaa asiakkaalle eri toimittajien integroitujen ratkaisujen toteuttamisen. Partneriohjelmaan kuuluu useita IP-laitteiden sekä integroinnin kumppaneita. Teknologiakumppaneiden lisäksi yhtiöllä on useita toimittajakumppaneita, joihin kuuluvat muun muassa Securitas Systems Oy, Oy Hedpro Ab, Turvatiimi Oyj ja Nordic Lan & Wan Communication Oy. [http://www.asansecurity.com/]

Bewator Finland

Bewator Oy kuuluu Bewator Group -yhtymään, joka on yrityksen kotisivujen mukaan johtava kansainvälinen turvallisuuteen ja kulunohjaukseen erikoistunut yritysryhmä. Frost & Sullivanin mukaan Bewator sijoittuu Euroopan kolmen johtavan kulunohjausvalmistajan joukkoon sekä Skandinavian ykköseksi. Turvatuotteiden valikoimaan kuuluvat muun muassa kulunohjauksen ratkaisut, palo- ja rikosilmoituksen sekä videovalvonnan kokonaisjärjestelmät. Tuotteita markkinoidaan maailmanlaajuisesti noin 50 maassa sekä omien yhtiöiden että kansainvälisen jakeluverkoston kautta. Projektisuunnittelu, asennus ja tuotekoulutus suoritetaan maailmanlaajuisen verkoston kautta, joka koostuu yli 10 000 turvajärjestelmäasentajasta ja yhteistyökumppanista. Vuonna 2005 Bewator myytiin Siemens Building Technologiesille, mutta Bewator jatkaa kuitenkin saman tuotenimen alla. [http://www.bewator.com/fi/]

Environics Oy

Environics kuuluu Finntemet Group -konserniin. Environicsin tarjoaa asiakkailleen tilannetietoisuutta ja seurausten hallintaa tuotteinaan CBRN-anturit ja -ilmaisinlaitteet, integroidut verkot sekä CBRN-tiedusteluvälineet. Environicsin keskeisiä tuotteita ovat esimerkiksi kannettavat CWA-detektorit, kädessä pidettävät kemikaalidetektorit, CWA-detektorijärjestelmät autoihin, laivoihin ja kiinteisiin sovelluksiin, integroidut moniantujärjestelmät sekä lisälaitteet, palvelut ja varaosat. [http://www.environics.fi/] Yrityksen menestystuote on matkapuhelinta muistuttava taskukokoinen analysaattori. Sen myynnistä kertyi 80 % viime vuoden 16 miljoonan euron liikevaihdosta. Tärkeää yhtiölle on ollut myös Nato-kelpoisuuden antavan aqap-standardin saaminen. Yrityksen pääasiakkaita ovat eri maiden viranomaiset. Environics käyttää tuotekehitykseen 25 % liikevaihdostaan. [Repo 2006]

Environics kuuluu security-alalla toimivaan yhdeksän yrityksen CBRN Finland -allianssiin, johon kuuluvat myös Temet Oy, Mavatech, M. Vahamaa Oy, Vaisala Oy, Dekati Oy, Suojasauma Oy, Rados Oy ja Kiitokori Oy. Nämä yritykset edustavat vahvasti puolustusvoimiin liittyvää liiketoimintaa. Verkottumalla yritykset pyrkivät vastaamaan kasvaviin tarpeisiin kehittää CBNR-uhilta (kemialliset, biologiset ja radioaktiiviset aineet) suojautumiseen liittyviä tuotteita. Asiakaskunta on kasvanut ja laajentunut myös muualle perinteisestä puolustusvoimien asiakkaista. Nyt tarvitaan yhä räätälöidympiä ratkaisuja, joiden kustannustehokkaan kehittämisen allianssin yhteistyö mahdollistaa. [CBNR Finland 2006]

F-Secure Oyj

F-Securen kotisivulla kerrotaan, että yrityksen toiminta-ajatuksena on suojata kuluttajia ja yrityksiä tietokoneviruksia, muita Internetin uhkia sekä mobiiliviruksia vastaan. Yrityksen tavoitteena on olla markkinoiden luotettavin tietoturvayhtiö, joka takaa nopean

vastineen uhkiin. F-Securen ratkaisut sisältävät virustentorjuntatuotteita, tunkeutumisen eston sisältäviä palomuurituotteita sekä roskapostinestoon ja vakoiluohjelmien poistoon tarkoitettuja työkaluja. Työasemille, palvelimille ja verkkoratkaisuille suunnatut sovellukset sopivat saumattomasti yhteen ja ovat keskitetysti hallittavissa. Kumppaniensa kautta yritys tarjoaa tietoturvaa myös palveluna. [http://www.f-secure.fi/]

G4S Security Services Oy

G4S Security Services Oy on entinen Falck Security Oy, joka vaihtoi nimensä vuoden 2007 alusta. G4S tarjoaa muun muassa hälytyskeskuspalveluja, lukitustuotteita ja -palveluja, turvallisuusjärjestelmiä, vartiointi- ja paloturvallisuuspalveluja sekä riskienhallintakonsultointia. Kotisivullaan yritys kertoo tarjoavansa asiakkailleen turvallisuusratkaisuja ja palvelukokonaisuuksia. Tytäryhtiö G4S Cash Services (Finland) Oy tuottaa arvokuljetus- ja rahankäsittelypalveluja. [http://www.g4s.com/fin/fi/]

Hedengren Security

Hedengren Security on oleellinen osa vuonna 1918 perustettua Hedengren-konsernia, jonka turvaliiketoimintoihin sisältyy Hedengren Securityn lisäksi Oy Neptosec Ab ja Oy Neptolux Ab. Yritys toimittaa turvallisuusjärjestelmien kokonaisratkaisuja yhteistyökumppaniensa kanssa valtionhallintoon, kaupan alalle, pankeille, teollisuuteen, puolustusvoimille ja myös yksityissektorille. Hedengren Securityn järjestelmätoimitukset kattavat yksittäiset laiteratkaisut ja useimpien turvallisuusjärjestelmien integroidut kokonaisuudet kameravalvonta-, murtohälytys-, kulunvalvonta-, henkilöturva-, viestintä-, palo- ja turvavalojärjestelmissä. Asiakaskohtaiset toteutukset pohjautuvat Hedengren Securityn oman tuotekehityksen suunnittelemiin keskuksiin ja hallintaohjelmiin sekä tunnettujen päämiesten ilmaisimiin, kameroihin ja tallentimiin.
[http://www.hedpro.fi/etusivu_security]

Hytest

Raunion [2006] mukaan Hytest on Suomen pitkäikäisimpiä ja kannattavimpia biotekniikkayhtiöitä, jonka liikevaihto kasvaa 10–20 %:n vuosivauhdilla. Myynnistä 98 % viedään rajojen ulkopuolelle. Yhtiö valmistaa monoklonaalisia vasta-aineita sekä antigeenejä diagnostiikkateollisuuden raaka-aineiksi, pääasiassa erilaisten laboratoriotestien avainkomponenteiksi. Diagnostiikkamarkkinat kasvavat tasaisesti ja globaalisti. Kehittyvissä maissa kasvu on nopeampaa, mutta läntisissäkin maissa tarvitaan koko ajan uusia ja entistä parempia testejä. Bioterrorismin uhka on saanut etenkin eri maiden puolustusvoimat liikkeelle, ja yritys on myynyt viime vuosina monille puolustusvoimille vasta-aineita testeihin, jotka liittyvät kansallisiin uhkiin. Yrityksen asiakkaita ovat myös kansainväliset diagnostiikka-alan yritykset ja tutkimusryhmät. Samantyyppisellä diagnostiikka-alueella toimii myös suomalainen Medix, joka valmistaa vasta-aineiden lisäksi myös varsinaisia testejä. [Raunio 2006]

Insta DefSec Oy

Insta DefSec kuuluu Insta Group Oy -konserniin (ent. Instrumentointi Oy). Kotisivullaan Insta DefSec kertoo tarjoavansa kotimaisille ja kansainvälisille asiakkailleen ratkaisuja ja palveluja verkkokeskeisiin johtamis-, tietoliikenne- ja koulutusjärjestelmiin sekä sähköisen liiketoiminnan verkottumiseen ja vahvaan tietoturvaan. Lisäksi yritys tuottaa puolustusjärjestelmien integrointi- ja ylläpitopalveluja. Yhtiön mukaan teknologiaratkaisut mahdollistavat uudenlaisten toimintamallien hyödyntämisen, viranomaisyhteistyön, kansainvälisen yhteensopivuuden, paremman tilannetietoisuuden ja suorituskyvyn sekä erittäin korkean tietoturvallisuuden. Asiakkaita ovat puolustusvoimat, valtionhallinto, julkishallinto, korkeaa turvallisuustasoa vaativat yritykset, kriisinhallintaorganisaatiot sekä kansainväliset järjestelmätoimittajat. [http://www.insta.fi/insta_defsec/]

ISS Security

ISS Turvapalvelut eli ISS Security kuuluu osana ISS Palveluihin, joka on Suomen johtava kiinteistö- ja toimitilapalveluyritys. ISS Palvelut puolestaan kuuluu kansainväliseen ISS-konserniin. ISS Securityn kotisivuilla yrityksen kerrotaan toteuttavan asiakkailleen turvallisuusratkaisuja, jotka perustuvat tietotekniikkaan, turvateknologiaan ja henkilökohtaiseen läsnäoloon. Tuotteita ja palveluja ovat tietoliikenneratkaisut, turvajärjestelmät (mm. kulunvalvonta, videovalvonta, rikosilmoitus- ja kiinteistöhälytys, paloilmoitin- sekä henkilöturvajärjestelmät), paikallisvartiointi, piirivartiointi, aula- ja vastaanottopalvelut, hälytys- ja palvelukeskustoiminnot, myymäläturvallisuuspalvelut sekä turvallisuustarkastukset. Uutena palveluna on lanseerattu ISS Virtuaalivartija, joka tarjoaa turvallisuutta erikokoisiin asiakaspalvelupisteisiin. [http://www.fi.issworld.com]

Patria Systems

Patria on kansainvälisesti toimiva puolustusväline- ja ilmailuteollisuuskonserni. Päätuotealueet ovat panssaroidut pyöräajoneuvot, kranaatinheitinjärjestelmät, helikopterit ja lentokoneet sekä näiden elinkaaren tukipalvelut ja puolustuselektroniikkajärjestelmät. Patrian kotisivuilla kerrotaan, että yritys toimittaa omaan erityisosaamiseensa ja kumppanuuksiin perustuvia, kansainvälisesti kilpailukykyisiä ratkaisuja maailmanlaajuisille markkinoille. [http://www.patria.fi/]

Rapiscan Systems Oy

OSI-Systemsin omistama Rapiscan Systems on yhtiön kotisivujen mukaan maailman johtava metallinilmaisimien ja läpivalaisujärjestelmien valmistaja. Yrityksen tuotteet soveltuvat matkatavaroiden ja pakettien tarkastukseen, rahtitavaran ja ajoneuvojen tarkastukseen sekä käsimatkatavaroiden ja ihmisten läpivalaisuun.
[http://www.rapiscansystems.com/]

Temet Oy

Temet Oy kuuluu suomalaiseen Finntemet Oy -konserniin. Temetin kotisivulla yrityksen kerrotaan olevan kansainvälisesti arvostettu väestönsuoja- ja linnoiteratkaisujen tuottaja ja toimittaja. Yhteistoiminta sekä kotimaisten että ulkomaisten siviili- ja sotilasviranomaisten kanssa kuuluu olennaisena osana tuotekehitysohjelmaan. Temetin tuotteisiin kuuluvat muun muassa paineelta suojaavat, kaasulta tiivistävät, ilmaa suodattavat, tärähdykseltä vaimentavat sekä muut väestönsuojalaitteet ja -varusteet.
[http://www.temet.fi/]

Turvatiimi Oyj

Turvatiimin kotisivulla yrityksen kerrotaan tarjoavan monipuolisesti erilaisia turvapalveluja ja tekniikoita. Palveluihin kuuluvat muun muassa tekninen valvonta, videovalvonta, eurowatch, hätäpuhelinpäivystys, päivystyspalvelu, avainpalvelu, kulunvalvonnan pääkäyttö, porttipalvelu, tietoverkkovalvonta, muut turva- ja asiantuntijapalvelut sekä turvatekniikkasuunnittelu ja -järjestelmät. [http://www.turvatiimi.fi/]

Turvaykköset Oy

Turvaykköset Oy on kotimainen valtakunnallinen turva-alan ketju, johon kuuluu 16 osakasliikettä. Yrityksen tuotteet liittyvät kulunvalvontaan, lukitukseen, oviautomatiikkaan, videovalvontaan, avainhallintaan sekä rikosilmoitinlaitteisiin. Turvaykkösten toimintamalliin kuuluu tarjota asiakkaalle tarpeen mukaisia ratkaisuja. Turvaykköset osakasliikkeineen on kehittänyt konseptin, jossa on kuusi vaihetta 1) kohteessa tapahtuva auditointi, 2) asianmukaiset turvallisuusratkaisujen määrittelyt, 3) hankkeen kustannusarvio, 4) kerroksittaisen turvaratkaisun suunnittelu, 5) asentaminen, koulutus ja takuu sekä 6) jatkuva ylläpito ja tuki. [http://www.turvaykkoset.fi/]

Edellä lyhyesti esiteltyjen yritysten lisäksi markkinoilla toimii myös useita muita asiakkailleen turvallisuuteen liittyviä tuotteita ja palveluja tarjoavia yrityksiä. Turvallisuutta voidaan myydä myös muiden tuotteiden ja palveluiden ”oheistuotteena” tuottamassa lisäarvoa varsinaiselle päätuotteelle tai -palvelulle.

5. Security-alan markkinoita säätelevät tekijät

Tässä luvussa pohditaan *security*-alan markkinoita sääteleviä tekijöitä markkinaselvitysten sekä yrityshaastattelujen esiin nostamien teemojen kautta.

Erilaiset uhat luovat turvallisuusalan markkinat. Turvallisuus on korkealla ihmisen perustarpeiden hierarkiassa. Maslowin tarvehierarkian mukaan ihmisen tarpeet ovat muodostuneet hierarkkisesti siten, että ensin pyritään tyydyttämään perustavanlaatuiset fysiologiset tarpeet ja vasta tämän jälkeen sosiaaliset ja henkiset tarpeet. Maslowin mukaan ihmisen tarpeiden hierarkkinen järjestys on:

1. Fysiologiset tarpeet
2. Turvallisuuden tarpeet
3. Yhteenkuuluvuuden ja rakkauden tarpeet
4. Arvonannon tarpeet
5. Itsensä toteuttamisen tarpeet.

Toisaalta edellä kuvatun tarvehierarkian soveltuvuus nykypäivän ihmisiin ei ole aivan yksiselitteistä, koska esimerkiksi itsensä toteuttamisen tarpeet voivat toisinaan ylittää alemman hierarkiatason tarpeita.

Yrityshaastattelut tukevat käsitystä siitä, että *security*-markkinoiden syntymisessä keskeisintä on olemassa oleva uhka, johon lähdetään varautumaan erilaisin ratkaisuin. Uhkan syntyketjusta pyritään löytämään sellainen vaihe, jossa uhka voidaan estää esimerkiksi jonkin teknologisen ratkaisun avulla. Jos asiakas etsii estämis- tai suojautumiskeinoa juuri tähän uhkaan, ovat markkinat valmiina.

Uhat ovat erilaisia eri kulttuureissa ja tilanteissa, joten myös markkinat ovat erilaisia eri puolilla maailmaa ja eri olosuhteissa. Koska uhat muuttuvat, myös markkinat ovat muutoksessa. Uhat voivat muuttua esimerkiksi ympäristöolosuhteiden muuttuessa, toiminnan globalisoituessa, sotien ja kriisitilanteiden myötä sekä poliittisen päätöksenteon myötä. Uhkien torjuntakeinojen kehittyminen voi siirtää ja muokata uhkia sekä varautumisen tarvetta. Uhka ei kuitenkaan muodostu ainoastaan absoluuttisesta vaaratekijästä vaan myös tilanteen kokemisesta. Turvallisuuden tunteeseen vaikuttavat tekijät säätelevät markkinoita varsin voimakkaasti. Uhkien kokeminen ja hyväksyminen vaikuttavat asiakkaiden tarpeisiin ja vaatimuksiin. Tunne voi muuttua varsinaista uhkaa nopeammin ja säädellä näin markkinoita. Uhkien kokemiseen liittyvät muutokset näkyivät jollain tapaa jokaisen haastatellun yrityksen kehityksessä.

Security-alan liiketoimintaa on välillä kritisoitu siitä, että osa markkinoille pyrkivistä yrityksistä luo asiakkaalle voimakkaan huolen omasta turvallisuudestaan. Korostamalla uhkien seurauksien vakavuutta voidaan luoda pelkoja, joihin sitten myydään lievitystä

erilaisten ratkaisujen avulla. Tavallisen ihmisen tai yrityksen voi olla vaikeaa arvioida eri uhkien merkityksiä ja ratkaisun tarvetta. Toisaalta erilaisten uhkien realisoituminen tai välttäminen osoittaa asiakkaalle ratkaisun toimivuuden ja merkityksen. Todelliset, pelottavatkin, esimerkit kertovat uhista ja nostavat varautumisesta tehtävän päätöksen asiakkaan tietoisuuteen. Osa haastatelluista yrityksistä korosti erityisesti alalla toimimisen liittyviä eettisiä velvoitteita.

Haastatellut yritykset pyrkivät löytämään ratkaisuja pääasiassa seuraaviin uhkatyyppeihin:

- omaisuuden anastaminen (ihmisiä vahingoittaen / vahingoittamatta)
- omaisuuden tuhoaminen (eri mittakaavat)
- ympäristön tuhoaminen (eri mittakaavat)
- ihmisten tuhoaminen (eri mittakaavat)
- toiminnan häirintä (eri mittakaavat)
- salakuljetus.

Toiminnan mittakaava voitiin jaotella esimerkiksi rikolliseen toimintaan, järjestäytyneeseen rikollisuuteen, terrorismiin ja sotatilaan. Mittakaavat voitiin ymmärtää myös seurausten laajuuden kautta. Uhkien kohteet voitiin puolestaan ryhmitellä esimerkiksi seuraavalla tavalla:

- rakennukset
- kuljetukset (maa, vesi, ilma)
- teollisuuslaitokset
- sotilaskohteet
- kriittinen infrastruktuuri (liikenteen solmukohdat, energiaverkot, tietoverkot, vesihuolto)
- massatapahtumat ja kohteet, joissa joukkotuhon mahdollisuus
- instituutiot ja järjestelmät
- yhteiskunta
- alue, maa, valtio
- etninen ryhmä
- ihmiset (siviilit, sotilaat, pelastusviranomaiset, kriittiset avainhenkilöt)
- ympäristö (luonnon ympäristö, rakennettu ympäristö)
- organisaatiot ja yhteisöt (julkiset organisaatiot, yritykset, yhteisöt)
- irtain omaisuus
- merkityksellinen tieto
- maine (yksilö, organisaatio, yhteisö, alue, maa, valtio).

Vaikka uhan olemassa olo ja kokeminen synnyttävät *security*-alan markkinat, myös monet muut tekijät vaikuttavat markkinoihin joko vahvistavasti tai heikentävästi. Esimerkiksi poliittiset päätökset erilaisten järjestelmien käyttöönotosta koko maassa tai jopa EU:n alueella luovat juuri kyseiselle järjestelmälle laajat markkinat. Yrityshaastattelujen mukaan myös järjestelmän toimittajan valinta voi olla poliittinen päätös, joka perustuu maiden tai organisaatioiden vakiintuneeseen tai erilaisista tarpeista syntyvään yhteistyöhön. Myös lainsäädännöllä voidaan ohjata markkinoita. Jos lainsäädäntö edellyttää tietyn palvelun tai järjestelmän hankkimista, ovat markkinat olemassa. Tästä esimerkkinä ovat väestönsuojavaatimukset. Toisaalta lainsäädäntö, viranomaismääräykset, standardit ja vakuutusyhtiöiden suojeluohjeet vaikuttavat asiakkaiden ostopäätökseen, kun arvioidaan, täyttääkö tuote tai palvelu kyseiset vaatimukset. Lainsäädäntö voi myös rajoittaa tiettyjen ratkaisujen markkinoita. Tästä selkeä esimerkki on yksilön suojaan liittyvä lainsäädäntö, joka rajoittaa erilaisten tunnistusteknologioiden markkinoita.

Myös tuotteen standardinmukaisuus vaikuttaa ostopäätökseen vahvistamalla ratkaisun luotettavuutta ja helpottamalla asiakkaan tekemää arviointia tuotteista. Jos tietyllä, tyypillisesti uutta ja kehittyvää teknologiaa hyödyntävällä alalla ei käytetä lainkaan standardeja, ei asiakas välttämättä uskalla hankkia tuotteita vaan odottaa standardoinnin kehittymistä alalle. Esimerkiksi lentokentillä hankintoja vaikeuttaa turvateknologian standardoinnin kehittymättömyys: uusia investointeja ei uskalleta tehdä, koska hyötyä on vaikea arvioida ja vaatimukset voivat muuttua. Myös CBRNE-detektorien kohdalla standardointi vaikeuttaa asiakkaiden ostopäätöstä, koska laitteiden ominaisuuksia on vaikea vertailla ilman yleistä tasovaatimusta. Toisaalta esiin tuli myös huoli siitä, että EU:n hitaan turvallisuusteknologiaan liittyvän standardointikehityksen seurauksena USA ehtii luoda standardivaatimukset esimerkiksi satamiin ja lentokentille. Tällöin EU:ssa joudutaan kulkemaan USA:n vaatimusten perässä ja oma teknologiankehitys saattaa kärsiä. Tällöin eurooppalaiset teknologiatoimittajat saattavat jäädä markkinoilla altavastaajan rooliin.

Myös kansalaisten yleinen hyväksyntä turvallisuusteknologian käyttämisessä vaikuttaa markkinoihin. Kuten jo aikaisemmin todettiin, uhat ja turvallisuuden tunne voivat muuttua. Teknologian kehittyessä myös yleinen käsitys siitä, mitä ihmisten turvaamiseksi voidaan tehdä, muuttuu koko ajan. Teknologian tuomat uudet mahdollisuudet muuttavat esimerkiksi käsitystä siitä, mikä on riittävä suojautumiskeino. Muutoksen myötä myös yksityisyyden suojan rajat voivat muuttua. Tästä on esimerkkinä valvontakameroihin suhtautumisessa tapahtunut muutos. Aiemmin ihmisiä huolestutti valvontakameroiden lisääminen, mutta nyt kameroihin on totuttu. Tällainen suhtautumisen muutos on otettava huomioon myös markkinoilla.

Jotta uutta tuotetta osataan markkinoida oikeaan aikaan, edellytetään markkinoilla toimivilta yrityksiltä jatkuvaa trendien seuraamista. Toisaalta on otettava huomioon, että

hankittuaan järjestelmän tai tuotteen asiakas todennäköisesti pitää sitä tietyn aikaa eikä heti osta uusinta teknologiaa. *Security*-tuotteita, -ratkaisuja ja -palveluja tuottavien yritysten on siis seurattava, mikä kehitysaalto on meneillään ja osattava markkinoida sillä hetkellä aallon harjalla olevaa tuotetta kehittäen samalla jo seuraavaa sukupolvea. Tämä näkyi etenkin CBRN-detektorien markkinoilla, jossa teknologinen kehitys etenkin USA:n tutkimusrahan tuloksena on varsin nopeaa.

Turvateknologian ja kiinteistöturvajärjestelmien kehitysvauhdin kasvaessa kiinteistöturvallisuusalan yritykset ovat siirtyneet tuottamaan järjestelmiä osana kokonaispalvelua. Palvelujen tarjoaminen on sinänsä alalle tyypillistä, sillä esimerkiksi vartiointipalvelua on tarjottu pitkään. Nyt asiakas voi ostaa kiinteistö- ja turvajärjestelmiä palveluna, jolloin vältytään erilliseltä järjestelmäinvestoinnilta. Näin saadaan käyttöön myös uusinta teknologiaa. Tällainen malli auttaa teknologian kehittymisessä, sillä asiakkaan kynnys ostaa uutta vähenee. Kokonaisvaltaisten palvelua ja järjestelmiä sisältävien ratkaisujen markkinoiminen onkin tällä hetkellä yleisempi trendi kuin yksittäisten järjestelmien tai tuotteiden myynti. Kokonaisratkaisut helpottavat asiakkaan ostotilannetta, koska koko ongelmaan tai tarpeeseen saadaan ratkaisu asioimalla vain yhden toimittajan kanssa. Toisaalta asiakasyritysten hankinnat saattavat olla hajautettuna eri henkilöille niin, että kokonaispalvelun ostamisen sijaan kukin hankkija hankkii ratkaisua vain oman ”toimialueensa” tarpeeseen. Kokonaisratkaisujen tarjonnan yleistyminen saattaa muuttaa myös asiakasorganisaation hankintatoimen rakennetta.

Myös yksittäisen *security*-alalla toimivan yrityksen valinnat vaikuttavat markkinoilla selviytymiseen. Esimerkiksi yrityksen innovaatiotoiminnan kehittyneisyys vaikuttaa siihen, miten yritys voi tuoda ja luoda markkinoille uusia vaatimuksia. Myös yrityksen kyky reagoida markkinoilla tapahtuviin muutoksiin vaikuttaa selviytymiseen. Joillekin yrityksille ratkaisujen räätälöinti on avain markkinoille. Erityisesti turvallisuusalalla ratkaisuja joudutaan räätälöimään asiakasorganisaatioiden tarpeisiin kohteen ominaispiirteet huomioon ottaen. Tällöin ratkaisevana tekijänä on se, millaisia valmiita moduuleja on voitu kehittää ja kuinka hyvin näistä moduuleista voidaan nopeasti ja tehokkaasti saada asiakkaan omat tarpeet täyttävä ratkaisu. Tällöin tärkeään asemaan nousee asiakkaan kuuntelu, hyvien perusmoduulien kehittäminen sekä moduulien yhdistämiskyky. Tietyn asiakassegmentin hyvä hallinta voi antaa yritykselle lähes yksinoikeudet tämän asiakassegmentin markkinoihin.

Turvatuotteissa yksi keskeinen ominaisuus on niiden ennaltaehkäisevyys. Näkyvä ja/tai hienoon teknologiaan perustuva tuote, ratkaisu tai palvelu voi näkyvyydellään estää rikollisen toiminnan kohteessa. Hyviä esimerkkejä kohteen houkuttelevuuden pienentämisestä torjuntatoimen näkyväksi tekemisellä ovat näkyvä vartiointi, kamerat ja lukitukset. Myös puolustusvälineiden korkea teknologia luo kuvan haasteellisesta vastuksesta. Hyvää ja näkyvää teknologiaa voidaan hankkia myös asiakasorganisaation tai

alueen maineen parantamiseksi. Sekä hienon teknologian että näkyvyyden kääntöpuolena ovat esimerkiksi hyökkäykset korkean tietoturvatason kohteisiin pelkästään haastavuuden takia.

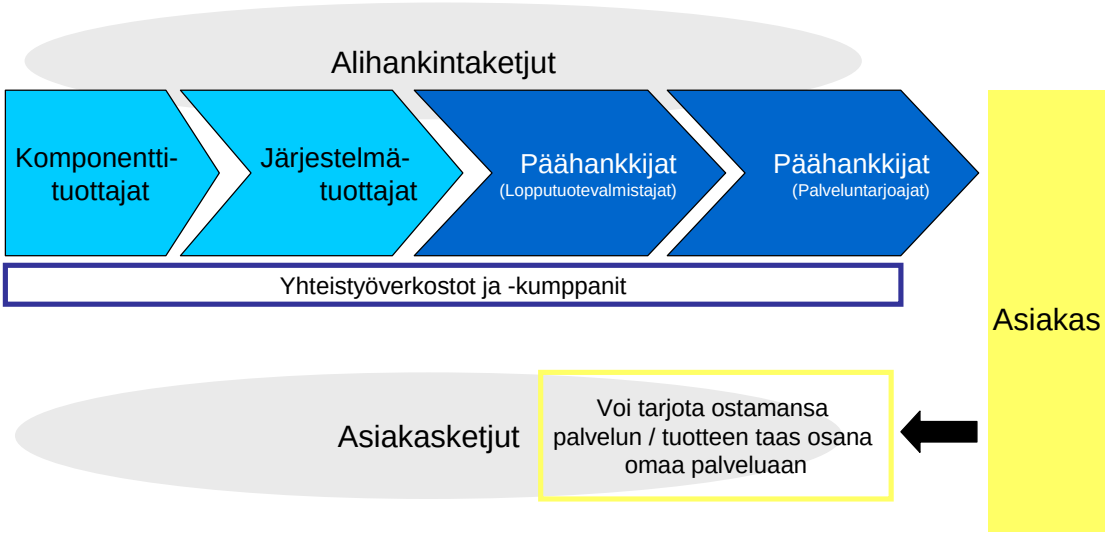
Myös tuotteen, ratkaisun ja/tai palvelun laatu on tärkeää turvallisuusalalla. Joissain tapauksissa asiakas haluaa vain minimivaatimukset täyttävän ratkaisun. Näin on usein esimerkiksi lainsäädännön edellyttämien tuotteiden kohdalla (muun muassa väestönsuojat ja palovaroitin). Kriittisissä kohteissa laadun merkitys kuitenkin korostuu. Joskus asiakkaan on vaikea ymmärtää laadun merkitystä. Esimerkiksi väestönsuojien kohdalla on taustalla oletus, ettei suojaa koskaan tarvita, mikä voi vaikuttaa laatuvaatimuksiin. Laadun merkitystä voidaan kuitenkin pyrkiä osoittamaan testituloksien avulla. Joissain tapauksissa laadun kriteerit ovat määritettävissä standardoinnilla. *Securityyn* liittyviä tuotteiden toimittajia ja palveluntarjoajia voidaan myös laittaa paremmuusjärjestykseen yleisten arviointikriteerien mukaan. Esimerkiksi lentokenttiä, satamia ja kuljetusyrityksiä listataan ja pisteytetään myös toiminnan turvallisuuden perusteella. Parhaiksi valitut saavat luonnollisesti etua markkinoilla. Näin esimerkiksi yleinen liiketoiminta-alueen tuotteiden ja palvelujen laatu vaikuttaa kaikkiin alueella toimiviin yrityksiin. Myös muut toimittajan maineeseen liittyvät tekijät, kuten patenttien omistaminen, työntekijöiden ammattitaidon osoittaminen (esim. tutkinnot) ja maahan liitettävät mielikuvat, voivat vaikuttaa siihen, keneltä asiakas tuotteen tai palvelun hankkii. Työntekijöiden luotettavuus on erittäin kriittinen tekijä turva-alalla toimivissa yrityksissä, joissa työntekijällä on pääsy asiakasyrityksen alueelle ja tietoihin.

Ostopäätökseen vaikuttavia tekijöitä ovat myös tuotteen, ratkaisun ja/tai palvelun yhteentoimivuus, yhteensopivuus ja integroitavuus. Jos tuote tai järjestelmä saadaan helposti yhdistettyä muihin tuotteisiin ja järjestelmiin, vaatii käyttöönotto vähemmän muutoksia. Myös lisäominaisuuksien lisäämismahdollisuus myöhemmin on tärkeää. Erilaiset tuotteen, ratkaisun ja/tai palvelun toimittajien verkostot voivat auttaa synergian tuomisessa palveluihin tai tuotteisiin. Etenkin tietoturva-alalla tällaisia verkostoja ja sopimuksia on muodostettu. Myös kiinteistöturvallisuuteen liittyviin valvonta- ja hälytysjärjestelmiin tällaista synergiaa on kehittynyt ja kehittymässä.

6. Arvoketjut

Tämän hankkeen puitteissa arvoketjun nähtiin muodostuvan komponenttien tuottajista, järjestelmien tuottajista, lopputuotteen ja/tai palvelun tuottajista, ostajista sekä käyttäjistä (Kuva 9). Suuri osa haastatelluista yrityksistä edusti lopputuotevalmistajia ja palvelun tarjoajia. Erilaisilla teknologiantoimittajilla nähtiin merkittävä rooli *security*-alan yritysten alihankintaketjussa. *Securityyn* liittyvissä tuotteissa ja palveluissa voidaan hyödyntää hyvin paljon erilaisia teknologioita, ja siksi monet eri komponenttiyritykset voivat liittyä arvoketjuun.

Tuotekehitysvaiheessa osa yrityksistä teki tai oli tehnyt yhteistyötä tutkimuslaitosten kanssa. Yhteistyökumppaneiden, kuten VTT:n, avulla arvoketjun eri toimijoita voidaan koota yhteisiin turvallisuusteknologiaa ja alan liiketoimintaa kehittäviin hankkeisiin. Koska osa yrityksistä kuului suuriin kansainvälisiin konserneihin, tehtiin yhteistyötä myös konsernien sisällä. Yhteensopivuuden varmistamiseksi jotkut yritykset toimivat erilaisissa verkostoissa. Etenkin tietoturvayritykset toivat esiin yhteensopivuuteen liittyviä kumppaniverkostoja. Myös kiinteistöturvapuolen palveluntarjoajien ja järjestelmäntoimittajien sivustoilla kerrottiin yhteistyökumppaneiden nimiä. Kokonaispalveluna myytävissä ratkaisuissa usein jokin osa palvelusta tai osa tuotteista tuli muilta yrityksiltä. CBRN-alan suomalaisilla yrityksillä oli myös yhteinen verkosto erityisesti kansainvälisessä myynti ja markkinointitarkoituksissa.



Kuva 9. Arvoketjun perusrakenne.

Yrityksen asema arvoketjussa voi myös siirtyä. Kun yksittäisen komponentin tai järjestelmän tuottajalle tulee paine tuottaa kokonaisratkaisuja, siirtyy yritys arvoketjussa eteenpäin. Joskus paine siirtymään voi olla suuri: jos ei toimita kokonaisratkaisua, ei ole enää edes komponenttimarkkinoita. Arvoketjussa siirtymisen päätös voi olla yrityksen

oma tietoinen valinta muokata markkinoita tai tilanteeseen voi joutua ”pakon” edessä muiden toimijoiden muuttaessa toimintaansa.

Kysymys *securityyn* liittyvän tuotteen, ratkaisun tai palvelun ostajasta ja käyttäjästä ei ole aivan yksiselitteinen. Ensinnäkin turvallisuusominaisuus voi tulla mukana ostetussa tuotteessa tai palvelussa, jolloin ostopäätös ei suoranaisesti tai yksinomaan perustu tuotteen turvallisuuteen. Esimerkiksi ostettaessa kuljetuspalvelua oletetaan palveluun sisältyvän turvallisuus eli edellytetään, ettei kuljetettavaa tuotetta varasteta tai vahingoiteta kuljetuksen aikana. Asiakas ei kuitenkaan tällöin varsinaisesti osta turvallisuuspalvelua, vaan turvallisuus on lisäarvo muuhun palveluun. Myös turvallisuuden loppukäyttäjän arviointi on joissain tapauksissa vaikeaa. Ostaako ja käyttääkö esimerkiksi viranomainen, ilmailulaitos, lentoyhtiö vai lentomatkustaja viime kädessä lentoon liittyvän turvallisuuden. Turvallisuus voi myös kuulua palveluun niin vahvasti, ettei loppukäyttäjä voi sitä poistaa edes niin halutessaan. Toisaalta loppukäyttäjä on otettava huomioon tuotteen tai palvelun suunnittelussa, vaikkei hän varsinaisesti osta turvallisuutta. Käyttäjien kokemus palautuu tuotteen tai palvelun ostajalle ja vaikuttaa näin seuraavaan ostopäätökseen.

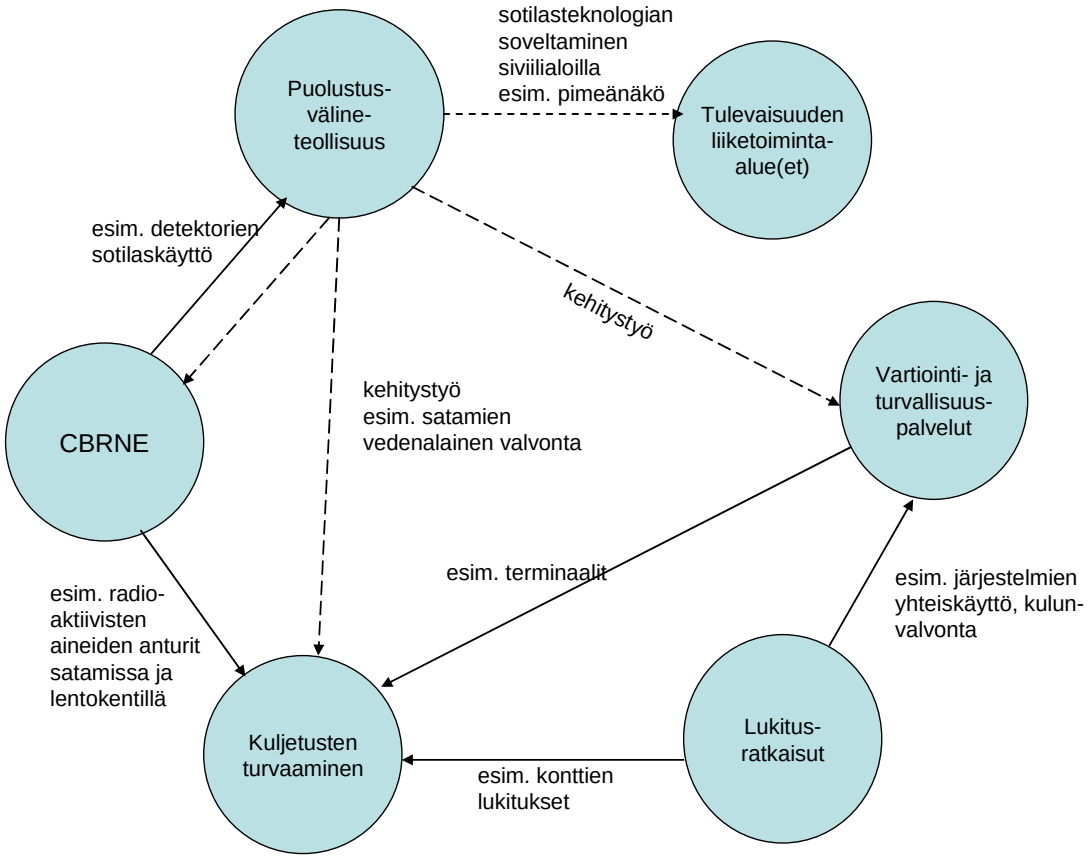
Haastatelluissa yrityksissä tyypillisiä asiakkaita olivat muun muassa

- valtionhallinto
- viranomaiset (tulli, rajavalvontalaitokset, ilmailuviranomaiset, pelastusviranomaiset, eri valtioiden puolustusvoimat ja puolustusministeriöt)
- kriisienhallintaorganisaatiot
- ilmailulaitokset (→ lentoyhtiöt → matkustajat) ja satamalaitokset (→ operaattorit → kuljetusyritykset → kuljetettavan tavaran omistajat)
- terminaali-, jakelu- ja logistiikkakeskusoperaattorit
- teollisuuslaitokset
- korkeaa turvallisuustasoa vaativat yritykset ja organisaatiot (mm. hotellit ja sairaalat)
- kiinteistöyhtiöt
- rakennusyhtiöt
- tavalliset yritykset
- yksityiset ihmiset.

7. Hahmotus klusterista ja kilpailukykymallista

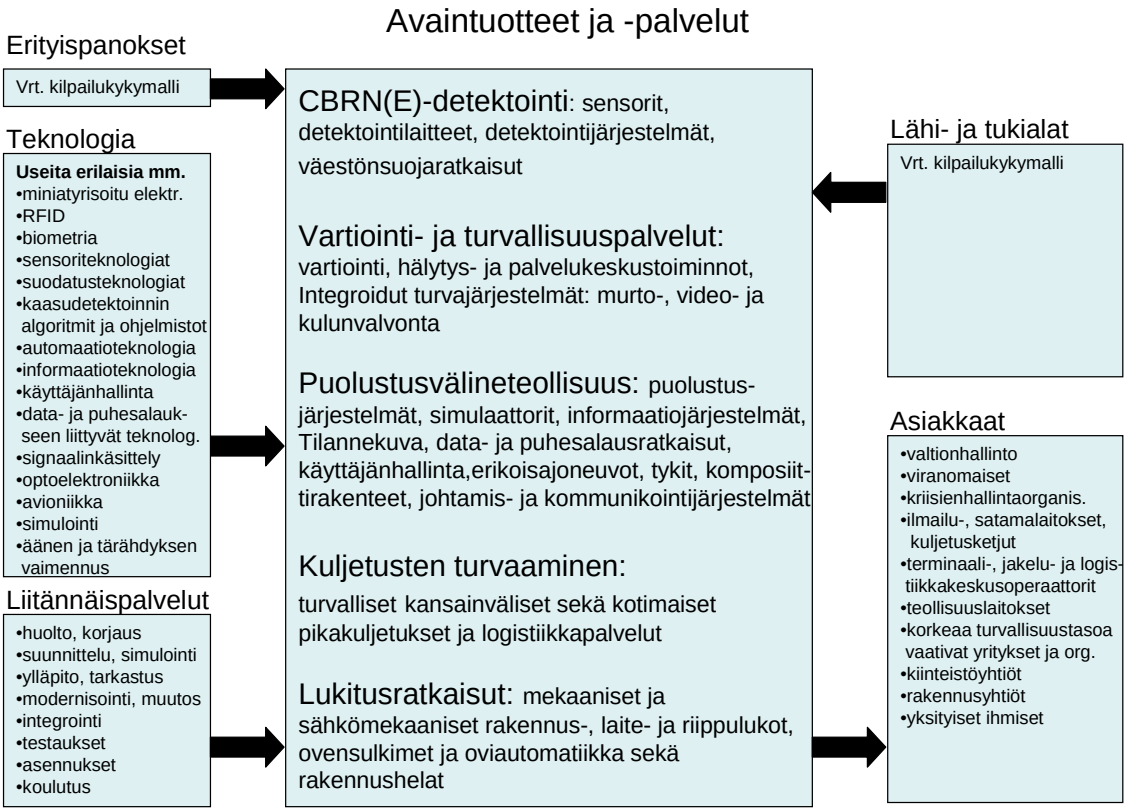
Securityyn liittyvää toimialaa tai klusteria on hyvin vaikea määrittää, sillä yritykset toimivat eri toimialoilla. Myös eritasoisia markkinat synnyttäviä uhkia ja kohteita on hyvin erilaisia, joten tarpeet ovat hyvin eritasoisia. Klusterin muodostamisen lähtökohtana ovat usein tiettyä avaintuotetta valmistavat yritykset, jotka muodostavat klusterin ytimen. [Viitanen et al. 2003] Tärkeä on käsitys siitä, mitkä tuotteet markkinoilla yhdessä muodostavat liiketoiminta-alueita. Vaihtoehtoinen tapa on tarkastella, mitkä toimialat yhdessä muodostavat liiketoiminta-alueita. [Virtanen & Hernesniemi 2005]

Hankkeessa haastatellut yritykset jakautuivat melko selkeästi tuotteidensa ja toimialansa perusteella seuraaviin erillisiin liiketoiminta-alueisiin: CBRN(E)-detektointi, vartiointi- ja turvallisuuspalvelut, puolustusvälineteollisuus, kuljetusten turvaaminen sekä lukitusratkaisut. Nämä kaikki liiketoiminta-alueet liittyivät jollain tapaa *securityyn*, mutta yhtä yhteistä klusterina toimivaa liiketoiminta-aluetta ei voitu tunnistaa. Klusterihan tarkoittaa yhtä eri tuotteista tai toimialoista muodostuvaa liiketoiminta-aluetta. Kunkin tunnistetun liiketoiminta-alueen sisällä havaittiin arvoketjuja ja aktiivisia verkostoja. Liiketoiminta-alueiden välillä ei kuitenkaan juuri havaittu aktiivisia verkostoja. Hankkeen aikana ei myöskään noussut esiin selkeää yhteistä tarvetta tai toivetta liiketoiminta-alueiden keskinäisille verkostoille. Klusterin määrittelyssä juuri keskinäinen vuorovaikutus ja verkostomainen yhteistoiminta tuottavat klusterin jäsenille selvästi osoitettavissa olevia hyötyjä [Jääskeläinen 2001; Viitanen et al. 2003]. Jonkinlaisia yhteyksiä tai yhteisiä intressialueita liiketoiminta-alueiden väliltä kuitenkin löytyi. Näitä intressien yhteyksiä on esitetty tarkemmin kuvassa 10. Teoreettiset välituoteostojen mahdollisuudet on esitetty kuvassa nuolin. Välituoteosto on tavara, teknologia tai palvelu, jonka liiketoiminta-alue ostaa toiselta ja käyttää panoksena omassa tuotannossa. Esimerkiksi vilkastunut puolustusvälineteollisuuden ratkaisujen siirtäminen myös siviilipuolelle saattaa luoda uusien tuotteiden ja palvelujen myötä myös aivan uusia liiketoiminta-alueita *security*-kentälle.



Kuva 10. Securityyn liittyvien liiketoiminta-alueiden yhteydet.

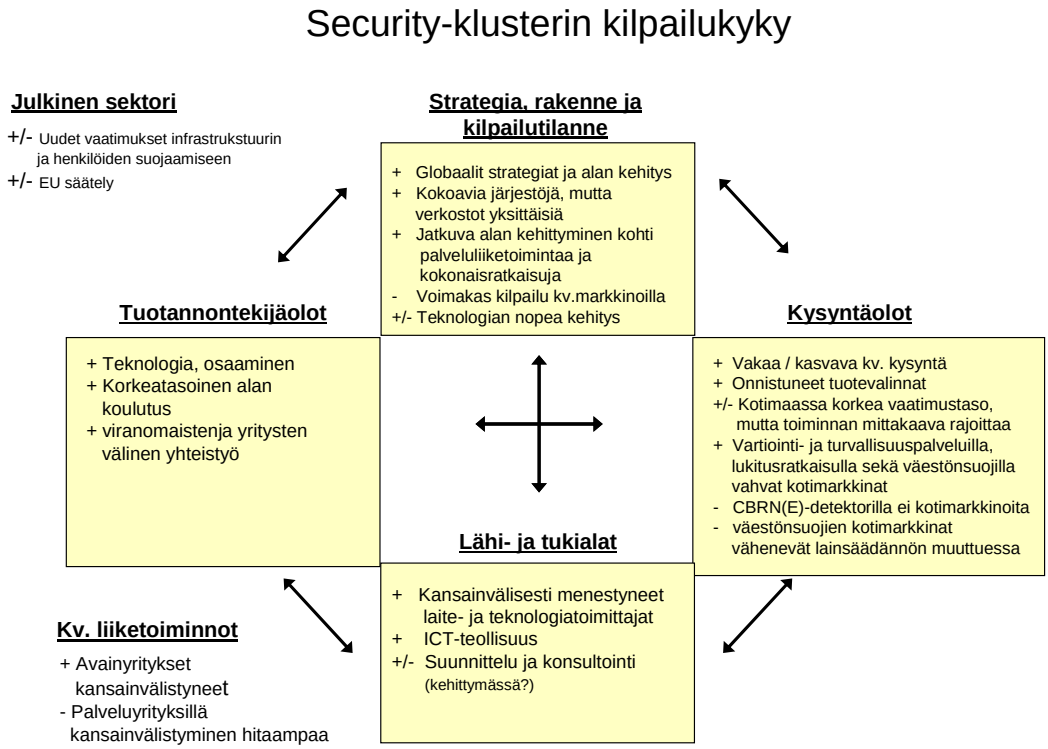
Edellä mainitut liiketoiminta-alueet voisivat muodostaa yhteisen *security*-klusterin, mikäli eri alueiden tuotteet muodostaisivat jonkinlaisen arvonlisäketjun ja toimijoiden välillä olisi aktiivista vuorovaikutusta. Tällä hetkellä arvonlisäketjua eri liiketoiminta-alueiden välisille tuotteille on vaikea nähdä. Toisin sanoen esimerkiksi detektointilaitteet sekä vartiointi- ja turvallisuuspalvelut eivät muodosta mitään jalostusarvon lisäämisen ketjua keskenään. Tällaisen ketjun muodostuminen on kuitenkin tulevaisuudessa mahdollista. Myös jonkinlaisen klusterirakenteen synty *security*-liiketoiminta-alueiden kesken on mahdollinen. Yhteisen klusterikaavion hahmottamiseksi edellä mainittujen liiketoiminta-alueiden avaintuotteet ja -palvelut sekä muut tekijät yhdistettiin kuvaan 11.



Kuva 11. Teoreettinen security-klusteri avaintuotteiden ja palvelujen kautta kuvattuna.

Myös ydinyrityksillä on merkittävä rooli klusterien syntymisessä ja toiminnassa. Tutkimuksessa tunnistettujen liiketoiminta-alueiden sisäisinä ydintoimijoina voidaan pitää niitä yrityksiä, jotka seuraavat tarkasti asiakkaiden tarpeita ja tuottavat ratkaisuja näihin tarpeisiin synnyttäen samalla taakseen alihankintaketjun. Toisaalta ydintoimija voidaan määritellä esimerkiksi seuraavien ominaisuuksien perusteella: vakaa, asiakasrajapinnassa toimiva, innovoiva, verkostoitunut, laadukkaat tuotteet tai palvelut, synnyttää ympärilleen toimintaa ja luo työpaikkoja.

Klustereihin liittyy myös kilpailukyvyn mallintaminen. Kuvaan 12 on hahmoteltu Porterin timanttimallin avulla eri liiketoiminta-alueiden yhteisiä kilpailukykytekijöitä, jotka muodostavat teoreettisen *security*-klusterin kilpailukyvyn. Tässä teoreettisen *security*-klusterin on siis ajateltu muodostuvan edellä mainituista liiketoiminta-alueista. Koska liiketoiminta-alueet eroavat toisistaan, myös eri alueiden kilpailukykytekijöissä on eroja. Tässä kilpailukykymallissa on näin ollen pyritty kuvaamaan lähinnä liiketoiminta-alueille yhteisiä piirteitä, mutta myös joitakin eroja on nostettu esimerkinomaisesti esiin. Kustakin liiketoiminta-alueesta laadittu kilpailukykymalli kertoisi kuitenkin tarkemmin alueen tilanteesta.



Kuva 12. Hahmotus security-klusterin kilpailukyvystä.

Securityyn liittyvien liiketoiminta-alueiden pohdinnassa tulee ottaa huomioon myös yleisten megatrendien vaikutus. Esimerkiksi globalisoituminen, verkottuminen, taloudellinen integraatio, tekninen ja teknologinen kehitys erityisesti tieto- ja kommunikaatiotekniikassa, palveluyhteiskunnan kehitys sekä julkisen sektorin murros ovat huomioon otettavia asioita.

8. Pohdinta ja johtopäätökset

Tässä julkaisussa esitetyt näkökannat perustuvat kirjallisuudesta poimittuihin tietoihin ja näkemyksiin sekä pieneen määrään yrityshaastatteluja. Yrityshaastatteluilla pyrittiin saamaan syvällinen kuva kunkin yrityksen liiketoiminta-alueesta ja toiminnasta. Haastatteluissa saatiin hyvin esiin eri liiketoiminta-alueiden piirteitä ja toimintaa säätteleviä tekijöitä. Verkostoista ja kumppanuussuhteista ei sen sijaan saatu kovin yksityiskohtaista tietoa. Kokonaisuudessaan yrityshaastattelut olivat kuitenkin hyvä keino hankkia alustavaa tietoa varsin hajanaiselta ja tilastoimattomalta *security*-liiketoiminta-alueelta. Markkinatutkimusten avulla yritykset voitiin sijoittaa myös yleisempään viitekehykseen.

Markkinatutkimusten, muun kirjallisuuden sekä yrityshaastattelujen pohjalta muodostettiin käsitys *security*yn liittyvästä toimijakentästä sekä markkinoihin vaikuttavista tekijöistä. Toimijakentän muodostavat turvallisuuteen liittyviä tuotteita ja palveluja tuottavat yritykset, tuotteita ja palveluja ostavat yritykset, eri viranomaistahot, eri järjestöt, tutkimus- ja opetuslaitokset sekä erilaiset yhteistyöfoorumit. Keskeisenä kotimaisena julkisena rahoittajana oli Tekes. Käyttäjänä, asiakkaana, tutkimuskohteena ja vaikutusten kohteena myös yksilöllä ja yhteiskunnalla on rooli toimijakentässä. *Security*-markkinat muodostuvat erilaisten uhkien kautta, mutta niihin vaikuttavat useat eri tekijät, kuten poliittiset päätökset, lainsäädäntö, standardointi, ihmisten yleinen käsitys turvallisuudesta, erilaisten ratkaisujen yleinen hyväksyttävyys ja vaikutukset yksityisyyden suojaan, teknologian kehitys, tuotteiden ja palvelujen kypsyystaso ja laatu sekä ratkaisujen synergia- ja integrointitarpeet. Koska uhat, uhkien kokeminen ja teknologian kehitys ovat jatkuvasti muuttuvia elementtejä, ovat myös *security*-markkinat muuttuvassa tilassa. Muutosta tuo esimerkiksi turvallisuusalan markkinoiden ja ICT-markkinoiden yhdistyminen.

Turvallisuuteen liittyviä tuotteita ja palveluja toimittavat yritykset ovat yhä enemmän siirtyneet toimittamaan asiakkailleen kokonaisratkaisuja yksittäisten järjestelmien sijaan. Tämä on nähtävissä jokaisella hankkeessa tunnistetulla liiketoiminta-alueella. Tällöin erilaisten liitännäispalvelujen merkitys ja kokonaisvaltaisempi lähestymistapa ovat lisääntyneet. Koska yritykset harvoin kykenevät tuottamaan yksin kaikkia toimittamansa kokonaisratkaisun osia, ovat myös erilaiset alihankinta-, arvo- ja asiakasketjut sekä verkostot nostaneet merkitystään. Tällä hetkellä turvallisuuteen liittyvät konsultointipalvelut ovat eräs kehittymispotentiaalia omaava alue. Ratkaisuja toimittavat yritykset voivat integroida ratkaisuun myös konsultointipalvelua. Toisaalta pelkkiä konsultointipalveluja tuottavat yritykset voivat joko verkottua ratkaisuntoimittajien kanssa tai sitten pyrkiä luomaan asiakasyritykseen entistä pidemmän ja kiinteämmän suhteen. Palvelu voi kehittyä myös esimerkiksi siten, että asiakkaille myydään turvallisuuspuolen hankintapalveluja. Tämä tarkoittaa sitä, että hankintapalvelun toimittaja tutkii ja valitsee asiakasyrityksilleen turvallisuutta parantavia teknologioita, tuotteita, palveluja ja ratkaisuja.

Haastatelluista yrityksistä osa toimi voimakkaasti kotimarkkinoilla ja osa lähes ainoastaan kansainvälisillä markkinoilla. Tyypillinen kotimaan toimija on vartiointi- ja turvallisuuspalveluyritys. Tosin tämän alan yrityksistäkin suurimmat toimivat osana kansainvälistä konsernia. Terrorismiuhkiin ratkaisuja tuovat yritykset sen sijaan toimivat lähes kokonaan kansainvälisillä markkinoilla. Näin ollen teoria kilpailukyvyn kehittymisestä vahvojen kotimarkkinoiden kautta ei ole ainakaan kattavasti sovellettavissa *security*-kentälle. Globaaleille *security*-markkinoille voidaan yrityshaastattelujen perusteella päästä joko vahvalla ydinosaamisella jostakin *security*-liiketoiminta-alueesta tai integroimalla *security* oheispalveluksi ja osaksi jotain muuta ydinosaamista. Useiden *securityyn* liittyvien teknologioiden ja tuotteiden kohdalla yleiset EU:n standardointikuviot ovat jäljessä. Tämä koskee etenkin nopeasti kehittyviä teknologioita ja liittyy muun muassa CBRNE-detektointiin ja läpivalaisuun. USA:ssa standardointi on näillä alueilla jo pidemmällä ja vaarana on, että eurooppalaiset yritykset joutuvat nyt toimimaan USA:n ehdoilla. Myös tietyt velvoitteet toiminnasta ja teknologian käytöstä tulevat nyt USA:sta. Esimerkiksi satamia koskeva konttien seulonta (*screening*) on pitkälti USA:n velvoittamaa. Tämä kehitys voi rajoittaa eurooppalaisten yritysten teknologian kehitystyötä, kun vain amerikkalaiset ratkaisut hyväksytään markkinoille.

Työn haasteena oli uuden käsitteen, *security*-klusterin, ymmärtäminen ja hahmottaminen. Klusteri-käsitteestä löytyi runsaasti kirjallisuutta, mutta käsitteen yhdistäminen *security*-liiketoiminnan määrittelemättömään käsitteeseen tuotti vaikeuksia. Kun klusterilla tarkoitetaan yleensä yhtä eri tuotteista tai toimialoista muodostuvaa liiketoiminta-aluetta, tuntui *security* yhtenä liiketoiminta-aluekokonaisuutena aivan liian abstraktilta ja jäsentymättömältä. *Securityyn* liittyvät markkinatutkimukset hajottivat myös käsitteen hyvinkin erilaisiksi teknologioiksi, tuotteiksi ja suojattaviksi kohteiksi. Yrityshaastattelut tukivat käsitystä siitä, että *security*-liiketoiminta-aluetta ei mielletä vakiintuneena kokonaisuutena, vaan *securityyn* liittyy useita eri liiketoiminta-alueita. *Security*-klusteria ei siis ainakaan vielä ole olemassa. Tässä tutkimuksessa päädyttiin lopulta kuvaamaan teoreettista s*ecurity*-klusteria eri liiketoiminta-alueiden yhdistelmänä (CBRNE-detektointi, vartiointi- ja turvallisuuspalvelut, puolustusvälineteollisuus, kuljetusten turvaaminen ja lukitusratkaisut). Teoreettinen klusteri saatiin hahmotettua klusterin ja kilpailukyvyn mallinnuksessa yleisesti käytettyjen kaavioiden avulla. Teoreettista klusteria ei kuitenkaan voi pakottaa toimimaan, vaan klusterin syntyyn on tultava tarve eri liiketoiminta-alueiden sisältä.

Klusterin järjestäytyminen tapahtuu yleensä luonnollisella tavalla ilman vakioitunutta prosessia. Koordinointia kuitenkin tarvitaan useiden erilaisten toimijoiden yhteistyön organisointiin. [Viitanen et al. 2003] Olosuhteita voi luoda julkisin ja yksityisin koulutusjärjestelmien avulla, kannustusohjelmilla, julkisilla ja yksityisillä tutkimusjärjestelmillä sekä infrastruktuuria kehittämällä. Innovaatioympäristöä voidaan tukea kehittämällä teknologiaa ja liiketoimintaosaamista yrityskeskeisinä kehitysprosesseina

sekä kehittämällä yritysverkostoja ja innovaatioympäristöjä [Virtanen & Henrnesniemi 2005]. Suomen *security*-klusterin kehittäminen vaatisi siis otollisten olosuhteiden aikaansaamista klusterikehitykselle. Eräänä mahdollisuutena voidaan tunnistaa Suomen *Sisäisen turvallisuuden ohjelman* sekä Tekesin valmisteleman *Turvallisuusalan teknologiaohjelman* mukanaan tuomat yhteistyöverkostot sekä uudet innovaatiot. Parhaimmillaan ohjelmien tuloksena syntyy uutta *securityyn* liittyvää liiketoimintaa ja vanhat liiketoiminta-alueet jäsentyvät tarkemmin. Myös yksityisen sektorin panos on välttämätön olosuhteiden luonnissa, jotta kilpailuetu aikaansaadaan. Yrityspuolella on oltava vastaanottorakenne julkiselle tuelle.

Security-liiketoimintaa tarkasteltaessa tulee ottaa huomioon myös yhteydet *safetyyn*, ja tietoturvaan. Samat teknologiset ratkaisut voivat hyödyttää koko turvallisuuskenttää ja usein myös vaikutusta on vaikea rajata selkeästi tahalliseen vahingontekoon tai tahattomaan toimintaan liittyväksi. Yhteistyötä tarvitaan siis koko turvallisuuskentällä – ei vain *securityyn* liittyvien toimijoiden kesken.

Lähdeluettelo

Amended proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL concerning the 7th framework programme of the European Community for research, technological development and demonstration activities (2007–2013). 2006. Brussels 28.06.2006. COM(2006) 364final. [viitattu 15.9.2006]
Saatavissa: http://ec.europa.eu/research/future/pdf/com2006_364_final_en.pdf

Arjen Turvaa – Sisäisen turvallisuuden ohjelma. 2004a. Tiivistelmä. Helsinki: Sisäasiainministeriö. 19 s.

Arjen Turvaa – Sisäisen turvallisuuden ohjelma. 2004b. Valtioneuvoston periaatepäätös 23.9.2004. 80 s.

Baldwin, D. A. 1997. The concept of security. Review of International Studies, Vol. 23, s. 5–26.

Buzan, B. 1983. People, states, and fear: the national security problem in international relations. Brighton: Wheatsheaf. 262 s.

CBRN Finland. 2006. [verkkosivusto]. [viitattu 15.9.2006].
Saatavissa: http://www.cbrnfinland.fi/index.php

Country Industry Forecast – European Union. Security Industry. 4624-90. 2004. Frost & Sullivan.

Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi. 2006. Helsinki: Sisäasianministeriö. 37 s. (Sisäasianministeriön julkaisuja 15/2006.)

European Industrial and Commercial Security Products and Systems Markets. 2005. Extended TOC. Frost & Sullivan. [viitattu 23.9.2006].
Saatavissa: https://www.frost.com

European Homeland Security – A Market Opportunity Analysis. 2005. Extended TOC. Frost & Sullivan. [viitattu 23.9.2006]. Saatavissa: https://www.frost.com

Finnsecurity. 2006. Turvallisuusalan yritysten suhdanne- ja toimialaraportti 2006: Selvitys turvallisuusalan yritysten markkinoista, yritysprofiilista, kasvuyrittäjyydestä ja lähiajan suhdanneodotuksista. Tiivistelmä.
Saatavissa: http://www.finnsecurity.fi /www/att.php?id=4

Frost & Sullivan. 2006. [verkkosivusto]. Saatavissa: https://www.frost.com

Gherardi, S., Nicolini, D. & Odella, F. 1998. What do you mean by safety? Con-flicting perspectives on accident causation and safety management in a construc-tion firm. Journal of Contingencies and Crisis Management, Vol. 6, No. 4, s. 202–213.

Growth Partnership Service: Defense & Security. 2006. Subscription overview. Frost & Sullivan. [viitattu 15.9.2006] Saatavissa: https://www.frost.com

Hakala, J. 2004. Vartioimisliikkeen rooli turvallisuuden ylläpitäjänä. Turvallisuusalan vuosikirjassa 2005. Helsinki: Finnsecurity ry. S. 23.

Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi 69/2001. FINLEX, Valtion säädöstietopankki. Ajantasainen lainsäädäntö. [viitattu 30.1.2007].
Saatavissa: http://www.finlex.fi/ fi/esitykset/he/2001/20010069

Hernesniemi, H. 2004. Klusteri – menestyksen avuksi. Elintarvikkeet ja terveys -teknologiaohjelman vuosiseminaari 31.3.2004. [viitattu 15.5.2006] Saatavissa: http://websrv2.tekes.fi/opencms/opencms/OhjelmaPortaali/Kaynnissa/ELITE/fi/ Dokumenttiarkisto/Viestinta_ja_aktivointi/Seminaarit/Vuosiseminaari04/Tekes3103041.ppt

Homeland Security Advanced Research Projects Agency (HSARPA). 2006. SBIR Program. [Verkkosivusto] [viitattu 23.9.2006] Saatavissa: http://www.hsarpasbir.com/

Homeland Security Reseach. 2006. [verkkosivusto] [viitattu 23.9.2006] Saatavissa: http://homelandsecurityresearch.com/index.html

Hyvärinen, L. 2002. Turvateknologia Pohjois-Savossa. Selvitystyön raportti 2002. Kuopio: Pohjos-Savon TE-keskus, Teknologiayksikkö. 98 s. [viitattu 15.12.2005]. Saatavissa: http://www.tekes.fi/ohjelmat/Turva2003/turvateknologiaselvitys.pdf

Jokinen, H. & Kangasniemi, J. 2004. TRIO-toimenpideohjelma haastaa yritykset kasvuun. ELMO-teknologiaohjelman vuosiseminaari 10.3.2004. Teknologiateollisuus ry. (Esittelykalvot)

Jääskeläinen, J. 2001. Klusteri tieteen ja politiikan välissä: Teollisuuspolitiikasta yhteiskuntapolitiikkaan. Helsinki: Taloustieto Oy. 292 s. (ETLA Elinkeinoelämän Tutkimuslaitos. Sarja A/33.) Väitöskirja.

Kerko, P. 2001. Turvallisuusjohtaminen. Porvoo: PS-kustannus. 368 s.

Laitinen, K. 1999. Turvallisuuden todellisuus ja problematiikka. Tulkintoja uusista todellisuuksista kylmän sodan jälkeen. Tampere: Tampereen yliopisto, politiikan tutkimuksen laitos. 355 s. Väitöskirja. (Studia Politica Tamperensis 7.)

Leskinen, M. 2004. Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät. Opas tilojen omistajalle ja käyttäjälle. Espoo, Sähköinfo Oy. 24 s. Saatavissa: http://www.turva-alanyrittajat.fi/ajankohtaista/toimitilaturvallisuus.pdf

Levä, K. 2003. Turvallisuusjohtamisjärjestelmien toimivuus: vahvuudet ja kehityshaasteet suuronnettomuusvaarallisissa laitoksissa. TUKES-julkaisu 1/2003. Väitöskirja. Tampereen teknillinen yliopisto. 163 s.

Liikanen, E. 2004. Eurooppalainen tietoturva. Tietoturvatapahtuma 2004, Helsingin Messukeskus 5.2.2004.

Tietoturvaklusterin esiselvitys. 2003. Helsinki: Liikenne- ja viestintäministeriö. 37 s. (Liikenne- ja viestintäministeriön mietintöjä ja muistioita B27/2003.)

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Jyväskylä: Gummerus Kirjapaino. 310 s.

Möller, N. 2005. Analysing safety: epistemic uncertainty and the limits of objective safety. Teoksessa: Brebbia, C.A., Bucciarelli, T., Garzia, F. & Guarascio, M. (toim.) Safety and security engineering. Gateshead: WIT Press. S. 63–72.

Naumanen, M. & Rouhiainen, V. (toim.) 2006. Security-tutkimuksen roadmap. Espoo: VTT. 69 s. (VTT Tiedotteita – Research Notes 2327.)

Oikarinen, M. 2003. Turvallisuusteema USA:ssa. TEKES-turvaseminaari 10.3.2003.

Porter, M. E. 1990. The Competitive Advantage of Nations. London: MacMillan. 855 s. (Republished with a new introduction, 1998.)

Porter, M. E. 1998. Clusters and the New Economics of Competition. Harvard Business Review, Nov–Dec 1998, s. 77–90.

Ratliff, E. 2005. Fear, Inc: How Homeland security became the biggest market opportunity since the dotcom boom. Wired, Dec. 2005. S. 258–263, 282, 284. [viitattu 4.9.2005]. Saatavissa: http://www.wired.com/wired/archive/13.12/homeland_pr.html

Raunio, H. 2006. Hytest kehittää vasta-aineita bioterrorismiin. Tekniikka & Talous, 8.6.2006.

Repo, H. 2006. Environics haistaa myrkkykaasut Naton puolesta. Tekniikka & Talous, 27.9.2006.

Rintakoski, K. 2006. Turvallisuus ja yhteiskunta – Euroopan turvallisuustutkimusohjelma ja Suomen mahdollisuudet. Tekes, Turvallisuusalan teknologiaohjelman valmisteluseminaari Helsinki 1.12.2006.

Räikkönen, M. & Lanne, M. 2004. Esiselvitys security-alasta ja sen kehitysnä-kymistä VTT/TUO/RIS:n näkökulmasta. VTT Tuotteet ja tuotanto. 42 s. (TUO42-044979.) (VTT:n sisäiseen käyttöön)

Savola, J. 2004. Turvallisuusjohtaminen ja yhteiskunta. Turvallisuusalan vuosikirjassa 2005. Helsinki: Finnsecurity ry. S. 21.

Steinman, J. 2006. Boom in security short-lived. International Herald Tribune, 7. September.

Suomen Teollisuussijoitus Oy. 2006. Teollisuussijoitukselta ja Atinelta yli miljoonan sijoitus videovalvontajärjestelmiä kehittävään ASANiin. [viitattu 5.10.2006]. Saatavissa: http://www.teollisuussijoitus.fi/ajankohtaista/150206.html

Sölvell, Ö., Lindqvist, G. & Ketels, C. 2003. The Cluster Initiative Greenbook. Stockholm, Bromma tryck AB. 92 s.

Tekes. 2006. Tekes valmistelee turvallisuusalan teknologiaohjelmaa. [viitattu 27.9.2006] Saatavissa: http://akseli.tekes.fi/opencms/opencms/OhjelmaPortaali/ohjelmat Turva/fi/system/uutinen.html?id=2696&nav=Uutisia

Turvallisuus.net. 2006. Yritysturvallisuus. [viitattu 27.9.2006] Saatavissa: www.turvallisuus.net

Turvallisuusohjelman valmistelu. 2006. Ympäristöturvallisuus sektorikuvaus. Luonnos. Tekes. 9 s.

Viitanen, M., Karvonen, T., Vaiste, J. & Hernesniemi, H. 2003. Suomen meriklusteri. Helsinki: Tekes. 191 s. (Teknologiakatsaus 140/2003.)

Virtanen, E. & Hernesniemi, H. 2005. Klusterin evoluutio. Prosessikuvaus. Helsinki: Tekes. 282 s. (Teknologiakatsaus 174/2005)

Yritysten rikosturvallisuus 2005 – Riskit ja niiden hallinta. 2005. Helsinki: Keskuskauppakamari ja Helsingin seudun kauppakamari. 55 s.

YTNK. 1999. Yritysturvallisuuden neuvottelukunta. Helsinki: Teollisuuden ja Työnantajain Keskusliitto & Palvelutyönantajat ry. 10 s.

YTNK. 2006. Yritysturvallisuuden osa-alueet [verkkojulkaisu]. Yritysturvallisuus EK. [viitattu 1.6.2006]. Saatavissa: http://www.ek.fi/ytnk/yritysturvallsuus/index.php.

Yritysten verkkosivuja

http://www.abloy.fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.asansecurity.com/ [verkkosivusto] [viitattu 15.2.2007]

http://www.bewator.com/fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.environics.fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.f-secure.fi/] [verkkosivusto] [viitattu 15.2.2007]

http://www.g4s.com/fin/fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.hedpro.fi/etusivu_security [verkkosivusto] [viitattu 15.2.2007]

http://www.insta.fi/insta_defsec/ [verkkosivusto] [viitattu 15.2.2007]

http://www.fi.issworld.com [verkkosivusto] [viitattu 15.2.2007]

http://www.patria.fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.rapiscansystems.com/ [verkkosivusto] [viitattu 15.2.2007]

http://www.temet.fi/[verkkosivusto] [viitattu 15.2.2007]

http://www.turvatiimi.fi/ [verkkosivusto] [viitattu 15.2.2007]

http://www.turvaykkoset.fi/ [verkkosivusto] [viitattu 15.2.2007]

Liite A: Turvallisuuteen liittyviä viranomaisia

Kauppa- ja teollisuusministeriö Huoltovarmuuskeskus Kuluttajavirasto Puolustustaloudellinen suunnittelukunta Turvatekniikan keskus (TUKES)	*Oikeusministeriö* Oikeuslaitos Onnettomuustutkintakeskus Rikoksentorjuntaneuvosto Rikosseuraamusvirasto Tietosuojavaltuutetun toimisto
Sisäasiain ministeriö Hätäkeskuslaitos Kihlakunnat Pelastustoimi Poliisi Rajavartiolaitos Turvallisuusalan neuvottelukunta Turvallisuusalan valvontayksikkö	*Sosiaali- ja terveysministeriö* Kansanterveyslaitos Säteilyturvakeskus Työsuojeluhallinto Vakuutusvalvontavirasto
Ympäristöministeriö Alueelliset ympäristökeskukset Itä-Suomen Ympäristölupavirasto Länsi-Suomen Ympäristölupavirasto Pohjois-Suomen Ympäristölupavirasto Suomen ympäristökeskus	*Ulkoasian ministeriö* Suomen edustustot ulkomailla Ulkoasianhallinto
Valtiovarainministeriö Tulli	*Puolustusministeriö* Puolustusvoimat
Liikenne- ja viestintäministeriö Lentoturvallisuushallinto Viestintävirasto	

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2388
VTT–TIED–2388

Tekijä(t)
Lanne, Marinka & Kupi, Eija

Nimeke

Miten hahmottaa security-alaa?
Teoreettinen malli Suomen security-liiketoiminta-alueista

Tiivistelmä

Turvallisuusala on moniselitteinen ja osin hahmottumatonkin käsite. Termi yhdistetään helposti Suomen virallisissa tilastoissa esiintyvään toimialaluokitukseen vartiointi- ja turvallisuuspalvelut. Turvallisuuteen liittyviä tuotteita, ratkaisuja ja palveluja tarjoavien yritysten joukko on kuitenkin huomattavasti tätä yksittäistä toimialaa laajempi.

Tässä julkaisussa pohditaan alustavasti kansallisella tasolla niitä liiketoiminnan alueita, joiden ympärille security-liiketoiminta todennäköisimmin voisi kehittyä. Lisäksi pohditaan, miten nämä liiketoiminta-alueet voisivat muodostaa klusterin ja mitkä tekijät vaikuttavat security-markkinoihin. Security-termillä turvallisuuden tarkastelu rajataan etenkin tahallisilta vahingonteoilta suojaamiseen.

Markkinatutkimusten, muun kirjallisuuden sekä yrityshaastattelujen pohjalta hankkeessa muodostettiin käsitys securityyn liittyvästä toimijakentästä sekä markkinoihin vaikuttavista tekijöistä. Markkinoiden nähtiin muodostuvan erilaisten uhkien kautta. Markkinoihin vaikuttaviksi tekijöiksi tunnistettiin esimerkiksi poliittiset päätökset, lainsäädäntö, standardointi, teknologian kehitys, ihmisten yleinen käsitys turvallisuudesta sekä erilaisten ratkaisujen yleinen hyväksyttävyys ja vaikutukset yksityisyyden suojaan. Securityyn liittyvissä markkinatutkimuksissa käsiteltiin hyvinkin hajanaisesti erilaisia teknologioita, tuotteita ja suojattavia kohteita.

Yrityshaastattelut tukivat käsitystä siitä, että security-liiketoiminta-aluetta ei mielletä vakiintuneena kokonaisuutena, vaan securityyn liittyy useita eri liiketoiminta-alueita. Hankkeessa päädyttiin lopulta kuvaamaan teoreettista security-klusteria havaittujen liiketoiminta-alueiden yhdistelmänä. Teoreettista klusteria ei kuitenkaan voi pakottaa toimimaan, vaan klusterin syntyyn on tultava tarve eri liiketoiminta-alueiden sisältä.

ISBN
978-951-38-6924-3 (URL: http://www.vtt.fi/publications/index.jsp)

Avainnimeke ja ISSN	Projektinumero
VTT Tiedotteita – Research Notes 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	4790

Julkaisuaika	Kieli	Sivuja
Toukokuu 2007	Suomi, engl. tiiv.	52 s. + liitt. 1 s.

Projektin nimi	Toimeksiantaja(t)
Security-VTT: Suomen security-klusterin hahmottaminen	VTT

Avainsanat	Julkaisija
business security, Finland, security markets, service providers, government, research communities, educational institutions, financial institutions, defence industry, CBRNE-detection technology providers, guarding and security services, transport security solutions, locking solutions	VTT PL 1000, 02044 VTT Puh. 020 722 4404 Faksi 020 722 4374

Series title, number and
report code of publication

VTT Research Notes 2388
VTT–TIED–2388

Author(s)
Lanne, Marinka & Kupi, Eija

Title

Security as an area of business

Abstract

As an area of business, the concept of security is quite ambiguous and unclear. Security market research reports categorise the security industry in different ways and into several parts; there is currently no common approach, and even the areas and concepts are not well-defined. Even so, there is mutual consensus that the security industry has been growing. This report considers, at a national level, which areas of business have potential in the security sector, how those areas can constitute a cluster, and which factors affect security markets. Throughout this report, security is considered to be the state of being free from the danger of intentional damage.

The business of security includes companies that provide products and services, the companies buying and using those products and services, the government, the research community, educational institutions, financial institutions, and institutions that promote collaboration. Individuals and society also play an important role: as clients, users of products and services, research subjects, and even as a subject of influence. A diverse range of dangers and the associated perceptions on risk have given rise to an extensive and broad security market. There are several different factors that influence the market, for example, political decisions, legislation, standards, technology trends, public opinions on safety and security, and public acceptability of different solutions and the associated effects on privacy protection.

In this study, a theoretical security cluster was outlined by combining some areas of the security business: the defence industry, providers of CBRNE-detection technologies, guarding and security services, transport security solutions and locking system solutions. These areas of business, however, represent only part of the entire security business. Furthermore, this cluster model is purely theoretical and only a real need, deriving from the desires of the stakeholders (members of theoretical cluster), can make the cluster function.

ISBN
978-951-38-6924-3 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN	Project number
VTT Tiedotteita – Research Notes 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	4790

Date	Language	Pages
May 2007	Finnish, engl. abstr.	52 p. + app. 1 p.

Name of project	Commissioned by
Security-VTT: Suomen security-klusterin hahmottaminen	VTT Technical Research Centre of Finland

Keywords
business security, Finland, security markets, service providers, government, research communities, educational institutions, financial institutions, defence industry, CBRNE-detection technology providers, guarding and security services, transport security solutions, locking solutions

Publisher
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

Turvallisuusala on moniselitteinen ja osin hahmottumaton käsite. Tässä julkaisussa pohditaan alustavasti kansallisella tasolla niitä liiketoiminnan alueita, joiden ympärille security-liiketoiminta todennäköisimmin voisi kehittyä. Lisäksi pohditaan, miten nämä liiketoiminta-alueet voisivat muodostaa klusterin ja mitkä tekijät vaikuttavat security-markkinoihin. Security-termillä turvallisuuden tarkastelu rajataan tahallisilta vahingonteoilta suojaamiseen.

Markkinatutkimustarkastelu sekä yrityshaastattelut tukivat käsitystä siitä, että security-liiketoiminta-aluetta ei mielletä vakiintuneena kokonaisuutena. Hankkeessa kuvataan teoreettista security-klusteria esiin nousseiden liiketoiminta-alueiden yhdistelmänä. Teoreettista klusteria ei kuitenkaan voi pakottaa toimimaan, vaan klusterin syntyyn on tultava tarve eri liiketoiminta-alueiden sisältä.

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

VTT
PB 1000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

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

ISBN 978-951-38-6924-3 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)