



# LAUREA

# SATERISK-projektin suunnittelu ja vaatimusmäärittely



Viitanen, Jouni

2009 Leppävaara

**Laurea-ammattikorkeakoulu**  
Laurea Leppävaara

## **SATERISK-PROJEKTIN SUUNNITTELU JA VAATIMUSMÄÄRITTELY**

Jouni Viitanen

Jouni Viitanen

### SATERISK-projektin suunnittelu ja vaatimusmäärittely

Vuosi 2009

Sivumäärä 94

SATERISK-projektin tarkoituksena on selvittää satelliittipaikannuksen käyttöön liittyvät riskit. Paikannusta käytetään yleisesti tuottavuuden ja turvallisuuden parantamiseen. Länsimaissa yleisesti käytetty paikannusjärjestelmä GPS saa EU:n Galileosta lähivuosina kilpailijan. Galileo on tulevaan paikantamiskäyttöön liittyviä ongelmia pitää kartoittaa nyt, kun se on vielä mahdollista. Projekti pyrkii myös ratkaisemaan ja ennaltaehkäisemään ongelmia GPS- ja Galileo -järjestelmissä uusien teknologisten ratkaisujen avulla.

Tässä työssä kuvataan SATERISK-projektin suunnittelu, tehdään vaatimusmäärittely. Tuotetaan määritykset sille, mitä riskejä tulevaisuuden seurantajärjestelmien ja uuden teknologian tulee hallita. Tarvitaanko uusia, kenties autonomisia tai interaktiivisia toimintamuotoja, joilla täytetään sekä turvallisuusalan, lainsäädännön, että yksityisyydensuojan vaatimukset.

Projektin ensimmäinen vaihe tuottaa projektisuunnitelman mukaisesti riskianalyysin satelliittipaikannuksen vaikutuksista paikannuttajan ja paikannettavan riskeihin paikannuksen käytön, teknisten sovellutusten ja lainsäädännön osalta.

Projekti pyrkii tilanteeseen, jossa paikannukseen ja seurantaan liittyvät turvallisuusalan toimintamallit, rikollisten suorittamat vastatoimet, lait sekä niiden muodostama liiketoiminnallinen riski eivät estä suomessa, tai valtakunnan rajojen yli tapahtuvaa paikannusta. Tämä paikannus on usein koneiden välistä paikannukseen liittyvää kommunikaatiota, jota kutsutaan M2M (Machine-to-Machine) kommunikaatioksi.

Galileo toimii aikaisintaan vuonna 2013, Riskienhallinnassa jo sen perusluonteesta johtuen katsotaan aina tulevaisuuteen. Useiden vuosien tulevaisuuteen suuntautuminen vaatii kuitenkin erilaisen lähestymismetodin. Tärkeimpiä vaatimuksia on suunnata riskikartoitusta myös tulevaisuuteen skenaariotyöskentelyn avulla. Tavoitteena on luoda erilaisia laite- ja palveluinnovaatioita tai tehostaa niiden käyttöönottoa.

Projektin aikana tehdyn tutkimustyön tuloksena suomalaiselle turva-alalle syntyy uutta kansainvälisen tason osaamista. Projekti tuo alalle myös uusia toimintamalleja ja ohjaa paikannusalan laite- ja järjestelmätoimittajien tuotekehitystä.

Avainsanat: vaatimusmäärittely, paikannus, satelliittipaikannus, GIS, riski, GPS, Galileo

Jouni Viitanen

### Planning and requirement analysis of the SATERISK-project

Year	2009	Pages	94
------	------	-------	----

SATERISK-projects goal is to find all the risks in using satellite-navigation. Tracking is used to decrease risks in logistics and optimize workflow. We need to know what are the risks and needs in legislation and in tracking equipments and systems to keep anyone safe. GPS-satellite navigation system commonly used in western counties will get a rival from EU:s own Galileo. Galileo will be operative in 2013. It is timely to evaluate the risks and needs, if we want to have guidance for future systems, legislation and regulation in general.

This requirement analysis is the first phase of SATERISK-project. What are those risks that must be tackled in tracking systems, and new technology used in them? Do we need new adaptive systems that can take care of security, legality and privacy issues, reacting actively to faced conditions and state of approved limits?

Is the lack of international legislation or user knowledge in tracking a risk?

Is it possible, that if you are tracking an asset in a foreign country, you might violate the local laws. Can the local authorities use other interpretation and think that tracking can in fact be seen as espionage? Is the tracker violating the privacy of the truck driver or other third party?

Projects goal is that all the procedures used by security oriented companies or authorities, counter measurements by the criminals, legislation and the business risks created by the all of them is not preventing the use of tracking in international traffic.

Most of this communication in tracking systems is machine to machine communication (m2m).

Key words: Requirement analysis, Galileo, Gps, Risk, GIS, Tracking

## Sisällys

1	Johdanto .....	6
1.1	Taustaa .....	6
1.2	Tarve.....	9
1.3	Tavoite .....	12
1.4	Rajaukset.....	13
1.5	Raportin rakenne .....	14
2	Tutkimusmenetelmät .....	14
2.1	Empiirisen aineiston hyödyntäminen ja aineistolähtöinen analyysi .....	15
2.2	Triangulaatio .....	16
3	Käsitteiden määritelmät .....	17
4	Vaatusmäärittely .....	23
4.1	Vaatusmäärittely tarkistaminen .....	23
4.2	Tärkeimmät vaatimukset.....	24
4.3	Riskin määritelmä .....	24
4.3.1	SATERISK-projektissa riski ei sisällä mahdollisuutta .....	25
4.3.2	Mahdollisuudet.....	25
4.3.3	Muutos riskiyhteiskunnan suuntaan otettava huomioon.....	26
5	Kohteellisuus vaatimukset .....	27
5.1	Tutkimuksen perspektiivi on paikannuttajan näkökulma.....	27
5.2	Venäjä otettava huomioon.....	28
5.3	Käyttäjävaatimukset .....	29
5.4	Reaaliaikaisuusvaatus.....	30
5.5	Yhteiskuntavastuu .....	31
5.5.4	Tiedonvaihto elinkeinoelämän ja viranomaisten välillä.....	32
5.5.5	Kuljetus- ja logistiikka-alaan kohdistuva rikollisuus .....	33
5.5.6	Yksityisyyden suoja .....	33
5.6	Tavoitteena tulevaisuuden turvallisemmat palvelut. ....	34
5.6.7	Nykytila .....	35
5.6.8	Tulevaisuus .....	35
5.7	GALILEON otettava huomioon .....	36
5.8	GPS otettava huomioon.....	37
5.9	GLONASS otettava huomioon .....	37
5.10	COMPASS (Beidou) otettava huomioon.....	38
6	SATERIS-projektissa käytettävät prosessit ja työkalut.....	38
6.1	Käytetyt menetelmät on kirjattava osaksi riskikartoitusraporttia.....	38
6.2	Graunded Theory .....	39
6.3	Peste .....	39

6.4	Villi kortti (Wild card) .....	40
6.5	SWOT-analyysi.....	41
6.6	Riskikartoituksen yhteenveto.....	41
6.7	Skenaariotyöskentely .....	42
6.8	Toinen iteraatio skenaarioiden yhteensovittamiseksi.....	43
6.9	Delfoi-menetelmä .....	44
6.10	Tulevaisuustaulukko.....	44
7	Tarve aikakriittisille GIS-järjestelmille.....	45
7.1	Tilannekuvan muodostamisen ongelmia .....	46
7.2	EU-rajat ylittävä liikenne .....	52
7.3	Samantyyppisiä projekteja muualla maailmassa.....	56
7.4	Tavoitteet, linjat ja odotettavissa olevat tulokset.....	56
8	Seuraavat kehittämis- ja tutkimuskohteet.....	57
	Lähteet: .....	58
	Liitteet:.....	64
	Liite 1: SATERISK-projektin suunnitelma.....	65
	Liite 2, TEKES-rahoituspäätös SATERISK-projektille .....	85
	Liite 3: Jamming detection in the future navigation and tracking systems .....	87

## 1 Johdanto

Satelliittipaikannus ja sen käyttö ovat yksi nopeimmin kasvavista toimialoista. Lissabonin strategian mukaisesti EU ([www.ESA.eu](http://www.ESA.eu)) tekee erittäin huomattavia panostuksia paikantamiseen liittyvien projektien toimintaan. Suomessa TEKES on vahvasti tukemassa alan tutkimustoimintaa. EU:n tasolla suurin ja näkyvin projekti on Galileo-satelliittipaikannusjärjestelmä, jonka piti olla Public-Privat-Partnership-projekti. Valitettavasti toistaiseksi rahoitus on kuitenkin jäänyt julkisen sektorin vastuulle.

Nykyisin suurin osa paikannuksesta on end user -paikannusta, eli palveluiden etsintää tai ajoneuvonavigointia, mutta paikannusta käytetään myös yleisesti tuottavuuden ja turvallisuuden parantamiseen. Valtioneuvosto on sisäisen turvallisuuden ohjelmassa ohjeistanut (Sisäasiainministeriön julkaisu 15/2006), että kun yrityksissä kehitetään uusia menetelmiä ja toimintamalleja on tuotekehittelyn yhteydessä tuotteisiin ja palveluihin voitava sisällyttää riittävät rikostorjunnalliset ja turvallisuutta parantavat ominaisuudet.

### 1.1 Taustaa

Kirjoittajalla on yli kymmenen vuoden kokemus satelliittipaikannusjärjestelmien kehittämisestä ja käytöstä. SATERISK-projekti on syntynyt kirjoittajan kokemuksista ja havainnoista, jotka antoivat viitteitä hallitsemattomista riskeistä paikannuksen käytössä. Riskit eivät johtuneet suoraan laitteista, eikä myöskään pelkästään niiden käyttötavoista, vaan näiden molempien yhdistelmistä. Kokonaisuutta ei selvästikään kukaan ollut perehtynyt miettimään.

Havainnot alkoivat muuttua ajatuksista kirjalliseen muotoon Laurea AMK:n kansainvälisen turvallisuusjohtamisen opintojen yhteydessä. Tuolloin kirjoittaja laati omien ideoidensa pohjalta yhdessä Jussi Ojalan ja Julius Tuomiston kanssa projektisuunnitelman (liite 1) ja TEKES-hakemukseen, joka johti myöhemmin positiiviseen rahoituspäätöksen (liite 2) ja SATERISK-projektin syntyyn.

Kirjoittaja on myös osallistunut toisena kirjoittajana 16 th Saint Petersburg International Conference of Integrated Navigation Systems (25-27.5.2009) konferenssipaperin kirjoittamiseen. Kirjoittaja on osakkaana yrityksessä joka valmistaa teknisen tiedustelun välineistöä viranomaiskäyttöön. Yksi tuoteryhmä yrityksellä on juuri satelliittipaikannuksen käyttöön perustuvat tiedonkeruulaitteet eli IGD:t (Information Gathering Device).

Tätä työtä varten on haastateltu laajasti sekä yksityisen että viranomaispuolen edustajia. Haastatellut henkilöt on valittu sillä perusteella, että heillä on mittavaa kokemusta satelliitti

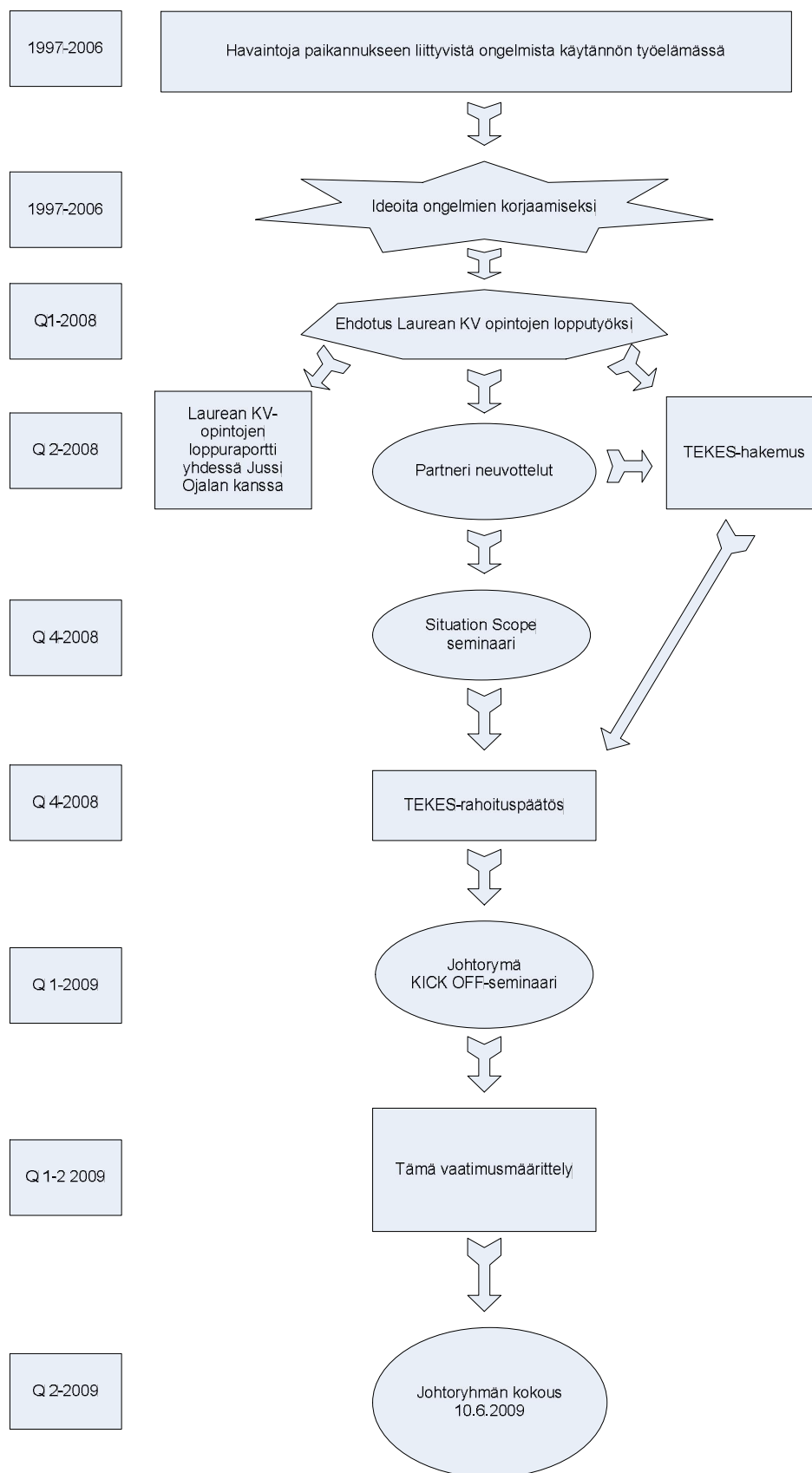
paikannusjärjestelmistä, turvallisuus- tai logistiikkalasta tai kaikista näistä alueista. Haastatteluja siteerataan tässä työssä anonymisti siten, että kaikkien haastatellut mainitaan lähde-  
luettelossa, mutta ei yksilöidä kyseisen lainauksen kohdalla. Näin on menetelty koska osaa tiedoista ei voitaisi tämän työn käyttöön antaa, jos ne voitaisiin yhdistää suoraan johonkin alan toimijaan. Kirjoittaja on katsonut olevan tärkeää saada kaikki mahdollinen tieto tarpeista ja riskeistä käyttöön. Haastattelujen muistiinpanot ovat kirjoittajan hallussa.

Kirjallisista lähteistä saatua tietoa, kirjoittajan omaa kokemusta, sekä haastatelluilta henkilöiltä saatua tietoa mahdollisista riskitekijöistä on tässä vaatimusmäärittelyssä hyödynnetty nostamalla havaittujen riskitekijöiden abstraktiotasoa ylemmäs. Empiiristen kokemusten ja kirjallisuuden pohjalta on pyritty löytämään riskien lähteet ja draiverit, joiden avulla on siten määritelty aihealuevaatimukset. Tätä pohjaa on pyritty avaamaan kirjoittamalla vaatimusten yhteyteen perusteluja.

Tältä ylemmältä abstraktiotasolta palataan sitten riskikartoitusprosessissa takaisin käytännön riskeihin, mutta nyt huomattavasti tiheimmällä seulalla ja useamman henkilön toimesta. Näin riskikartoituksesta on tarkoitus saada kattava.



Kuvio 1. SATERISK-projektiin johtanut tapahtumaketju



## 1.2 Tarve

Paikannusta käyttävät viranomaiset ja yksityinen turvallisuusala yleisesti, vaikka siitä arvioidaankin syntyvän riskejä. Riskejä on yksittäisen toimijan erittäin vaikeata kartoittaa, ja monesti vain toivotaan että syntyvät riskit olisivat vaikutukseltaan vähäisempiä kuin ne, joita paikannuksella poistetaan tai pienennetään. Paikannuksesta syntyvät riskit, niiden todennäköisyys ja mahdolliset vaikutukset tulee olla tiedossa.

Sirkka Heinonen on tulevaisuuden tutkimuksen seuran Futura-lehden ( 4/2008, 13) artikkelissaan kiinnittänyt huomiota siihen, että teknologiaa kehitetään ja käytetään ongelmien ratkaisemiseksi ja riskien välttämiseksi, mutta huomattavasti vähemmän huomiota kiinnitetään teknologian itsensä synnyttämille riskeille.

Esimerkiksi rahtiin kohdistuva varkaus on joko yrityksen sisäistä tai ulkoista toimintaa tai molempien yhdistelmä. Varkaus voi tapahtua toimitusketjun useissa eri solmukohdissa tai kuten usein Euroopassa myös maantiekuljetusten yhteydessä. Rahtikirjat ja paikannustieto siirtyvät sähköisesti paikasta toiseen, mutta hyvin harvalla on käsitystä missä ja minkälaiset laitteistot tietoa välittävät.

Sisäasiainministeriön yrityksiin kohdistuvan rikollisuuden tilannekuvan (2009) mukaan logistiikkatoimintoihin kohdistuu monimuotoista ja kooltaan erilaista omaisuusrikollisuutta. On sekä pieniä, monesti myös sarjoina toteutettuja varkaustapauksia että suuria kertaluontoisia joko tavaraeraan, ajoneuvoon ja lastiin tai kalustoon kohdistuvia varkausrikoksia. Murtautamalla tehtyjä rikoksia kohdistuu sekä ajoneuvoihin että terminaaleihin. Suomalaisyritysten hoitamia kuljetuksia on ryöstetty eniten eräissä Länsi-Euroopan maissa ja Venäjällä. Näissä tapauksissa myös kuljettaja saattaa joutua väkivallan kohteeksi. Itse kuljetusliiketoiminta kärsii myös petosrikollisuudesta johtuvia tappioita.

Sisäministeriön mukaan kuljetus- ja logistiikkatoimintojen kansainvälisyys, nopeus ja sujuvuus tekevät alasta erityisen alttiin ammattimaisen ja järjestäytyneen rikollisuuden toiminnalle sekä kohteena että välineenä. Huomattava ja jatkuvasti kasvava osa logistiikka-alaan kohdistuvista omaisuusrikoksista onkin ammattimaista tai järjestäytynyttä rikollisuutta. Teot toteutetaan suunnitelmallisesti ja ammattitaitoisesti, logistiikan toimintaympäristöä järjestelmällisesti hyödyntäen tarvittaessa väkivaltaisin keinoin. Sekä kaluston turvallisuuden parantaminen että arvokkaat kohteet kasvattavat henkilökunnan riskiä joutua väkivallan kohteeksi.

Claire Mayhew, Australian Institute of Criminology, in "The Detection and Prevention of Cargo Theft" (2001)kertoo raportissaan, että 80 % varkauksista on lähtöisin yritysten sisäältä. Rikollisilla on suuri tarve saada tietoa siitä, missä tavara on ja kuinka arvokkaasta lastista on kysy-

mys. Vain pieni osa kuljetuksista on sellaisia joille löytyy käyvät jälkimarkkinat ja joita kannattaa varastaa.

Euroopan Unioni on kiinnittänyt tähän huomiota ja Neuvoston asetuksessa toimitusketjun turvallisuuden parantamisesta (SEC(2006)251). Raportissa todetaan että ilmailu- ja meriliikenteen turvallisuuteen on kiinnitettävä runsaasti huomiota. Meri- ja lentoliikennemarkkinoilla on vain hyvin rajallinen määrä toimijoita, jotka toimivat ennen kaikkea valvottavissa olevilla maantieteellisesti rajatuilla ja määritellyillä alueilla. Satamissa on voimassa ISPS (International Ship and Port facility Security Code) -ohjeistus, jonka tarkoitus on lisätä meriturvallisuutta satamissa ja laivoilla. Toimielin tämän koodin takana on YK:n alajärjestö IMO (International Maritime Organization). Ohjeistuksen kehittäminen lähti suurelta osin Yhdysvaltojen turvallisuustarpeista.

Ohjeistuksessa painotetaan mm seuraavia kohteita:

- Aidatut satama-alueet.
- kuljetuksille varattava saapumisaika etukäteen, jolla taataan viivytyksetön pääsy satama-alueelle.
- Kaikkien yksiköiden mukana on oltava tavaraluettelo
- vaaralliset aineet ilmoitettava erikseen.
- kuljettajien yöpyminen aidatun alueen sisäpuolella on kielletty.
- Viranomaisilla on oikeus suorittaa pistokokeita kaikista lastiyksiköistä.

ISPS-koodi jakautuu lisäksi turvallisuustasoihin, jotka vaihtelevat tilanteesta ja mahdollisista uhkakuviista riippuen. Maan turvallisuusviranomaiset määräävät turvallisuustasoista ja ne voivat vaihdella satamasta satamaan.

Lentoasemia koskevat varsin tiukat kansainvälisen siviili-ilmailujärjestön ICAON (International Civil Aviation Organization) määräykset. Lentoliikenteeseen liittyvä logistiikkaketju tulee olla tunnistettu ja suojattu. Satamissa ja lentoasemilla turvajärjestelyihin on siis totuttu ja ne ovat varsin tehokkaita sekä osin lain tasolla säädeltyjä.

Maaliikenteen toimitusketjulla on kokonaisuutena hyvin erilaiset mittasuhteet, juuri tästä syystä sinne on hyvin vaikeaa luoda satamien tai lentoasemien tasoista turvallisuutta. Jo pelkästään kuljetuksia ja niitä avustavia palveluja tarjoaa Komission tilastojen mukaan 595 971 yritystä, jotka tekevät 258014 M € liikevaihtoa (European comission 2008, 100-101).

Niiden koko vaihtelee suurista monikansallisista yhtiöistä pienyrityksiin, ja ne edustavat hyvin erilaisia toimintakulttuureja ja yritystaustoja. Ne kattavat koko yhteisön alueen.

Useimmilla näistä yrityksistä ei nykyisellään ole turvallisuudenhallintajärjestelmää, ja yleisesti ottaen turvatasoja on vasta alettu parantaa. Tulevaisuudessa tullaan kiinnittämään paljon huomiota siihen että toimintaketjun toimintoihin liittyvä tietojenkäsittely on suoritettava suojatusti. Vanha sanonta on, että ketju on yhtä heikko kuin sen heikoin lenkki. Satamien ja lentokenttien muutoin korkea turvataso kärsii, jos turvallisuus pettää muualla, tai ainakin se lisää näiden pisteiden jo muuten kovaa ruuhkaisuutta, kun kaikki pitää tarkistaa uudelleen.

Transported Assets Protection Association (TAPA 2009, 18) pitää eräänä tärkeänä keinona estää arvokkaiden lastien varkauksia sitä, että autot varustetaan GPS- tai muulla vastaavalla paikannuksella. TAPA ei kuitenkaan aseta paikannuslaitteistoille mitään vaatimuksia, riittää, että sellainen on asennettuna ja sitä käytetään.

Suomen sisäministeriö on todennut, että Logistiikka-alan muuttuva toimintaympäristö asettaa haasteita alaan kohdistuvalle valvonnalle ja että alalla on syytä panostaa rikostorjunnan toimintamallien hahmottamiseen sekä alan yksityisten toimijoiden että viranomaisten keskuudessa.

Satelliittipaikannusta voidaan hyödyntää myös muuhun turvallisuustyöhön, kuin vain rikostorjuntaan. The Federal Motor Carrier Safety Administration (FMCSA) joka on U.S. Department of Transportation alainen virasto ja jonka päätehtävä on pahojen vaikutuksiltaan suurien liikenne onnettomuuksien vähentäminen on tehnyt testejä paikannuksen eduista liikenne ja ympäristö-turvallisuudelle.

Viraston raportissa todetaan että GPS-paikannuksen ja hätäpainikkeiden käyttö tuotti positiivisen tuoton investoinneille paikannukseen kaikissa tutkitussa käyttöskenaariossa. Erityisen paljon riskit vähenivät vaarallisten aineiden kuljetuksissa ja nimenomaan niiden varkausriskien pienenemisenä. Tutkimuksessa on laskettu rahallinen arvo myös yleisen turvallisuuden paranemiselle, kuten terrorismiriskin pienenemiselle.

SATERISK-projekti käsittelee satelliittipaikannusteknologiaa ja sen käyttöä, sekä tuotetun informaation saattamista luotettavaan, helposti hyödynnettävään muotoon esimerkiksi tilannekuvan luomista varten. Erilaisten ulkoistamistoimintojen jatkuessa tilannekuvaa tulevat tarvitsemaan Suomessa satelliittipaikannusta suorittavien viranomaisten, kuten Poliisin, Tullin, Puolustusvoimien ja Rajavartiolaitoksen lisäksi myös paikannustoimintaa suorittavat yksityiset safety- ja security- sektorien yritykset.

Riskien kartoituksen tarve on ilmeinen ajatellen kokonaisia aloja, jotka hyödyntävät paikannussovellutuksia. Tässä projektissa tehtävän riskikartoituksen pääpainopiste on kuitenkin turvallisuuden tuottamisessa. Turva-alalla käytetään paikannusta ihmisten, ympäristön ja omaisuuden suojaamiseen, mutta myös edellä mainitun tilannekuvan luomiseen.

Yksi keskeinen osa ihmisten turvallisuuden parantamisessa on huumausaineiden salakuljetuksen estäminen. Euroopan unionissa arvioidaan että noin 25-30 miljoonaa aikuista on käyttänyt jotakin laitonta huumausainetta viimeisen vuoden aikana. Huumausaineiden käyttö ja salakuljetus rikkovat yhteiskuntarauhaa aiheuttaessaan rikoksia ja korruptiota. Päihteiden käyttö on myös merkittävä EU:n kansalaisten terveyteen vaikuttava tekijä, sillä huumeisiin liittyvät tartuntataudit (HIV/AIDS, hepatiitti) ovat merkittävä kansanterveyden uhka EU:ssa. Maailmanlaajuisesti laittomien huumeiden kaupan uskotaan olevan maailman kolmanneksi suurin elinkeinoala öljyn ja asekaupan jälkeen. (huumausaineita koskeva EU:n tiedoksianto KOM 2007 781). Samaa reittiä kuin huumausaineet kulkee myös ihmiskauppa, aseet ja laiton raha (haastattelut).

### 1.3 Tavoite

Tällä vaatimusmäärittelyllä pyritään varmistamaan, että myöhemmin tuotetut tulokset ovat relevantteja suhteissa esitettyihin tarpeisiin. Kirjallisilla ohjeilla pyritään varmistamaan, että työryhmien riskikartoituksen tulokset ovat keskenään vertailukelpoisia. Tavoitteena on kerätä mahdollisimman yksityiskohtaista tietoa, jota voidaan hyödyntää useissa eri työpaketeissa. Samalla myös varmistetaan, että työpakettien tuottama tieto on yhdistettävissä saumattomaksi ja yhteneväksi kokonaisuudeksi. Projektin lähtökohta on paikannuksen nykyisen käytön tarkastelu ja analysointi. Tämän tavoitteen täyttämiseksi on projektiin jo alun perin pyritty ottamaan asiantuntija jokaiselta paikannuksen arvoketjun osa-alueelta.

Tyypillisesti ratkaisuksi tarpeisiin on yritetty tuottaa joku fyysinen tuote tai sitten teknologiaa hyödyntävä palvelu. Nykyään tarve muodostuu kuitenkin epämääräisemmäksi käsitteeksi ja sen tyydyttäminen on vaikeammin hahmoteltavissa. Tarve ei ole yksinkertainen esine tai palvelu, vaan arvoketju, joka muodostuu itse tuotteesta ja siihen kiinteästi liittyvistä lisäarvopalveluista.

On tarkoitus että SATERISK-projektin mukana saamme kattavan riskikartoituksen, mutta perimmäisenä tarkoituksena ovat tämän uuden tiedon pohjalta syntyvät uudet laite-, palvelu- tai koulutusinnovaatiot. Näiden innovaatioiden on myös tarkoitus luoda uutta, tuottavaa ja kansainvälistä liiketoimintaa.

Tämä vaatimusmäärittely on perusta sille kehitystyölle, jonka avulla määritellään järjestelmän tai palvelun ominaisuudet ja toiminnot. Vaatimusmäärittelyllä pyritään myös selvittämään kaikkien projektissa mukanaolijoiden sekä yhteiskunnan yleiset tarpeet. Vaatimuksia paikannusjärjestelmien toiminnalle asettaa järjestelmän tilaaja, suunnittelija, toteuttaja, sidosryhmät, sen käyttäjät sekä mahdollisesti kotimainen ja kansainvälinen lainsäädäntö. Koska lainsäädäntö on monelta osin puutteellista, eikä pysy aina teknisen kehityksen vauhdissa on otettava huomioon yhteiskunnan yleinen etu, joka ehkä sitten joskus tulevaisuudessa kiteytyy myös lainsäädännöksi ja muuksi regulaatioksi.

#### 1.4 Rajaukset

Tämän vaatimusmäärittelyn kohteena olevan projektin nimi on SATERISK. Kyseinen nimi on yhdistelmä sanoista satellite navigation risks. Nimensä mukaisesti tämä työ käsittelee vain satelliittinavigointia ja sen riskejä. Maailmassa on tällä hetkellä kaksi maailmanlaajuista toimivaa järjestelmää. Pisimpään on toiminut amerikkalaisten GPS, ja venäläisten Glonass on useiden vuosien tauon jälkeen saamassa täyden toimintakykynsä takaisin. Lisäksi tulossa ovat tulossa EU:n galileo, jonka suunnitellaan aloittavan operatiivisen toimintansa 2013 sekä kiinalaisten Compass, jonka kiinalaiset toivovat saavansa toimimaan alueellisesti noin 2011.

Tässä työssä ei käsitellä muuhun paikannukseen, kuten esimerkiksi verkkopaikannukseen liittyviä riskejä. Ulko- ja sisätiloissa tapahtuva verkkopaikannusta tapahtuu eri teknologioilla. Esimerkiksi GSM, WIMAX, WLAN, BT tai ZIG BEE. Asia on sinällään tärkeä ja monessa kohdin riskit muistuttavat satelliittipaikannuksen riskejä. Niiden ottaminen osaksi tutkimusta nykyisillä resursseilla on kuitenkin mahdotonta.

Tässä työssä ei myöskään käsitellä niitä riskejä, jotka liittyvät suoraan satelliitinpaikannusjärjestelmien hallintasegmenttiin. Kyseisen segmentin tehtävänä on valvoa ja ylläpitää järjestelmää. Segmentti koostuu valvonta-aseista joissa tarkkaillaan järjestelmän toimintaa ja tiedotetaan siitä käyttäjiä. Hallintoasemien paikat ovat koko järjestelmän kiintopisteinä. Hallintasegmentin tärkein laite on järjestelmän pääkello, joihin järjestelmän muita kelloja verrataan.

Järjestelmän avaruussegmentti koostuu satelliiteista. Nämä ovat se osa järjestelmää, joka näkyy paikannuksen käyttäjän paikannusvastaanottimelle. Avaruussegmenttiin kuuluvia osia ei tässä työssä käsitellä. Syynä molempiin edellisiin rajauksiin on se, että järjestelmät ovat strategisesti erittäin tärkeitä ja niitä koskeva tieto erittäin salaista ja vaikeaa, ellei mahdoton saada riittäväällä tarkkuudella tämän työn lähtökohdaksi.

Tässä työssä ei myöskään käsitellä differentiaalikorjausjärjestelmistä johtuvia lisäriskejä. Näitä differentiaalikorjauksia käytetään yleisesti lento ja laivaliikenteen paikannuksessa, jossa on mahdollisesti poikkeavia riskejä. Kyseiset palvelut vaativat WAAS-yhteensopivat paikannusvastaanottimet. Normaleissa yleisesti käytettävissä vastaanottimissa ominaisuutta ei ole.

## 1.5 Raportin rakenne

Tässä raportin ensimmäisessä osassa on kerrottu syitä, jotka johtivat tähän projektiin, mihin sillä tähdätään ja miten aihepiiriä on rajattu. Seuraavaksi käydään läpi tutkimusmenetelmiä. Tutkimusmenetelmiä seuraa osio, jossa ovat paikannukseen liittyvät tärkeimmät määritelmät. Määritelmiä on käsitelty varsin laajasti siinä tarkoituksessa, että yhtenäinen ja selkeä kriteeristö helpottaa projektin toimintaa jatkossa.

Seuraavaksi käsitellään projektin varsinainen vaatimusmäärittely. Ensin käydään läpi miten projektissa määritellään riski. Seuraavaksi ovat kohteellisuusvaatimukset. Vaatimuksiin kuuluu myös työkaluvalikoima, eli keinot joilla riskejä kartoitetaan sekä nykytilanteessa, että tulevaisuudessa.

Vaatimusten jälkeen käydään vielä erikseen läpi tarve reaaliaikaisille GIS-järjestelmille. Näiden jälkeen on vuorossa tutkimussuunnitelma sellaisena kuin se hyväksyttiin TEKESissä.

Lopussa vielä vedetään yhteen tavoitteita ja niitä tutkimustarpeita jotka eivät mahdu vielä nykyisen projektin piiriin.

## 2 Tutkimusmenetelmät

Elektroniikkateollisuudessa puhutaan ns. koiranvuosista, eli yhdessä vuodessa on tavallaan seitsemän vuotta. Tämän voi helposti laskea esimerkiksi siitä, että Nokian ensimmäiset GSM-puhelimet olivat lähes muuttumattomina markkinoilla useita vuosia. Nykyään markkinoille saapuu koko ajan uusia malleja, jotka poistuvat jopa alle vuodessa markkinoille tulostaan. Turvallisuusalan ohuilla resursseilla tässä kehitysvauhdissa on joskus vaikea pysyä mukana. Jatkuvasti tulee uutta teknologiaa, jonka käyttökelpoisuutta pitäisi arvioida, mutta resursseja tähän toimintaan ei ole saatu lisää. Selvitystyössä ei aina voida käydä asioita läpi kovin perusteellisesti, koska muutoin kyseinen teknologia on jo vanhentunutta selvityksen valmistuessa. Tähän ongelmaan tiedon käyttökelpoisuudesta suhteessa aikaan ja käytettyyn metodiin palataan myöhemmin osiossa skenaariotyöskentely.

SATERISK-projektissa ja tässä työssä ei voida käyttää vain yhtä tiettyä analyysimenetelmää vaan on yhdistelty erilaisia lähestymistapoja. Tätä kvalitatiivisen tutkimuksen tapaa on luonnehdittu alun perin ranskankielisellä sanalla *bricolage*, tällä viitattiin alun perin käsityöläiseen, joka käyttää monenlaisia keinoja saadakseen työn tehtyä. *Bricolage* kuuluu konstruktivististen metodien perheeseen.

SATERISK on varsin laaja projekti ja siinä joudutaan tutkimaan varsin erityyppisiä asioita sähköisistä häiriöistä ihmisen käyttäytymiseen asti. Käytössä tulee olemaan monilla työpaketinvetäjillä ja tutkijoilla hyvinkin erilaisia työmenetelmiä. *Bricolage*, kokonaisuuden kokoaminen palasista, on vertauskuva sille, että tutkijalle ei tässä vaatimusmäärittelyssä määrätä ennakoon menetelmää jota soveltaa aineistoon, vaan tutkija ottaa SATERISK-työkalupakistaan erilaisista mahdollisista lähestymistavoista yhden tai useamman, ja valitsee sekä yhdistelee näistä sopivat, ehkä täysin omanlaisensa analyysitavat.

Tässä tutkimuksessa tulee olemaan käytössä suuri määrä erilaisia mittareita ja työkaluja. Tässä vaiheessa ei pyritäkään ottamaan kantaa siihen ovatko kaikki mittarit valideja, vaan ainoastaan siihen että tutkimuksen strategia on validi. Ei keskitytä menetelmiin, vaan siihen mitä tietoa halutaan ja valitaan sitten menetelmät sen mukaan. ( Anttila 2000, 202)

Tässä työssä käsitellään paljonkin tulevaisuudentutkimusta, mutta ei osana tätä raporttia, vaan eräänä vaatimuksena SATERISK-projektin seuraavan vaiheen toteutukselle.

Tässä vaatimusmäärittelyvaiheessa ei ole mahdollista määritellä kaikkia tulevassa tutkimuksessa käytettyjä metodeja kovin tarkasti, koska se rajaa muutoin liikaa työryhmien työskentelytapoja ja estää siten myös halutun triangulaation syntymistä.

Suurimpana ohjeena on skenaariotyöskentelyn valitseminen tulevaisuuden tutkimuksen tärkeimmäksi toteuttamistavaksi ja lista tärkeimmistä työkaluista. Tämäkin lähinnä siitä syystä, että mahdollistetaan työpakettien tulosten helpompi yhteensovittaminen. Tulevaisuudentutkimuksen metodeista ja työkaluista enemmän osiossa 10. SATERISK prosessi.

## 2.1 Empiirisen aineiston hyödyntäminen ja aineistolähtöinen analyysi

Riskejä ei voi lähteä etsimään pelkästään teoriaan tukeutuen, vaan riskienkartoitusta tehdään todellisissa ympäristöissä, siellä missä riskit oikeasti toteutuvat, jos toteutuvat. On pyrittävä monipuoliseen aineiston keräämiseen. Kun halutaan luoda uutta ei voida tukeutua vain olemassa olevaan teoriaan. Työpakettien riskikartoituksen yhteydessä tekemä materiaali on oltava kaikkien työpakettien yhteisessä käytössä jolloin samalla syntyy materiaali-triangulatiota. SATERISK-projektissa mahdollisesti syntyvää uutta teoriaa rakennetaan siis empiirisestä aineistosta lähtien alhaalta ylöspäin.



## 2.2 Triangulaatio

Triangulaatiolla pyritään kohottamaan tutkimuksen luotettavuutta. Saterisk projektissa kyseessä on riskien löytäminen. Jotta saavutettu riskikartoitus olisi riittävän täydellinen ja luotettava tulevaisuuteen suuntautuvan osion lähtökohdaksi, tulee tuloksia varmistaa triangulaation avulla. Triangulaation avulla osoitetaan, ettei jokin tulos ole pelkästään sattumanvarainen, vaan sama tulos on saavutettu useilla eri lähestymistavoilla. samaa tutkittavaa ilmiötä lähestytään monelta eri suunnalta, monimenetelmällisesti.

SATERISK-projektissa riskit ovat se juoni, joka on tutkimustehtävän kantava idea. Tämän tulee vaikuttaa menetelmien valintaan, riskienarvioinnissa mukana olevien henkilöiden valintaan sekä aineiston kokoamiseen. Tämä voi käytännön tasolla tarkoittaa sitä, että rahankuljetusten paikannuksen riskejä käsitellään erikseen itse kuljettajien ja erikseen työnjohdon kanssa. Tuloksia verrataan vasta myöhemmin keskenään ja saadaan näin kuvaa samasta asiasta eri katsantokannoilta. Käytännössä tämä johtaa siihen, että riskienkartoitus tehdään useaan kertaan siten, että käytettävä menetelmä ja jopa työskentelyyn osallistuvat henkilöt vaihtuvat.

SATERISK-projektissa samaa aihetta käsitellään myös eri aikaulottuvuuksilla ja tutkitaan esimerkiksi jonkin käyttömallin kehittymistä ja muuntumista aikaperspektiivillä. SATERISK on usean eri tutkijan yhteinen projekti, joissa kukin lähestyy aihetta eri suunnista. Tämä mahdollistaa sen, että samaan projektiin voidaan mahdollistaa monia eri lähestymistapoja. Tutkimuksella ei ole tarkoituksena löytää pelkkiä faktoja, vaan jos mahdollisuutta faktojen saavuttamiseen ei ole, keskitytään oikean suunnan löytämiseen. Löydettyjen riskien pohjalta voivat projektin osalliset tehdä jatkotutkimuksia, demonstraatioita ja testejä ja jopa prototyyppejä erilaisista laitteista tai käytäntöjä.

SATERISK-projektissa käytetään Denzin (1978) nelijakoista triangulaatiomallia : (Denz 1978)

1. Aineistotriangulaatio - useammanlaisia aineistoja (esim. haastattelu tai lehtiartikkeleita)
2. Tutkijatrigulaatio - kaksi tai useampia tutkija tutkijoita tutkii ilmiötä
3. Teoriatrigulaatio - tutkitaan aineistoa erilaisilla teorioilla
4. Menetelmätigulaatio - tutkimuskohdetta tutkitaan useilla aineistonhankinta- ja tutkimusmenetelmillä. Saterisk-projektissa ei pyritä keskittymään vain joihinkin lähteisiin, vaan kaikki mahdolliset lähteet tulee ottaa käyttöön, näin aineistotrigulaatio toteutuu. Projektissa toimitaan ryhmissä, ja usein samaa asiaa saatetaan tutkia eri kokoonpanoissa, joka muodostaa vahvan tutkijatrigulaation.

Teorian käyttöä ei ole rajattu mihinkään määrättyyn teoriaan. Monimenetelmällisyys tarkoittaa usein myös erilaisten teoreettisten selitysmallien tai useiden rinnakkain koottujen aineistojen käsittelyä rinnakkain. (Cohen & Manion 2002, 269-280)

Esimerkiksi paikannusta Venäjällä voidaan tarkastella lainsäädännön valossa, viranomaiskäytännön valossa tai yksityisen käyttäjän kokemusten perusteella. Aikaisempia muiden ryhmien löydöksiä ei anneta uudelle ryhmälle suoraan käyttöön, vaan pyritään puhtaalta pöydältä etenemään eri keinoin kohti valittua päämäärää ja katsotaan sitten onko saavutettu tulos samansuuntainen aikaisempien tulosten kanssa.

Jos tutkija voi osoittaa, että eri menetelmillä ja päästään samaan tulokseen tai että eri menetelmät tukevat samoja hypoteeseja, ne saavat vahvistusta ja triangulaation käytöllä on voitu vahvistaa tutkimuksen validiutta.

### 3 Käsitteiden määritelmät

Käsitteiden määritelmät otetaan tämän työn osaksi, koska niitä pyritään muokkaamaan ja kehittämään SATERISK-projektin jatkokäyttöön.

Seuraavat määritelmät ovat peräisin Tekniikan Sanastokeskus ry:n julkaisemasta Paikannus-sanastosta, ellei muuta ole erikseen merkitty. Sanat ovat käytettävyyden helpottamiseksi aakkosjärjestyksessä.

#### Ajoneuvon seuranta

Yksittäiseen ajoneuvoon kohdistuva seuranta.

Ajoneuvon seuranta voidaan käyttää esimerkiksi kuljetusten tehostamiseksi tai kalliiden merkiautojen seurantaan varkauksien ehkäisemiseksi.

#### EGNOS.

Lyhenne sanoista European Geostationary Navigation Overlay Service. GPS-järjestelmän paikannustarkkuutta Euroopassa parantava järjestely, jossa lasketaan GPS-satelliittien lähetteelle differentiaalikorjaukset useilla vertailuasemilla. Korjaukset ovat koko mantereen keskiarvoja – vertaa DGPS. EGNOS-satelliitti lähettää GPS:n satelliittikohtaiset korjaukset GPS-signaalina WAAS-yhteensopiville GPS-vastaanottimille.(Helsingin Navigaattorit)

GPS, global positioning system

Yhdysvaltain puolustusministeriön ylläpitämä ja hallinnoima maapallon kattava satelliittipaikannusjärjestelmä GPS tarjoaa erikseen siviili- ja sotilaskäyttöön koodatun paikannuspalvelun.

#### Hajontakuvio

Hajontakuviolla viitataan pistepilveen mikä syntyy, kun havaintoyksiköt sijoitetaan kahden muuttujan muodostamaan koordinaatistoon. Se antaa silmämääräisen käsityksen muuttujien välisen yhteyden voimakkuudesta ja muodosta. (tilastokeskus, käsiteluettelo)

#### Henkilön seuranta

Yksittäiseen henkilöön kohdistuva seuranta

Henkilön seurannan avulla voidaan esimerkiksi tarkkailla vanhuksen sijaintia ja terveydentilaa, tarkistaa avovankilan vangin sijainti tai etsiä kadonnutta henkilöä.

#### Hätäpaikannus

Hätälähettimen tai telepäätelaitteen paikannus, kun käyttäjän tiedetään tai epäillään olevan avun tarpeessa. Suomen lainsäädäntö sallii pelastusviranomaisille kadonneeksi ilmoitetun henkilön matkaviestimen paikannuksen.

#### Hätäpuhelupaikannus

Hätänumeroon yhteyden ottavan puhelimen hätäpaikannus.

Hätäkeskus voi saada teleyritykseltä soittajan puhelimen sijaintitiedon.

#### Isokroni

Samanaikajänkä, joka yhdistää kartografisessa esityksessä saman ajan saavia pisteitä. (Ihmäki, V-P.)

#### Katvealue

peittoalueen sisällä oleva alue, jossa yhteyden saanti tai ylläpito ei onnistu

Katvealueita voivat olla esimerkiksi junatunneli, kellari ja hissi.

#### Koordinaatisto

Vertausjärjestelmä, jossa pisteen sijainti ilmoitetaan mitattavina lukuina tai kulmina ennalta määrättyjen koordinaattiakselien tai nollatasojen suhteen

Suomalaisissa maastokartoissa käytetään kkj:n yhtenäis- ja peruskoordinaatistoja, jotka perustuvat Gauss-Krügerin projektioon ja projektiokaistojen mukaisiin keskimeridiaaneihin. WGS 84 sisältää ns.

maantieteellisen koordinaatiston (ellipsoidikoordinaatiston).

Koordinaatit pl; koordinaattitieto

Sijainnin ilmaisevat koordinaattilukuarvot ja niiden yksikkö sekä tiedot käytetystä koordinaattijärjestelmästä ja koordinaatistosta. Koordinaatit ilmaistaan paikannuslaitteissa usein WGS 84 -järjestelmässä maantieteellisinä pituus- ja leveysasteina, esimerkiksi 60° 00' 00" (60 astetta, 0 minuuttia, 0 sekuntia) pohjoista leveyttä (latitudi), 27° 00' 00" itäistä pituutta (longitudi). Julkaistuissa kartoissa käytetään usein paikallisia koordinaatistoja; suomalaisissa maastokartoissa käytetään kartastokoordinaattijärjestelmän (kkj).

Paikannus; paikanmääritys; sijainnin määrittäminen

Kohteen sijainnin määrittäminen vertausjärjestelmässä.

Kohteen sijainti voidaan määrittellä muun muassa koordinaatti- tai osoitejärjestelmässä, aluejaossa, matkaviestinverkon solukkojärjestelmässä tai valitun reitin tai tunnettujen kohteiden suhteen

Paikannuttaja: paikannuksen pyytäjä;

osapuoli, joka tilaa paikannettavaa koskevan sijaintitiedon (1)

Esimerkiksi työnantaja voi sopia huoltotyöntekijöidensä matkaviestimien paikantamisesta työajalla. Tällöin työnantaja on paikannuksen pyytäjä ja työntekijä paikannettava.

paikannusluvan antaja

osapuoli, joka on antanut luvan paikannukseen ja sijaintitiedon välitykseen

paikannettava

paikannuslaitteen tai paikannettavan laitteen käyttäjä tai kantaja, jonka sijaintitieto (1) halutaan saada selville. Paikannettava voi olla ihmisen lisäksi esimerkiksi ajoneuvo tai kotieläin, jos siihen on kiinnitetty paikannuslaite tai paikannettava laite.

### Paikkatieto

Paikannettua kohdetta kuvaavan sijaintitiedon ja kohteen ominaisuuksia kuvaavien tietojen muodostama kokonaisuus. Kohteiden ominaisuuksia ovat muun muassa tunnisteen, mittaushavainnot, luokitukset ja kuvailut.

Paikkatieto voi kertoa esimerkiksi tietyn rakennuksen sijainnin lisäksi sen, että rakennus on punainen ja kolmikerroksinen.

Yleiskielessä paikkatieto-sanaa käytetään joskus, kun tarkoitetaan sijaintitietoa.

### Paikkatietojärjestelmä; GIS

(Geographic information system; GIS)

Tietojärjestelmä, joka käsittelee paikkatietoa ja tukee erityisesti sijaintitiedon käsittelyä ja hallintaa. Paikkatietojärjestelmä tukee sijaintiin perustuvaa indeksointia, hakuja, analyysejä ja visualisointia.

### Reitinoptimointi

reitinmäärittäminen, jossa lasketaan tiettyjen ehtojen mukainen, sopivin reitti

### Seuranta

Paikannukseen perustuva, määrävälein toistuva tai muilla perustein tapahtuva kohteen mahdollisimman ajantasainen sijaintitiedon välitys sekä kohteen mahdollinen tarkkailu. Esimerkiksi ajoneuvon seuranta on yleistä kuljetusten tehostamiseksi. Seurannan avulla pystytään myös löytämään nopeasti lähin vapaa yksikkö, jos apua tarvitaan.

### Sijaintitiedon luovutus; paikannustiedon luovutus

Sijaintitiedon siirtäminen osapuolelta toiselle. Sijaintitiedon luovutuksen tulee perustua sopimukseen tai lakiin. Esimerkiksi teleyritys voi luovuttaa asiakkaansa sijaintitiedon lisäarvo-palvelun tuottajalle, jos asiakas on antanut tähän suostumuksensa, tai pelastusviranomaisille lain nojalla.

Sijaintitiedon välitys; paikannustiedon välitys

Sijaintitiedon tekninen siirtäminen tietojärjestelmien välillä

Sijaintitiedon välitys voi tapahtua paikannusjärjestelmästä tietoa hyödyntävälle sovellukselle.

Sijaintitieto; paikannustieto

Vertausjärjestelmässä ilmaistu kohteen sijainti. Sijaintitieto voidaan ilmoittaa esimerkiksi koordinaatein, kertoa osoitteen avulla tai viittaamalla kohteeseen, jonka koordinaatit tunnetaan. Tällaisia kohteita ovat esimerkiksi paikannimet ja erilaisten alueiden nimet. Sijaintitieto voi kertoa esimerkiksi tietyn rakennuksen sijainnin koordinaattien tai osoitteen avulla, vrt. paikkatieto.

Solu

Samaa maantieteellistä aluetta palvelevan, tiettyyn tukiasemaan kuuluvan lähetin-vastaanottimen peittoalue. Solun muoto määräytyy antennin suuntakuvion ja ympäröivän maaston perusteella. Sen kokoon vaikuttavat muun muassa lähettimen teho ja taajuusalue. Soluja voidaan nimetä muun muassa koon mukaan, esimerkiksi pikosolu, mikrosolu ja makrosolu. Suunta-antennilla muodostettua solua voidaan kutsua sektoriksi.

Solupaikannus

Matkaviestinverkon solutunnusten avulla tapahtuva verkkopaikannus.

Solupaikannuksen tarkkuus vaihtelee solujen koon mukaan, ja sitä voidaan parantaa käyttämällä esimerkiksi ajastusennakko (timing advance, A) ja signaalitasotietoja (Rx-level). Cell ID ja CI ovat lyhenteitä englannin termistä "cell identity", joka on suomeksi solutunnus.

Verkkopaikannus

Matkaviestinverkon avulla tapahtuva paikannus. Verkkopaikannuksessa tieto kytkentätilassa olevan matkaviestimen sijainnista on matkaviestinjärjestelmässä

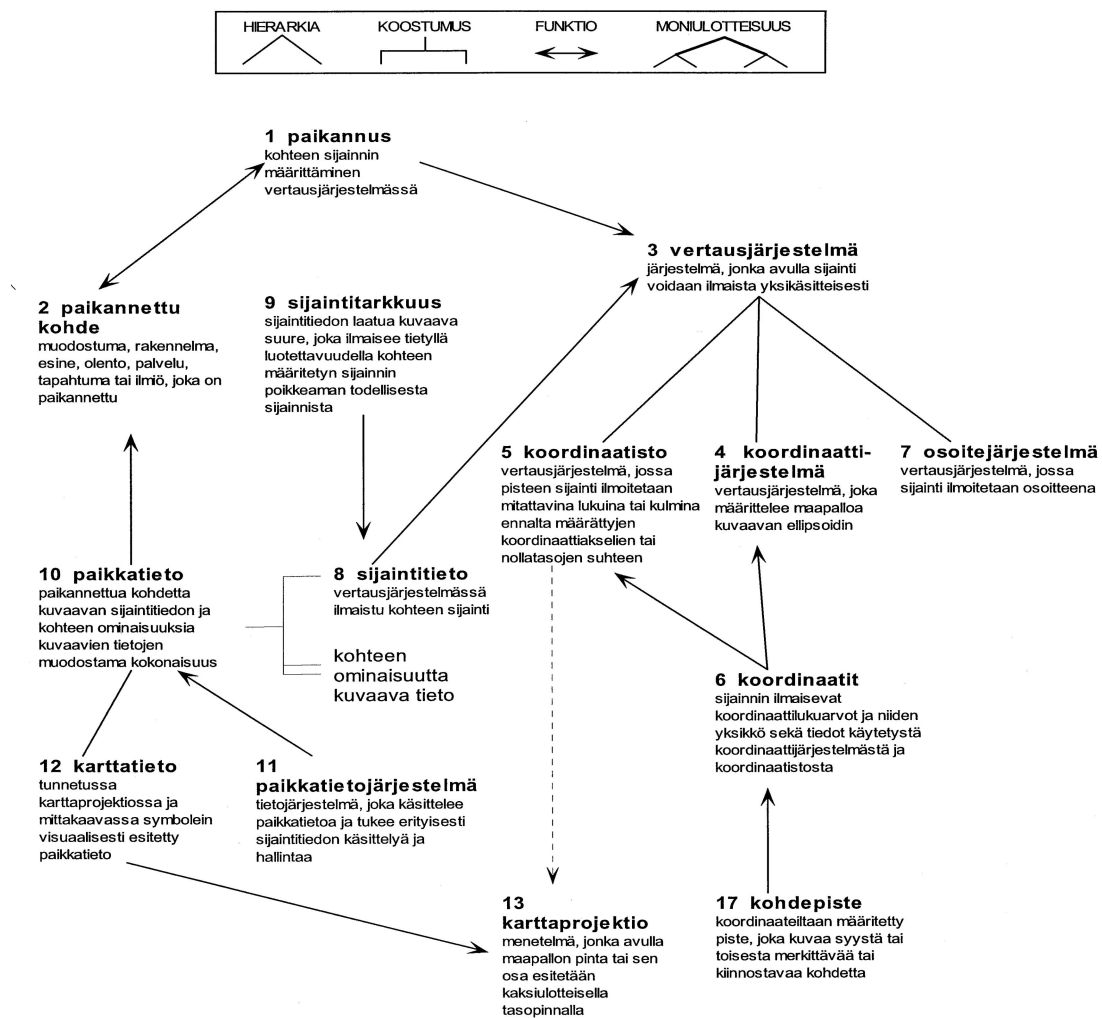
Vertausjärjestelmä

Järjestelmä, jonka avulla sijainti voidaan ilmaista yksikäsitteisesti.

Vertausjärjestelmiä ovat muun muassa koordinaatti- ja osoitejärjestelmät, koordinaatistot, erilaiset aluejaot sekä reitistöt.

## WAAS

Lyhenne sanoista Wide Area Augmentation Service. WAAS-satelliitti lähettää GPS:n satelliittitikohtaiset korjaukset GPS-signaalina WAAS-yhteensopiville GPS-vastaanottimille.. GPS-järjelmien vaatimukset requirements analysisn analyysistelmän paikannustarkkuutta Amerikan mantereella parantava järjestely, jossa lasketaan GPS-satelliittien läheteelle mannerkohtaiset differentiaalikorjaukset useilla maa-aseilla. (Helsingin navigaattorit)



KUVIO 2. Paikannuksen yleiskäsitteet (Tekniikan sanastokeskus 2002)

## 4 Vaatimusmäärittely

Vaatimusmäärittely on ensimmäinen työvaihe uuden järjestelmän tekemisessä tai vanhaa korjatessa. Vaatimusmäärittely asettaa tavoitteen toivotusta lopputuloksesta. Todellisuutta on myös se, että kehitys-projektissa on useita eri tahoja, jotka ovat tottuneet määrittelemään tavoitteet ja riskit eri tavoilla.

Kunnolla tehty vaatimusmäärittely helpottaa projektin kustannusten ja saavutettavien hyötyjen arviointia. Vaatimusmäärittelyn ensimmäisessä vaiheessa kuvataan myös sellaisia ominaisuuksia, joita ei tulla jatkossa toteuttamaan. Tämän ensimmäisen vaiheen jälkeen määritellään ne rajat joissa järjestelmän tulee toimia.

Wiegiers (2003, SIVU PERKELE!!!) kertoo kirjassaan vaatimusmäärittelylle mm seuraavia etuja

- vähentää vaatimusvirheitä.
- Vähentää uudelleenkehittelyä
- vähentää tarpeettomia ominaisuuksia
- vähentää parantamiskustannuksia
- Vähentää väärinymmärrystä
- vähentää laajuusongelmia
- vähentää kaaosta
- helpottaa testausta
- lisää tekijöiden tyytyväisyyttä
- nopeuttaa toimitusta

Wiegierssin esimerkit ovat alun perin ohjelmistokehitykseen, mutta tukevat hyvin myös tämän työn tavoitteita.

### 4.1 Vaatimusmäärittely tarkistaminen

Vaatimusmäärittelyä on syytä pyrkiä käymään läpi ja tarkentamaan useaan kertaan projektin kestäessä, koska on mahdollista että jotkut havainnot vaativat tarkempaa selvitystä. Suurempia vaatimusmäärittelyyn liittyviä askeleita on kolme kappaletta.

- 1) Tämä ensimmäinen vaatimusmäärittely
- 2) Nykyhetken riskikartoituksen jälkeinen vaatimusmäärittelyn tarkistus
- 3) Tulevaisuus-skenaarioiden yhdistämisen jälkeen pidettävä vaatimusmäärittelyn tarkistus



Vaatimusmäärittelyjä voidaan muuttaa muutenkin kun saadaan uutta, katsontakantaa muuttavaa tutkimustietoa. Hyvin tehty vaatimusmäärittely varmistaa kuitenkin sen, että kulloiseltakin tietopohjalta tehdään oikeita suuntauksia, ja kehityksen myöhemmässä vaiheessa säätytään isoilta muutoksilta. Vaatimusmäärittelyn muutokset on kuitenkin aina hyväksyttävä projektin johtoryhmällä.

Tässä vaatimusmäärittelyssä ei esitetä vaatimuksia työn jakamiseksi esimerkiksi teknologiaan, lainsäädäntöön tai käyttöön. Tämä jako on tarkoituksellisesti tehty jo tutkimussuunnitelman työpakettijaon yhteydessä. Tarkoituksena on että työpaketit keskittyvät omaan osaalueeseensa esim. tekniikkaan, mutta voivat raportoida myös havaitsemiaan riskejä esimerkiksi lainsäädännössä. Nimenomaisesti on pyritty madaltamaan rajoja jolloin osa-alueet menevät hieman limittäin ja aukkoja jää mahdollisimman vähän.

#### 4.2 Tärkeimmät vaatimukset

Tässä vaatimusmäärittelyssä on pelkkien vaatimusten esittämisen lisäksi käyty joiltain osin varsin laajasti läpi myös vaatimusten taustoja. Tällä on tarkoituksena edistää sitä, että varsinaista riskiarviointityötä tekevät voisivat suunnata riittävästi huomiota näille osa-alueille. Työpakettien vastuuhenkilöiksi tulee valita sellaiset henkilöt, joilla on syvällistä tietoa kyseiseltä tutkimusalueelta. Osaamisen ei tarvitse olla kattavaa kunhan se on asiantuntijatasolla jollain osa alueella. Ryhmät tulee koota niin, ettei osaamiseen jää aukkoja jotka voisivat aiheuttaa riskikartoitukseen aukkoja. Vastuuhenkilöllä tulee olla riittävästi aikaa tutkimuksen tekemiseen, koska on tärkeää, että hän osallistuu kaikkiin projektin vaiheisiin.

Määrittely on jaettu kolmeen osaan:

- |        |        |                                      |
|--------|--------|--------------------------------------|
| OSA 1. | luku 4 | kuvataan käytettävä riskikäsitys.    |
| OSA 2. | luku 5 | kuvataan varsinaiset vaatimukset     |
| OSA 3. | luku 6 | kuvataan työssä käytettävät työkalut |

#### 4.3 Riskin määritelmä

Kaikkeen olemiseen ja toimintaan liittyy aina riskejä. Yleisesti ottaen kaikki riskin määritelmät muistuttavat läheisesti toisiaan, useissa painotetaan pelkästään vahingon tai epätoivotun tapahtuman mahdollisuutta, esim. Vaughan (1997, 8) määrittelee riskin olosuhteeksi, jossa tapahtuman lopputulos poikkeaa toivotusta tai odotetusta lopputuloksesta. Riski on siis vahingon mahdollisuus. Lähes kaikki riskit ovat alun perin ihmisten toiminnan aiheuttamia ja siksi niihin voidaan myös vaikuttaa ja varautua ja niiltä voidaan yleensä myös suojautua.

Liiketoiminnan yhteydessä riskin katsotaan sisältävän uhkien lisäksi myös mahdollisuuksia. Esimerkiksi Venture Capitalist-liiketoiminta on riskihakuista.

Riskejä arvioitaessa näkemys riskistä muuttuu, kun arvioijan tietotaso muuttuu. Sateriskissa on kysymys juuri siitä että saadaan kokoon riittävän suuri asiantuntijaryhmä paikannusketjun eri osa-alueilta jotta pystytään luotettavaan riskikartoitukseen. Yksittäisen toimijan on erittäin vaikea saavuttaa riittävä asiantuntemus koko osaamisalueelta. Asiantuntijat näkevätkin riskit usein todennäköisyyksinä ja riskien hahmotteluina (Kamppinen ym. 1995, 51)

Riskin käsitettä kuvaa seuraava kaavava (kamppinen ym. 1995, 15)

Riski (R) = Todennäköisyys ( P ) x Haitta (H)

Riskejä voidaan tarkastella esimerkiksi seuraavan juoksutuksen mukaan:

- riskien löytäminen
- riskien identifiointi
- riskin eristäminen
- riskikartan laatiminen
- priorisointi
- riskien lähteet ja draiverit
- riskien perussyt
- riskien seuranta
- raportointi

#### 4.3.1 SATERISK-projektissa riski ei sisällä mahdollisuutta

SATERISK-projektin ensimmäisessä vaiheessa riskejä tarkastellaan vain niiden aiheuttamien uhkien kautta. Beck (2006, 4) käyttää riskiyhteiskunnasta puhuessaan samaan tapaan riskikäsitettä, joka käsittelee riskejä ehdottoman negatiivisina asioina, siis haittoina.

Tulevaisuus-skenaarioiden yhteydessä käsitellään sekä riskejä uhkamerkityksessä, että myös tulevaisuuden mahdollisuuksia. Molempien kartoitus voi tapahtua samassa tilanteessa ja niiden keskinäinen yhteys pitää säilyttää, mutta molemmista tulee laatia myös erillinen listaus.

#### 4.3.2 Mahdollisuudet

SATERISK tähtää uusiin innovaatioihin, tulevaisuuden laitteisiin, tuotteisiin ja palveluihin. Kaikkia ilmeneviä mahdollisuuksia tulee tarkastella ja arvioida ovatko ne hyödynnettävissä.

Mahdollisuudet tulee käsitellä yhdessä riskien kanssa, mutta ne tulee raportoida erikseen, eikä sisällyttää riskeihin, niin kuin liiketoimintariskejä tarkastellessa joskus menetellään.

Suomen menestys on paljolti perustunut laadukkaaseen koulutusjärjestelmään, yritysten ja julkisen sektorin pitkäjänteisiin panostuksiin tutkimus- ja kehitystoimintaan sekä hyvin toimi-  
viin, verkostoituneisiin instituutioihin. Kilpailu innovaatiotoiminnan avoimessa maailmanlaa-  
juisessa toimintaympäristössä on nopeasti kiristymässä ja suhteelliset kilpailuetumme tulevat  
haastetuiksi. Suomen menestys kansainvälisissä kilpailukykyä ja tietoyhteiskuntakehitystä  
arvioivissa vertailuissa onkin viime vuosina ollut laskeva. (TEM. 2008, 6-8) Suunnan kääntämi-  
seksi tässä projektissa kaikki innovaatiot, joilla katsotaan olevan hyödyntämispotentiaalia,  
kirjataan ja viedään prosessin seuraavaan vaiheeseen.

#### 4.3.3 Muutos riskiyhteiskunnan suuntaan otettava huomioon

Elämme ympäristössä, jossa riskit lisääntyvät koko ajan. Alkuaan ihmisen riskit liittyivät lä-  
hinnä hengissä selviämiseen. Teknologian kehittyminen ja varallisuuden lisääntyminen on  
myöhemmin luonnut paljon uusia riskejä: Toimiiko teknologia kuten pitää, vai tuottaako se  
uusia riskejä? Onko omaisuus, niin materiaallinen kuin aineetonkin turvassa? Nykyaikainen  
yhteiskunta tuottaa niin paljon uusia riskejä, että ne eivät enää tahdo pystyä tunnistamaan ja  
sitä on vaikea pitää hallinnassa. Tiedostettujen riskien lisäksi on tiedostamattomien  
epävarmuuksien vyöhykkeitä.

SATERISK-projektissa tutkimme riskejä joiden vaikutuskanavat ovat hyvin monimutkaisia ja  
kietoutuneita yhteiskunnan erilaisiin prosesseihin ja palveluihin. Yksi selkeä ydin tutkimus-  
kohde on se mitä riskejä tuotamme yrittäessämme poistaa riskejä.

Saksalainen sosiologi ja yhteiskuntatieteilijä Ulrich Beck on lanseerannut termin Riskiyhteis-  
kunta. Beckin määritelmän mukaan riskillä tarkoitetaan systemaattista tapaa käsitellä yhteis-  
kunnan aiheuttamia vaaroja ja epävarmuuksia. olemme siirtyneet teollistuneesta yhteiskun-  
nasta eteenpäin ja tässä uudessa yhteiskunnassa vaikuttavat erilaiset lainalaisuudet, kuin  
teollisuusyhteiskunnassa. Beckin mukaan riskiyhteiskunta syntyy, kun erilaiset sosiaaliset,  
poliittiset, taloudelliset ja yksilölliset riskit karkaavat perinteisten turvainstituutioiden kont-  
rollista. Tälle yhteiskunnalle, jossa vasta opettelemme elämään, on keskeistä erilaisten riski-  
en muodostaminen ja niiden jakaminen. ( Beck.1992, 21 ).

Esimerkiksi paikannuksen käytössä voisi olla esimerkkinä rahankuljetusyhtiö, joka ostaa kulje-  
tusten paikannuksen ulkopuoliselta yritykseltä. Paikannuksen tuottaja tekee sen mahdoli-  
simman halvalla, ei huolehdi viestiliikenteen riittävästä salauksesta ja mahdollistaa näin ra-  
hankuljetuksen sijaintitiedon valumisen rikollisten saataville. Paikannusyrittäjä tekee enem-

män voittoa, mutta aiheuttaa samalla rahankuljetusyritykselle uusia riskejä, joista tämä ei välttämättä ole lainkaan tietoinen.

## 5 Kohteellisuus vaatimukset

SATERISK-kohdealuevaatimukset määritellään hyvin väljästi ja ne on esitetty jo projektisuunnitelmassa, eli logistiikan ja turva-alan paikannukset erilaiset sovellutukset. Uhkien torjunnassa ei pidä keskittyä vain tekniikkaan. Ihmisten rooli on turvallisuudessa erityisen tärkeä. Toimintatapojen turvallisuutta voidaan vahvistaa kouluttamalla henkilöstö paikannustiedon oikeaan käsittelyyn. Turvallisuustietoisuuden lisääminen kaikissa henkilöstöryhmissä on tärkeä tapa torjua laitonta tiedonkeruuta. Mikäli ilmiöitä ja niiden toteuttamistapoja ei tunneta, on niiden torjuminen erittäin vaikeaa.

Kansainvälisen yhteistyön mahdollisuuksia on samoin kehitettävä. Sisäasiainministeriön yrityksiin kohdistuvan rikollisuuden tilannekuvaraportissa (2006, 24) korostetaan, että lainsäädännön tasolla on huolehdittava riittävästä toiminta- ja tiedonvaihtokeinoista sekä valvonnasta myös rajat ylittävissä tilanteissa. Sekä viranomaisten että mahdollisuuksien mukaan myös yrityssektorin on pyrittävä hyödyntämään ulkomaisia ja kansainvälisiä kokemuksia rikoksentorjunnasta ja tiedonkeruusta.

### 5.1 Tutkimuksen perspektiivi on paikannuttajan näkökulma

Yksi tutkimuksen luotettavuuden tärkeimmistä kriteereistä on keskeinen kysymys siitä mikä on "totuus" ja kenen totuus se on. Jo pelkästään työpaikoilla voi todeta, että työnantajan ja palkansaajan "totuus" voi olla hyvinkin erilainen. Sama maailma näyttää eri näkökulmista hyvinkin erilaiselta, ongelma on se että ympäristö ei pidä välttämättä meidän totuuttamme yleisenä totuutena. Tätä subjektiivisuuden-objektiivisuuden rajanveto on aina ollut empiirisen tutkimuksen peruskysymyksiä. Tämän rajanvedon helpottamiseksi on saterisk projektissa valittu hyvin selkeästi paikannuttajan näkökulma. Vaihtelua jää vieläkin kun asiaa tarkastellaan yksityisen ja julkisen sektorin näkövinkkeleistä, mutta se on kuitenkin huomattavasti pienempi kuin ilman tätä rajausta.

Paikannuttajan näkökulman valitseminen vaikuttaa erityisesti siihen, millainen riskikäsityksensä muodostuu. Kulloinenkin riskikäsitys liittyy kiinteästi siihen mitä ihmiset pitävät ei-toivottuna tapahtumana. Arvokuljetus ryöstöä suunnittelevan riskit pienentyvät kun hän tietää mistä kuljetuksen löytää, vastaavasti samaan aikaan kuljetusyhtiön riskit, siis todennäköisen paikannuttajan riskit, kasvavat ainakin vastaavasti, todennäköisesti vieläpä moninkertaisesti. Ero riskeissä johtuu siitä kuinka paljon eri osapuolilla on voitettavaa tai hävittävää.

Perspektiivin rajaaminen paikannuttajan näkökulmaan ei kuitenkaan välttämättä tarkoita sitä, että muita näkökulmia voidaan jättää kokonaan huomiotta. On varmaa että myös paikannettavan henkilön asemaan ja yksityisyydensuojaan liittyviä asioita joudutaan tutkimaan, mutta koska näihin kohdistuvat riskit lopulta kumuloituvat paikannuttajan riskeiksi. Samoin yhteiskuntavastuu, jota käsitellään myöhemmin, on yksi keskeinen vaatimus ja yksityisyydensuoja tulee esille sielläkin. Päänäkökulmana säilytetään silti koko ajan paikannuttajan näkökulmana.

## 5.2 Venäjä otettava huomioon

Suomen lähialueista erityisesti venäjä ja sen tulevaisuus luo paljon riskejä ja myös mahdollisuuksia. Venäjälle suuntautuvilla kuljetuksilla on erittäin suuri merkitys koko suomen logistiikkatoimijoille ja sitä kautta myös turvallisuusalalle. Venäjän kuljetukset olivat taantumaan asti yksi Suomen kasvualoista. Vuonna 2006 Suomen kautta Venäjälle tuodun tavarahan arvo oli yhteensä 30,9 miljardia euroa, joka oli noin 30 % Venäjän koko tuonnista ja viisinkertainen Suomen omaan Venäjälle suuntautuvaan vientiin verrattuna (Märkälä, M, ym. 2007, 1).

Volyymien odotetaan taas laman jälkeen lähtevän kasvuun, mikä luo yhä uusia kehittämissaasteita. Venäjän talouden kehitys johtaa vähitellen myös sen viennin kehittymiseen, raaka-aineita aletaan jalostaa pidemmälle ja Venäjän teollisuuden arvokkaimpien tuotteiden vienti näkyy liikennevirtana Suomessa.

Suomi on maantieteellisen asemansa vuoksi keskeinen alue erityisesti Venäjän ja EU:n välisessä tavaraliikenteessä. Venäjän vienti- ja tuontitoiminta on Suomessa yhä enemmän määrin pienten venäläistaustaisten huolintayhtiöiden hallussa. Keskusrikospoliisin raportin mukaan (2008, 22) Järjestäytyneiden rikollisten omistamien tai vaikutusvallan piiriin kuuluvien rahtiyritysten arvioidaan hoitavan huomattavan osan EU:n ja Venäjän välisestä rahtiliikenteestä. Suomen etu on lisäarvopalveluissa, luotettavuudessa, turvallisuudessa, ja selvityksen perusteella Suomen satamien kautta kulkeva reitti säilyttäneen asemansa arvotavarahan kuljetusreitteinä myös tulevaisuudessa. (Ruutikainen ym. 2006, 31)

Suomen vienti Venäjälle oli vuonna 2006 hieman yli 6,2 mrd. euroa. Venäjä oli Suomen toiseksi tärkein vientimaa 10,1 %:n osuudella Suomen koko viennistä. Venäjälle suuntautuneesta viennistä arviolta 30 % oli muualla tuotettujen tavaroiden jälleenvientiä (Tullihallitus. 2008)

Tullihallituksen (2008) tilastojen mukaan Suomen Venäjän-viennistä vuonna 2006 noin 30 % koostui jälleenviennistä. Tämä jälleenvienti on suurten kaupan alan yritysten hoitamaa. Tyyppilliset jälleenvientituotteet, kuten henkilöautot, kodinkoneet ja tietotekniikka, muodosta-

vatkin pääosan kaupan alan yritysten viennistä Venäjälle. Teollisuustoimialojen tuotteista koneiden, laitteiden ja kuljetusvälineiden osuus on noussut huomattavasti. Venäjälle vienti kohdistuu siis verrattain usein varsin suurista ja arvokkaista tuotteista.

SATERISK- projektissa Venäjän oikeus tulee ottaa monellakin tasolla huomioon monesta eri näkökulmasta. Kansainvälisen oikeuden alalla yksi tärkeimpiä venäläisiä tutkimuslaitoksia on Kansojen ystävyysyliopisto Moskovassa, jonka kanssa Lapin yliopiston OTK:lla on yhteistyösopimus. Avaruusoikeuteen erikoistuneen professorin G.P. Zkukovin arvio kansainvälisen avaruusoikeuden kehitystendensseistä 1990- ja 2000 luvuilla saattaa olla hyvinkin relevantti hankkeen kannalta. Zkukovin mukaan kansainvälinen avaruusoikeus etenee kansallisen lainsäädännön tasolla, mutta ei niinkään kansainvälisen oikeuden tasolla, eikä esim. YK:n avaruussopimus v.1967 ole viime vuosina saanut riittävästi huomiota osakseen.

Venäjän erityispiirre on se että lainsäädännön, viranomaistoiminnan ja yritystoiminnan keskinäinen yhteys ei ole samalla tasolla kuin useissa muissa maissa, eli käytännön toiminta ja lainsäädäntö saattavat erota toisistaan normaalia enemmän.

Venäjän lehdistössä on ollut kirjoitus, josta ilmenee että Venäjän viranomaiset eivät voi sulkea pois GPS:n kieltämistä venäjän julkisissa kuljetuksissa. ( RIA Novosti. [www.divi.ru](http://www.divi.ru) ). Venäjä on pitkän tauon jälkeen saamassa omaa kansallista paikannusjärjestelmänsä ( GLONASS) toimintakuntoon. Venäjällä Glonass on aiemmin ollut lähinnä viranomaiskäytössä. On ollut tiedossa jo pitkään että sitä voidaan tulevaisuudessa käyttää myös siviilipuolella, mutta tämä lehtiartikkeli antaa merkkejä siitä että samalla myös protektionismi nostaa päätään. Toki on valion turvallisuudelle myös merkittävä asia, jos logistiikka perustuu vaikkapa vain osittain järjestelmään, jonka päällä oloa joku toinen valtio säännöstelee. Tämähän on sama asia miksi EU aloitti Galileo-projektin. Euroopassa tosin ei ainakaan vielä ole merkkejä tällaisesta protektionismista.

Venäjällä on myös paljon muita erilaista vahvistamatonta tietoa paikannukseen liittyen. Välillä puhutaan paikannuslisenkseistä, maan rajan yli lähetettävän paikannustiedon maksimitarkkuudesta. Tämänkaltaiset asiat ovat tärkeitä kokonaisuuden kannalta.

### 5.3 Käyttäjävaatimukset

Yleensä vaatimusmäärittelyssä käyttäjävaatimukset kuvaavat ne tehtävät, jotka käyttäjien tulee olla mahdollista suorittaa järjestelmän avulla. Käyttäjävaatimusten dokumentoimiseen käytetään usein esimerkki käyttötapauksia. SATERISK-projektissa emme alkuvaiheessa voi suoraan tehdä työkaluja käyttötapauksiin, vaan ensin meidän on etsittävä yhdessä asiantuntijoiden kanssa näiden käyttötapauksien sisältämät, ehkä vielä suurelta osalta tunnistamattomat

riskit. Nämä löydetty riskit yhdessä käyttötapausten ja muun tiedon tulevaisuuden käyttöympäristöstä kanssa muodostavat pohjan, josta voidaan päästä rakentamaan uusia ratkaisuja.

Suunnittelun alkuvaiheessa on saatava riittävästi tietoa loppukäyttäjien todellisesta käyttäytymisestä ja paikannuksen käyttötavoista, jotta voidaan estää se, että suunnataan kehitys epäoleelliseen ja kehitetään käyttäjien tarpeita vastaamattomia uusia tuotteita. Tässä projektissa tarve ei ole enää välttämättä ole mikään yksittäinen laite vaan siihen liittyvät olennaisesti erilaiset tulevaisuudessa kehitettävät lisäarvopalvelut.

Käyttötapausten kuvaamat toiminnalliset vaatimukset määrittävät sen, mitä kehittäjien tulee järjestelmään rakentaa, jotta käyttäjät voivat suorittaa järjestelmällä niitä tehtäviä, jotka käyttötapausten on määritellyt. Lopullinen vaatimusmäärittely koostuu toiminnallisten vaatimusten lisäksi ei-toiminnallisista vaatimuksista, kuten laatutekijöistä, rajoitteista ja muista ei-toiminnallisista vaatimuksista.

Käyttäjä on vaatimuksia tehtäessä määriteltävä varsin väljästi. Paikannusta käytetään varsin paljon yhteiskunnalle tärkeiden toimintojen turvaamiseen. Yhteiskunnan kokonaisuus on siis otettava huomioon.

#### 5.4 Reaaliaikaisuusvaatimus

Reaaliaikaisuudella tarkoitetaan tässä työssä sitä, että tapahtumiin voidaan reagoida lähes välittömästi. Nopeus reagoida lisää aina tuntuvasti myös käytettävyyttä. Turvallisuuslalla on selkeästi määritellyt, että tarkoituksena on ennaltaehkäistä ei-toivottuja tapahtumia. Rikollisuuden kansainvälistymisen ja ammattimaisuuden seurauksena yritysten riski joutua rikosten kohteeksi on kasvanut. Rikosriskejä voidaan hallita ennaltaehkäisevän kartoituksen ja toimintasuunnitelman avulla. Elinkeinoelämän Keskusliiton mukaan rikosten ennaltaehkäisy on aina kannattavampaa kuin jo tapahtuneiden vahinkojen selvitys.

Turvallisuuslalla rikostutkintaa tekevät vain viranomaiset, eli poliisi, tulli ja rajavartiolaitos. Yksityisen turvallisuusalan tehtävänä on toki edistää rikostutkintaa, mutta sillä ei ole mitään varsinaista osuutta tutkinnan suorittamisessa.

SATERISK-projektissa paikannusta tarkastellaan lähes reaaliaikaisen tiedon tuottamisena ja sen tuottaman tiedon hyödyntämistä operatiivisen toiminnan tehokkuuden parantamiseen ja ei-toivottujen tapahtumien estämiseen. On siis tarkasteltava tiedon oikeellisuuden lisäksi sitä, että paikannustieto pystytään välittämään kaikille toimijoille läpi koko ketjun niin nopeasti, ja että sillä pystytään vaikuttamaan tapahtumien lopputulokseen. Se että paikkatiedolla pystytään selvittämään tapahtumien ja prosessien kulkua ja mahdollisesti edistämään tutkintaa

on vasta toissijainen tavoite. Tätä reaaliaikaisuusvaatimusta tarkastellaan vielä tarkemmin osiossa tarve reaaliaikaisille GIS-järjestelmille.

## 5.5 Yhteiskuntavastuu

Huolimatta siitä, että perspektiivi on paikannuttajan perspektiivi, on kuitenkin koko ajan pidettävä mielessä yhteiskunnan etu syvemmällä tasolla kuin siten, että täytetään vain ajastaan jäljessä olevan lainsäädännön minimivaatimukset. Tässä työssä katsomme pitkälle tulevaisuuteen, jolloin myös lainsäädäntö tulee muuttumaan. Näitä muutoksia ollaan osittain tällä työllä saattamassa liikkeelle, jolloin on myös selvää, että niiden aiheuttamia muutoksia pitää pystyä myös ennakoimaan. Ei ole tarkoituksenmukaista luoda sellaisia järjestelmiä, jotka palvelevat vain paikantajan etuja, koska yhteiskunta on kuitenkin kaikkia ihmisiä varten ja yhteiskunnan tekemä lainsäädäntö tulee kuitenkin jollain viiveellä kuitenkin poistamaan liian tiukat toimenpiteet. Turvallisuuden vuoksi on joskus mahdollista heikentää yksilönsuojaa, mutta prosessin pitää olla läpinäkyvä ja muutosten suhteen hyväksyttävä.

SATERISK-projektissa tarkastelemme sellaista teknologiaa, jota voidaan hyvinkin helposti käyttää myös vallan välineenä. On turha kuvitella, että paikannusteknologiaa käytettäisiin aina oikein ja yhteiskunnallisesti hyväksyttävin perusteluin. Yhteiskunnassa on paljon erilaisia intressiryhmiä, jotka tarkastelevat asiaa lähinnä omasta katselukulmastaan. Tässä tutkimuksessa tarkastelukulmaksi on valittu nimenomaan paikannuttajan näkökulma. Projektin rahoittajat ja osanottajat ovat nimenomaan niitä tahoja jotka käyttävät paikannusta ja tulevat myös hyödyntämään tutkimuksessa saavutettavia tuloksia.

Laajempi yhteiskunnallinen näkökulma on kuitenkin kaikissa vaiheissa pidettävä mukana. Olemme tekemässä uutta osaamista koko yhteiskunnan hyväksi. Heiskanen ja kumppanit (25) määrittelevät teoksessaan eettinen johtaminen asian seuraavasti: ”eettinen johtajuus mahdollistaa edelläkävijyyden, jolloin organisaation toiminnan eettisyydestä tulee kilpailuetu, jonka avulla erotutaan muista alan toimijoista. Organisaatio kehittää jatkuvasti toimintamalliansa eettisyyttä ja hyödyntää niitä aktiivisesti toiminnanohjauksessa, viestinnässä ja yhteistyösuhteissa”.

EK:n (2001) mukaan yhteiskuntavastuu tarkoittaa osallistumista yhteiskunnan hyvinvoinnin tuottamiseen sekä vastuullisuutta suhteessa ympäristöön ja sidosryhmiin. Yhteiskuntavastuu koostuu EK:n taloudellisesta osasta, ympäristöosasta ja sosiaalisesta osasta. Näihin kuuluvat taloudellisen hyvinvoinnin tuottaminen, ympäristönsuojelu ja luonnonvarojen kestävä käyttö sekä hyvät toimintatavat ja vastuullisuus suhteessa henkilöstöön, asiakkaisiin ja kuluttajiin, verkostoyhteistyössä toimiviin kumppaneihin ja ympäristön asukkaisiin ja yhteisöihin.



Paikannusta käytetään monesti logistiikan tehostamiseen, eikä niinkään turvallisuuden lisäämiseen. Kasvihuoneilmiö tulee lisäämään tulevaisuudessa logistiikan tehostamistarpeita ja yksi jo yksi tärkeimmistä on paikannuksen käyttö. Yhden tavoitteen saavuttamiseksi ei voida ottaa suhteessa suurempia haittoja tai riskejä muualla. Yhteiskuntavastuun osana voidaan pitää myös sitä, että paikannuksella voidaan tarkkailla kuljettajien ajotapoja. Ajoneuvoista tuotetaan reaaliaikaisesti tietoa autosta, kuljettajan ajotavasta sekä ajo ja lepoajoista ja edistää näin liikenneturvallisuutta.

Kaikkien lopputulosten pitää tukea prosessien mahdollisimman suurta läpinäkyvyyttä ja yhteiskunnallista hyväksyttävyyttä. Asioita ei voida tarkastella pelkästään taloudellisuuden tai turvallisuuden näkökulmista vaan koko yhteiskunta tulee ottaa huomioon. Viranomaisetkin haluavat tehdä eettisyydestä kilpailuedun. Näyttö siitä että toiminta on eettisesti hyväksyttävää ja läpinäkyvää siltä osin kuin se voi olla, voi helpottaa myös viranomaisen toimintaa.

Viranomaisen saa enemmän luottamusta laillisuusvalvontaviranomaisilta ja vähemmän valituksia ”asiakkailta” kun kaikki on hoidettu oikein. Tämä taas voi edesauttaa lisärahoituksen saamista toimintaan tai lainsäädäntöuudistusten tekemistä. Lainsäädäntöä saadaan uudistettua siihen suuntaan, että viranomaiselle saadaan entistä enemmän uusia valtuuksia kun toiminnan oikeellisuudesta ja valvonnan tehokkuudesta voidaan olla varmoja.

Epävarmuus toiminnan laadussa näkyy heti rahoituksessa. Uusia valtuuksia ei uskalleta antaa jos vanhojenkin käytössä on epäselvyyksiä. Viranomaisillakin on selkeää kilpailua, Menestys ja hyvä tulos alalla tuo yleensä myös selkeästi paremman rahoituksen menestyneelle yksikölle. Hyvä tulos tarkoittaa myös sitä että veronmaksajat tai asiakkaat ovat tyytyväisiä saamaansa palveluun.

#### 5.5.4 Tiedonvaihto elinkeinoelämän ja viranomaisten välillä

Valtioneuvoston sisäisen turvallisuuden ohjelman (2006) yhtenä tavoitteena on poistaa hallinnollisia ja oikeudellisia esteitä tietojenvaihdossa yrityksiin kohdistuvien rikosten torjumiseksi niin, että yritykset saavat riittävän suojan ja viranomaiset riittävät tiedot yritysten rikosturvallisuustilanteesta. Tietojenvaihdon sääntelyssä säilytetään tasapaino rikostorjunnallisten ja yksityiselämän suojaan (yksityisyys, henkilötietojen suoja ja luottamuksellisen viestin salaisuus) liittyvien intressien välillä. SATERISK-projekti on erinomainen keino toteuttaa tätä valtioneuvoston asettamaa tavoitetta. Yhteistoiminnan mahdollistaminen on yksi ydinkysymyksistä.

Yhä enemmän erilaisia tehtäviä ollaan siirtämässä viranomaisilta yksityiselle sektorille, varsinkin vartiointiliikkeille. Tämä siirto voi väärin tehtynä aiheuttaa vakavia tiedonsiirron katkoksia ja heikentää näin yleistä turvallisuutta ja yhteiskunnan reagointikykyä.

#### 5.5.5 Kuljetus- ja logistiikka-alaan kohdistuva rikollisuus

Verkostoituminen on mainittu yhdeksi megatrendiksi useilla listoilla esimerkiksi (Larsen, 2006). Verkostoitumisen ydinkysymyksiä ovat tiedonsiirron ja logistiikan nopeutuminen ja kustannustehokkuus. Paikannus on tärkeä osa tätä kokonaisuutta.

Valtioneuvoston sisäisen turvallisuuden ohjelman (2006) mukaan kuljetusrikollisuus sisältää useita erilaisia rikosnimikkeitä, mm. salakuljetus, lastiysikköön ja lastiin kohdistuvat rikokset sekä harmaan talouden piiriin kuuluvat ilmiöt. Myös terroristit voivat käyttää kuljetettavaa tavaraa tai kuljetusta terroritoiminnan välineenä. Järjestäytyneen rikollisuuden lisääntyminen ja rikollisryhmien kiinnostus logistiikka-alaa ja kuljetustoimintaa kohtaan lisääntyy koko ajan. Kuljetettavan ja varastoitavan tavaran omaisuusarvot ovat suuret ja alaa käytetään keinona myös muulle rikollisuudelle kuten salakuljetukselle ja ennen kaikkea harmaalle taloudelle ja rahanpesulle. Kansainväliset logistiikkayritykset ovat houkuttelevia kohteita järjestäytyneelle rikollisuudelle. Kuljetuksiin ja logistiikkayrityksiin kohdistuva rikollisuus kasvaa Euroopassa 5 %:n vuosivauhdilla. Rikoksen kohteena olevat omaisuusarvot ovat kasvaneet huomattavasti. Mukaan on tullut väkivaltaisia piirteitä. Jatkossa on tärkeää kehittää logistiikka-alaan kohdistuvan rikollisuuden tunnistamista ja ilmiöön liittyvää seuranta. (Sisäministeriö 2006)

Rikosuhkaa tulee torjua suunnittelemalla yrityksille käytännön toimenpiteitä toiminnan turvaamiseen. Yrityksen tulee tuntea omat järjestelmänsä ja tiedonkäsittelykulttuurin todellinen tilanne, ja se tulisi olla jatkuvan tarkastelun kohteena. Tärkeää on että tarkastelussa huomioidaan kaikki tieto- ja viestintävälineet myös pitkissä alihankintaketjuissa.

Turun käräjäoikeuden päätöksestä (2008) ilmenee, että Liedon rahankuljetusryöstön yhteydessä rikollisilta takavarikoitiin häirintälaitte, jolla on mahdollista estää GSM-puhelinten ja GPS paikannusvastaanottimien toiminta.

Rikollisia on poliisin teknisen seurannan keinoin saatettu syytteeseen ja tuomittu rikoksista. Rikolliset ymmärtävät, että viranomaiset saattavat seurata heitä seurantalaitteella ja että iskun kohteena olevaa rahankuljetusautoa voidaan myös seurata paikannuslaitteella. Häirintälaitteen hankkimisella lyödään kaksi kärpästä yhdellä iskulla. Rikollisten oma paikka tai kohteen paikka ei välity enää eteenpäin. Tulevaisuudessa on ymmärrettävää, että myös rikolliset osaavat tekniikan käytön ja kilpajuoksu osaamisesta on alkanut tälläkin sektorilla.

#### 5.5.6 Yksityisyyden suoja

Lainsäädäntö tulee yleensä aina teknisen kehityksen jäljessä. Laki yksityisyyden suojasta työelämässä 13.8.2004/7597 luvun 21 § säädetään Yhteistoiminnasta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä.

”Työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoidellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluiksi edellä mainituista asioista”. (13.3.2009/126)

Esimerkiksi logistiikka alalla ei ole järjestelmää, josta edes kuljetusliike itse tietäisi, onko kuljetuksessa jokin kolli, jossa on seurantalaitte. Tätä on tulevaisuudessa kuitenkin pidettävä aina vain todennäköisempänä. Tehtäessä ehdotuksia tulevaisuuden laite ja toimintamalliratkaisuksi on työntekijöiden yksityisyyden suoja pidettävä koko mielessä sekä yhteiskuntavastuun perspektiivistä, että paikannuttajan mahdollisen vastuun perspektiivistä.

Ns. lex nokian käytännön sovellutukset ovat tätä kirjoitettaessa vasta muotoutumassa. Lex nokian yhteydet paikkatietoon ovat vielä avoimia kysymyksiä.

## 5.6 Tavoitteena tulevaisuuden turvallisemmat palvelut.

SATERISK-projektin tuotoksien tulee antaa suuntaa tulevaisuuden palveluille. Tästä syystä on tarpeellista panostaa tulevaisuuden tutkimukseen. Tulevaisuus ei ole ennalta määrätty ja sitä voivat muokata yksilöiden, instituutioiden ja luonnonvoimien toiminta. On olemassa tulevaisuus ilman toimintaa ja erilainen tulevaisuus toiminnan seurauksena. (Mika Mannermaa, 2003, 24).

SATERISK-projektin on tarkoitus muokata tulevaisuutta kehittämällä satelliittipaikannusta ja sen käyttöä. Jo projektia alun perin määriteltäessä oli tärkeää, että se valmistuisi ennen kuin EU:n oma paikannusjärjestelmä Galileo alkaa toimia n. vuonna 2013. Toisaalta tällä hetkellä paikannusjärjestelmistä ovat käytössä GPS, venäläisten Clonass ja jossain mittakaavassa myös kiinalaisten Compass.

Osa vaatimusmäärittelyä ja työpakettien suorittamaa riskikartoitusta on suuntautuminen toisaalta myös tulevaisuuteen. Tämän tutkimuksen vaatimusmäärittelyyn kuuluu, että kaikista tutkimuksen sisällä on selkeästi erotettavissa:

- a) nykyisin ja tällä hetkellä olevat riskit
- b) Riskit joita skenaarioiden pohjalta oletamme tulevan jollain todennäköisyydellä tulevan tapahtumaan tulevaisuudessa seuraavan viidentoista vuoden aikana.

Kuten kaikki meitä ympäröivä ovat myös riskit olemassa sekä ajassa, että tilassa. Tässä projektissa tulee siis riskikartoituksissa olla seuraavat ajalliset kohteet.

#### 5.6.7 Nykytila

Suomessa kaikilla turvallisuusviranomaisilla on erilaisia satelliittipaikannusta hyödyntäviä laitteistoja. Laitteistot ovat varsin usein suljettuja, vain määrättyyn käyttöön tehtyjä ratkaisuja. Erittäin harvoin laitteistoihin on integroitu viestiliikenteen salaus, joten niiden tuottaman tiedon siirtäminen ilman erillisiä raskaita salausjärjestelmiä ei onnistu. Usein jopa yhden viranomaisen käytössä olevat ratkaisut eivät toimi kunnolla muiden saman viranomaisen laitteistojen kanssa.

Liike-elämän logistiikan käytössä on myös lukuisia järjestelmiä, joita yleensä käytetään logistiikan optimoimiseen, mutta myös turvaamiseen.

Jos logistiikkatoimija tarvitsee jostain syystä viranomaisen apua liikkuvaan kohteeseen, jota hän itse paikantaa, ei hän tällä hetkellä pysty kuitenkaan toimittamaan paikkatietoa viranomaisen käyttöön. Hälytyskeskuksen perustavat toimintansa edelleen vain siihen, että avunpyytäjä toimittaa informaatiota vain puhelimella. Mitä riskejä on löydettävissä nykyisin käytössä olevista laitteistoista, niiden käyttöohjeistuksesta, käytöstä, ja mahdollisia käytön jälkeisiä riskejä. Arviointi perustuu siis kokemukseen ja käytettävissä olevaan tietoon.

#### 5.6.8 Tulevaisuus

Tulevaisuudentutkija Mika Mannermaa on antanut uuden kirjansa nimeksi ”Jokuveli”. Jokuveli-yhteiskunta on kyseisessä skenaariossa ”lempeän valvonnan, tietämisen ja unohtumattomuuden yhteiskuntaa”. Tärkein ero ”jokuveljen” ja Orwellin ”isonveljen” välillä on se, että valvonta on yhteisesti hyväksyttyä ja läpinäkyvää.

Jokuveli ei mannermaan mukaan ole yksittäinen toimija, vaan kokonaisuus johon kuuluvat julkiset toimijat, kuten poliittiset päättäjät ja viranomaiset, yritykset työnantajina ja tuot-

teiden ja palvelujen tarjoajina ja viime kädessä myös me kaikki kansalaiset, kukin omine intresseinemme. (mannermaa, M, 2008, 35).

Satelliittipaikannus ja sen tuottaminen läpinäkyvästi on yksi tärkeä näkökohta tässä projektissa. SATERISK-projektissa tutkimme uusia teknologioita ja käytänteitä osin tulevaisuudentutkimuksen keinoin. tulevaisuudentutkimuksella pyritään laajentamaan ihmisten tietoisuutta ja sitä kautta kehittämään heidän taitojaan, käyttäytymistään ja valintojaan. Tulevaisuuteen liitetään usein se, että kaikki muuttuu. Näinhän asia ei todellisuudessa ole vaan aina on myös asioita jotka pysyvät lähes entisellään, muuttuvat hyvin hitaasti. Useimmat ihmiset tarvitsevat jotain pysyvää, jotta voivat tuntea olonsa turvalliseksi, jatkuva muutos saattaa aiheuttaa epävarmuuden tunteen.

Megatrendit ovat jotain mitä olemme tietävinämme oletettavasta tulevaisuudesta. Megatrendit ovat siis voimia jotka sitovat yhteen nykyisiä ja tulevia maailmojamme. Tästä syystä kaikki jotka tekevät työtä strategioiden parissa ovat kiinnostuneita megatrendeistä. Monet käyttävät megatrendejä ikään kuin lähtökohtina tulevaisuuteen. Tulevaisuuden tapahtumiin vaikuttavat kuitenkin monet eri tekijät, yhteiskunta, yritykset, yksilöt, luonnonolosuhteet.

Englanninkielistä lähdemateriaalissa esiintyy usein kolmen P:n muistisääntöön erilaisista tulevaisuuksista, esimerkiksi Gitte Larsenin (2006)artikkelissa. Predictable, Possible, and the Preferred eli PPP. Suomeksi siis ennustettava, mahdollinen ja paras. Megatrendit ovat näitä ennustettavia, esimerkiksi ikääntyminen ja niin kuin hetki sitten vielä oli jatkuva varallisuuden kasvu. No varallisuuden kasvu ehkä heikkeni hetkeksi aika monilta, jatkuakseen taas pian, mutta maapallolla on paljon ihmisiä, joilla kehitys kulkee toiseenkin suuntaan. Tulevaisuudentutkimuksessa pitää aina pitää mielessä, ettei tuijoteta pelkästään megatrendeihin vaan katsotaan myös mikä on mahdollista tai mikä olisi paras vaihtoehto.

## 5.7 GALILEON otettava huomioon

Euroopan unioni näki tarpeen omaan järjestelmään jo 90-luvun alkupuoliskolla ja projekti-suunnitelmaa alettiin tehdä. Satelliittipaikannus on yleisin paikannuskeino. Radioverkkopohjaista paikannusta on myös kehitetty erilaisten järjestelmien päälle, muuta satelliitti paikannuspäälaitteiden halpeneminen ja niiden ylivoimainen tarkkuus verkkopaikannukseen verraten ovat aiheuttaneet sen että lähes kaikki liikkuva arvokas omaisuus kuten laivat ja lentokoneet paikannetaan satelliittipaikannuksella. Optimaalisen kattavuuden saavuttamiseksi tarvitaan satelliitti- ja maanpäällisten järjestelmien yhteistoimintaa.

GALILEO on Euroopan avaruuspolitiikan lippulaiva. Sen tavoitteita ovat muun muassa vastata kansalaisten tarpeisiin, palvella muita EU-politiikkoja, keskittyä avaruussovelluksiin ja parantaa Euroopan kilpailukykyä. GALILEO on täydellinen väline näiden tavoitteiden saavuttamiseen. (KOM. 2006. 769.)

Syy EU:n Galileo-projektiin on Euroopan avaruusjärjestö ESA:n mukaan halu varmistaa Euroopan kyky toimia. Nykyisin paikannus perustuu joko yhdysvaltojen GPS, tai venäläiseen Glonass järjestelmään. Molemmat järjestelmät on perustettu alun perin sotilaallista toimintaa varten. Kumpikaan edellä mainittu maa ei anna takuuta siitä, että Euroopalla on heidän järjestelmänsä jatkuvassa keskeytymättömässä käytössä. Esimerkkejä tarkoituksellisista käyttökatkoksista ja rajoitteista on.

Nämä järjestelmien käytön keskeytymiset eivät liity niinkään mahdollisiin teknisiin tai muihin ”force majur” ongelmiin vaan nimenomaan suurvaltapolitiikkaan ja sotilaalliseen toimintakykyyn.

GALILEO on myös nähtävä laajemmassa asiayhteydessä komission pyrkimyksissä edistää innovaatioita ja Lissabonin strategiassa, jossa julkisen sektorin toimilla voi olla ratkaiseva osuus maailmanlaajuisesti kilpailukykyisten yhtiöiden toiminnan edistämisessä. Se on hyvä esimerkki edelläkävijämarkkinasta. (KOM. 2006) . Euroopan Unionin parlamentti on hyväksynyt GALILEON käytön enenevässä määrin myös sotilaallisiin sovellutuksiin.

## 5.8 GPS otettava huomioon

NAVSTAR GPS ( Navigation Satellite Time and ranging) on kaikkialla maapallolla 24 tuntia vuorokaudessa toimiva, satelliitteihin perustuva järjestelmä, jonka avulla käyttäjä voi määrittää oman paikkansa ja nopeutensa sekä saada tarkan ajan. GPS on yleisin käytössä oleva satelliitipaikannusjärjestelmä. Järjestelmä on Yhdysvaltain puolustusministeriön (DoD) kehittämä ja omistama. GPS-satelliitit kiertävät maata 20200 kilometrin korkeudessa.. DoD sai yleisesti GPS.ksi kutsutun NAVSTAR projektinsa täyteen operatiiviseen käyttöön 27. Huhtikuussa 1995. (USNO 2009)

Satelliitit eivät ole maan suhteen paikallaan vaan kiertävät maan noin kahdesti vuorokaudessa. Satelliitteja on 27 kappaletta, joista käytössä on 24. Loput ovat varasatelliitteja. GPS-satelliitissa on kaksi lähetystaajuutta, joista vain toinen on saatavissa siviilikäyttöön.

## 5.9 GLONASS otettava huomioon

GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) on Venäjän käytössä oleva satelliittipaikannusjärjestelmä. Vaikka GLONASS-järjestelmä on monilta osin hyvin samankaltainen GPS-järjestelmän kanssa, niin suurimpana teknisenä erona voidaan pitää satelliittien erottelun perustumista taajuusjakoon (FDMA, Frequency Division Multiple Access) toisin kuin GPS:ssä, jossa erottelu perustuu koodijakoon (CDMA). (Airos, 2007). Venäjä panostaa voimakkaasti järjestelmän uusimiseen. On mahdollista että Venäjä haluaa että sen alueella käytetään vain GLONASS-järjestelmää.

#### 5.10 COMPASS (Beidou) otettava huomioon.

COMPASS on kiinalaisten oma satelliittipaikannusjärjestelmä, jossa on myös siviilisektorille oma vapaasti maailmanlaajuisesti käytössä oleva saatavuus. Kiinan televisiossa 18.1.2009 on julkaistu inside GNSS lehden mukaan tieto, että Kiina saa vuoteen 2015 mennessä taivaalle yli 30 paikannussatelliittia, joka tarkoittaa käytännössä sitä, että laitteisto toimii koko maapallon alueella. Saman lehden mukaan Johtaja Zhao Xiaojin, head of the astronautics department for China Aerospace Science and Technology Corporation on sanonut, että Kiina laukaisee ensi vuoden loppuun mennessä 10 satelliittia. Kyseinen määrä satelliitteja saattaa riittää alueellisen (Kiina) toimintakyvyn saamiseen. (Gibbons Media & Research LLC.2009.).

Tämä tarkoittaa P. Brownin (2008) Infowarmonitor-sivustolla julkaistun artikkelin mukaan sitä, että kiinalaisten COMPASS saavuttaa ainakin joillakin alueilla toimintakykynsä huomattavasti aikaisemmin kuin EU:N GALILEO.

### 6 SATERIS-projektissa käytettävät prosessit ja työkalut

Seuraavassa on kerrottu niitä riskiarvioinnin ja tulevaisuudentutkimuksen työkaluja joita tulisi käyttää tässä projektissa. On mahdollista käyttää myös muita työkaluja, mutta suositellaan jäljempänä kuvattuja. Tämä johtuu siitä, että samantyyppisillä työkaluilla työskennelleiden ryhmien työt on myöhemmin helpompi yhdistää.

#### 6.1 Käytetyt menetelmät on kirjattava osaksi riskikartoitusraporttia.

Mannermaan (2008, 103)mukaan monimutkaistuminen, riskiyhteiskunnan voimistuminen ja toisaalta luottamusyhteiskunnan välttämättömyyden muodostama kokonaisuus kuuluu tulevaisuuden tärkeimpiin megatrendeihin. On luonnollista, että riskit pitää ensin olla tiedossa, ennen kuin luottamusta voidaan lähteä rakentamaan.

Kullekin työpaketille muodostetaan vastuualueen vetäjän johdolla yksi tai useampi ryhmä, joka aloittaa riskikartoituksen valitsemallaan tavalla. Valittu riskikartoitusmetodi tulee kirja-

ta aina kyseisen riskikartoituksen alkuun. Satelliittipaikannuksen riskien merkityksen selvittämiseksi liike-elämälle ja muulle yhteiskunnalle täytyy riskikartoitusryhmän tehdä vielä seuraavien vaiheiden tueksi PESTE-analyysi. PESTE-analyysin tulosta on tarkoitus käyttää apuvälineenä riskikartoitusta tehtäessä. Samassa työpaketissa on jopa suotavaa pitää useita osanottajiltaan ja riskienanalyysitavoiltaan erilaisia kokouksia. Työpaketin vetäjä saa näin jo työpaketin sisällä aikaan triangulaatiota ja voi näin varmistua analyysin onnistumisesta. Työvälineitä riskienkartoitukseen löytyy esimerkiksi sivustolta PK/RH.fi. Yhtenä käytettävänä työkaluna tulee kuitenkin olla SWOT-analyysi.

## 6.2 Graunded Theory

Hypoteesi-käsitettä käytetään ilmaisemaan uutta, testaamatonta tai kiistanalaista teoriaa. Tällöin hypoteesilla viitataan teorian perusteltavuusasteeseen (Niiniluoto 1983, 122). Hypoteeseja eli oletuksia tulee käyttää selittävässä tutkimuksessa ja niiden esittäminen kuuluu tutkimukseen. Hypoteesi tarkoittaa sitä, että asetettuihin ongelmiin on mahdollista ennakoida ratkaisuja tai selityksiä (Hirsjärvi 2007, 154). Ei ole olemassa mitään yksiselitteistä kriteeriä sille, koska hypoteesi muuttuisi teoriaksi, varmasti myös tutkijoilla on ennako-olettamuksia tuloksista. Toisaalta kaikki ovat lähdössä tutkimukseen mukaan koska selviä aukkoja on edelleen tietämyksessä ja tutkijat oletettavasti yllättyvät ja oppivat paljon uutta tutkimuksen kuluessa. Mahdollista on, että alalla ja tässä projektissa on suurelta osin turvauduttava käytännössä toimivaksi osoittautuneeseen teoriaan. SATERISK-projektissa etsimme ensin käytännön maailmasta siellä olevat toimintamallit ja riskit ja näiden pohjalta Graunded Theory-mallin (Charmaz 2006, 10) mukaan ehkä pääsemme tilanteeseen, jossa voimme tietojemme pohjalta luoda uutta teoriaa.

## 6.3 Peste

Opetushallituksen (2004) Verkkosivuilla kerrotaan, että PESTE apumenetelmä, jolla selvitetään ilmiön tai organisaation poliittista, ekonomista, sosiaalista, teknistä ja ekologista tilaa ja tulevaisuutta. Monitoroituja muutosvoimia voidaan hyödyntää eri tavoin esim. yhteiskunnallisia skenaarioita laadittaessa ne voivat toimia tulevaisuustaulukon muuttujina tai vaikka taustamateriaalina organisaation laatiessa skenaarioita toiminnalleen. PESTE lista tulee laatia heti työn alussa, koska se on hyvin käyttökelpoinen ”idealista” riskikartoitusta tehtäessä

PESTE-nimi syntyy seuraavien muutosvoimien nimistä:

### Poliittiset

lainsäädännön rajoitukset, kansainväliset sopimukset, rikollisuus, yhdentymisen esim. EU, tutkimus-, kehittämis-, alue-, matkailu-, yms. politiikka;



#### Ekonomiset

maailman, Euroopan, alueen talouskehitys, talouskriisit ja lamat, kilpailurajoitukset, julkinen rahoitus ja tuet, ostovoima

#### Sosiaaliset,

Arvot, kulutuskäyttäytyminen, ikärakenne, muuttoliike, syntyvyys

#### Teknologiset:

informaatio- ja tietoliikenne, bio-, nano-, energiateknologiat, verkkokauppa, virtuaalimaailma

#### Ekologiset

kasvihuoneilmiö, ilmaston muutos, saastuminen, jäteongelmat, liikarakentaminen, ympäristötietoisuus, infrastruktuurin muutos

### 6.4 Villi kortti (Wild card)

Paras vaihtoehto kannattaa pitää mielessä vaikka se ei helpoin vaihtoehto olisikaan, koska tulevaisuudenhan saattaa onnistua tekemään, ja tällöin riman pitää olla tarpeeksi korkealla, niin kuin klassisessa esimerkissä Kennedystä ja kuuprojektista, jota oikeastaan kukaan ei pitänyt mahdollisena.

Villit kortit ovat siis tapahtumia jotka ovat mahdollisia, mutta epätodennäköisiä ja joilla on erittäin suuret vaikutukset. Viimeinen esimerkki villistä kortista, yllättäen tullut lama painaa nyt meidän niskaamme ja hajottaa jatkuvan kasvun megatrendiä.

Yhtä tärkeää kuin selvittää muuttujat on myös löytää ne asiat, jotka pysyvät ennallaan. Näistä voidaan sitten rakentaa uutta osaamista. Mannermaa kirjoittaa, että ”kaikkiallinen tietoyhteiskunta, ubiikkiyhteiskunta, voidaan ymmärtää tietoyhteiskunnan uudeksi vaiheeksi. Teknologian kehitys on edelleen voimakasta, mutta yhteiskunnallisesti merkittävämpiä ovat sisällöt, kysymykset siitä miten teknologiaa käytetään.” (Mannermaa 2008,25)

SATERISK-projektissa tulee kiinnittää teknologian lisäksi erittäin paljon huomiota siihen, miten laitteistoja käytetään ja valvotaan ja miten ne sopeutuvat yhteiskunnan tulevaan kehitykseen. Mannermaa (2008, 40) kirjoittaa kirjassaan tärkeän huomion ” Kun tietoyhteiskunnan ensimmäinen vaihe syventyy toiseen, ubiikkiyhteiskunnan vaiheeseen, yksipuolisen valvonnan mahdollisuus rasittaa ihmisten sietokykyä. On mahdollista luoda monisuuntaista valvontaa, ja luoda myös vallankäyttö läpinäkyväksi.

SATERISK-projektin puitteissa, etenkin sen skenaariotyöskentelyvaiheessa, tulee käydä keskusteluja myös yhteiskunnallisten tahojen kanssa, ei pelkästään projektissa mukana olevien toimijoiden kesken.

## 6.5 SWOT-analyysi

SWOT-analyysi on lyhenne seuraavien sanojen alkukirjaimista: S sanasta strength (vahvuus), W sanasta weakness (heikkous), O sanasta opportunity (mahdollisuus) ja T sanasta threat (uhka). SWOT-analyysi on ruudukon muotoinen.

SWOT- nelikenttäanalyysi on hyvin monikäyttöinen. Tarkastelu voi koskea joko koko toimintaa tai yksityiskohtaisemmin jotakin toiminnan osaa. Yksityiskohtainen tarkastelu on rajatumpi, eli kohteena voivat olla esimerkiksi markkinat, tuotteet tai henkilöstö. Parhaimmillaan SWOT-analyysi on yksinkertainen menetelmä, jota voidaan käyttää yrityksessä joko yksin tai ryhmässä työskennellen. Työnantajien keskusliiton EK:n PK/RH riskienhallintasivustolla suositellaan, että jokainen tekee analyysin ensin yksin ja kirjaa nelikentän ruutuihin yrityksen vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia. Tämän jälkeen kaikkien ajatukset kootaan ryhmätyönä yhteen. Tällaisella aivoriihi-menetelmällä kyetään tila selvittämään mahdollisimman kattavasti.

Analyysin teossa kannattaa noudattaa seuraavia periaatteita:

- Tee mahdollisimman yksinkertainen ja käytännönläheinen analyysi.
- Pidä erillään nykytila (vahvuudet, heikkoudet) ja ne tekijät, jotka vaikuttavat tulevaisuudessa liiketoiminnan onnistumiseen (uhat, mahdollisuudet).
- Pyri löytämään nelikentän jokaiseen ruutuun yritystäsi kuvaavia tekijöitä. Kirjaa kaikki mieleen tulevat asiat ruudukkoon. Mitä enemmän ideoita syntyy, sitä parempi.

SWOT-lomake on saatavana PDF-tiedostona.

## 6.6 Riskikartoituksen yhteenveto

Riskikartoitus tulee tehdä riittävän asiantuntijafoorumin kesken, mutta satelliittipaikannuksen pitkistä arvoketjusta johtuen ryhmiä tulee useita. Osa-alueiden riskienkartoituksen jälkeen tulee pitää työpakettien vetäjien ja tarvittaessa muiden asiantuntijoiden toimesta riskien yhteenvetokokous, jonka tarkoituksena on luoda yksi yhtenäinen dokumentti riskikartoituksen tuloksista. Kyseiseen dokumenttiin on pyrittävä liittämään myös työryhmien tekemiä taustamuistioita, koska ne saattavat olla seuraavissa vaiheissa tarpeen. Yhteenvedosta tulee tehdä erillinen SWOT-analyysi. Koottu dokumentti jaetaan kaikkien työpakettien vetäjille.

## 6.7 Skenaariotyöskentely

Galileon käyttöönottohetki on useiden vuosien päässä tulevaisuudessa. Normaali riskienkartointuskin katsoo aina tulevaisuuteen, mutta ei useinkaan useampien vuosien päähän. Jotta Sate-risk projekti voi toimia tulevaisuuden innovaatioiden pohjana täytyy sen tuottaa muutamia todennäköisiä yli 5 vuoden tähtäyksen tulevaisuus skenaarioita, joiden pohjalta laaditaan sitten vastaavat riskikartat. Skenaariotyöskentely voidaan aloitetaan vain, jos paikannuksen nykytilan riskikartointus on tehty ensin. Tulevaisuudentutkimuksen pohjaksi tulee olla vankka käsitys ainakin nykyisistä vahvuuksista, heikkouksista, mahdollisuuksista ja uhista. Tähän saadaan vankka pohja riskikartoituksen yhteenvedosta ja SWOT-analyysistä.

Skenaariotyöskentelyssä ei ole kysymys vain yhdestä menetelmästä. Kysymys on ennemminkin lähestymis- tai työskentelytavasta joka sisältää useita erilaisia menetelmiä ja työkaluja. Meristön mukaan skenaariotyöskentely on pohjimmiltaan keino luovuuden edistämiseksi. (Meristö 2003, 246)

Mannermaan mukaan skenaarioparadigma kuvaa perusnäkemystä, jonka mukaan tulevaisuudentutkimuksen ensisijainen tehtävä ei ole ennustaa todella tapahtuvaa tulevaisuutta, koska sen ei uskota - ainakaan vielä - olevan mahdollista. Ennustamisen sijaan tavoitteena on hahmottaa useita erilaisia laaja-alaisia ”käsikirjoituksia”, skenaarioita, joiden arvo ei määräydy niiden toteutumis- todennäköisyyden vaan skenaarioihin liittyvien tapahtumainkulkuihin liitetävien arvostusten perusteella. (Mannermaa, 2003, 32)

Tulevaisuuden skenaarioita pyritään tässä projektissa rakentamaan kultakin työpaketilta vähintään kolme. Mannermaa (1999, 66) toteaa, että mielekäs skenaarioiden määrä liikkuu kolmen ja viiden välillä: Kaksi on liian vähän, koska silloin on vaikeaa esittää muuta kuin dikotomin hyvän ja pahan skenaarion jako, joka todellisuudessa on vain vaihtoehdottoman, yhden tulevaisuuden malli.

Toimintamalliksi SATERISK-projektissa otetaan Meristön toimintatutkimusskenaarion prosessi, jossa on neljä päävaihetta. (Meristö, T. 2003, 240)

- 1) kuka ja missä me olemme
- 2) mitkä ovat mahdolliset maailmat
- 3) minne voimme mennä ja kuinka
- 4) minne päätämme mennä

Tulevaisuuden osio voidaan siis aloittaa vasta silloin kun nykytilanteen riskikartointus ja PESTE on valmis. Tästä syystä tämä osuus tehdään erikseen sen jälkeen kun työhön osallistuneet

ryhmät ovat ehtineet rauhassa tutustua nykytilanteesta laadittuun materiaaliin ja sisäistäneet sen. Tulevaisuuden ennustamisen pohjatieedoksi tarvitaan myös tietoa arvoista, toiveista, pe-loista, tavoitteista ja myös ns. hiljaista tietoa.

Yksi tulevaisuudentutkimuksen tehtävistä on mm arvioida tekniikan kehitystä tarpeista käsin ja selvittämään tekniikan valintaperusteita ja tekniikan merkitystä kehityksen näkökulmasta, mutta samalla pyritään myös paljastamaan inhimillisen toiminnan luomia uhkia ja katastro-faalisia riskejä ja analysoimaan niitä koskevaa yhteiskunnallista ja kansanvaltaista päätöksen-tekoa. (Vapaavuori 2003, 13)

Tieteen tieto on objektiivinen arvoneutraali tieto. Tätä voidaan kuitenkin soveltaa vain tut-kimuksen vaiheeseen jossa tutkitaan nykyisiä, olemassa olevia paikannuksen tuottamia riske-jä. Tulevaisuudentutkimuksessa hylätään tämä näkemys ja käytäntö. Tulevaisuudentutkimuk-sen tieto on arvorationaalista. Arvorationaalinen päättely ei koske ainoastaan järkevää keino-jen valintaa annetun päämäärän saavuttamiseksi vaan itse päämäärien valintaa hyvän elämän näkökulmasta. (Vapaavuori 2003, 18)

Skenaario on tapa kertoa tulevaisuuden vaihtoehtoista systemaattisella tavalla. se on kerto-mus joka sisältää halutun tai vältettävän tulevaisuuden kuvauksen ja sen perustelut ja kuva-uksen siitä, miten kuvattu vaihtoehto ajatellaan olevan saavutettavissa tai vältettävissä ny-kyisyydestä käsin (Vapaavuori 2003, 15).

Mannermaa (1999, 58) sanookin, että tutkivien skenaarioiden pyrkimyksenä on usein mahdolli-simman todennäköisten vaihtoehtojen löytäminen. Tähän päästään siten, että vaihdellaan joidenkin peruskehityskulkujen painotusta eri vaihtoehtoissa. Tutkiva skenaario voi myös perustua olettamuksiin ja johtopäätöksiin: skenaarion laatija esittää silloin, että jos jokin määrätty päätös tehdään tai toimenpide pannaan täytäntöön, sen seuraamukset ovat skenaa-riossa esitetyn kaltaisia. ( Masini 1993, 93-94)

Jälkimmäisessä tapauksessa prosessi ei jää skenaarioiden laatimiseen, vaan sen kuluessa on myös työstettävä omaa toimintaa ja strategista työskentelyä, tehtävä valintoja oman tulevai-suuden suuntaamiseksi ja jatkettava prosessia ensimmäisen työskentelyvaiheen ohi.

## 6.8 Toinen iteraatio skenaarioiden yhteensovittamiseksi

Kertaluontoisena skenaariotyöskentely avaa uusia näkökulmia ja vaihtoehtoja. SATERISK- pro-jekti on jaettu erillisiin työpaketteihin, joilla on omat vastuuhenkilöt. Eri työpakettien ske-naariot vaikuttavat väistämättä muihin. Tästä syystä skenaariotyöskentely ei ole vain kerran suoritettava projekti, vaan se joudutaan todennäköisesti käymään läpi ainakin toiseen ker-taan sen jälkeen kun työpaketin vetäjät ovat tutustuneet muiden työpakettien tuottamiin skenaarioihin.

Tämän yhteenvedon helpottavana työvälineenä tullaan käyttämään eri työpakettien vetäjien yhdessä tekemää tulevaisuustaulukkoa. Tulevaisuuskartta on mahdollisten tulevaisuuksien symbolinen kuvaus. Sen symbolit-sanat, kuvat, luvut, taulukot, merkinnät -määrittelevät aiheita ja teemoja, joita kartan laatijat syystä tai toisesta pitävät tärkeinä tulevaisuuden elementteinä (vapaavuori 2003, 125).

## 6.9 Delfoi-menetelmä

Delfoi on asiantuntijamenetelmä jossa ryhmään valitaan tarkasteltavaa aihetta eri näkökulmista hallitsevia eksperttejä, joilla arvioidaan olevan poikkeuksellista tutkittavaan aihepiiriin kohdistuvaa tietoa ja näkemystä. Nämä asiantuntijat saatetaan vuorovaikutukseen aiheen teemojen ja toistensa kanssa tavalla, jossa korostuvat asiaperustelut eli argumentit vastaajien aseman ja auktoriteetin sijasta. (Sihvola 1997)

SATERISK-työpaketeissa tuotetaan erilaisia näkökulmia, hypoteeseja ja väitteitä, jotka täytyy yhdistää ja saattaa avoimen asiantuntijakritiikin ja argumentoinnin kohteeksi. Työpakettien vetäjät ja tarvittava määrä muita asiantuntijoita osallistuu Delfoi-prosessiin jolla pyritään saavuttamaan yhteinen jaettu näkemys siitä mihin ollaan menossa. Delfoin tulos viedään vielä tarvittaessa työryhmän uudelleen tarkastettavaksi, jotta varmistetaan, että yhteistä näkemystä koottaessa ei jätetä tärkeitä asioita huomioitua. Samalla Delfoin pohjalta luotu uusi yhteinen kuva voi sisältää työpaketin riskitarkastelua tekeville vielä jotain uusia tarkastelu-kohtia, josta on löydettävissä uusia riskejä.

## 6.10 Tulevaisuustaulukko

Kaikista eri skenaarioista pyritään tekemään tiivistelmä ( synopsis) joka on tarpeeksi yksinkertainen, jotta se voidaan liittää osaksi riskikarttaa. Tulevaisuustaulukko ei esitä yhtä vaihtoehtoa tulevaisuudelle samaan tapaan kuin esimerkiksi monissa projekteissa käytetty roadmap, vaan se eroaa siten, että siinä on mahdollista esittää monta vaihtoehtoa samalla kertaa. Tulevaisuustaulukon tarkoitus on olla osa ponnistus pohjaa kohti uusia innovaatioita.

Aiheiden ja teemojen otsikoita kutsutaan skenaariomuuttujiksi. Tämä skenaariomuuttujien lista on samalla kertomuksen rajausta ulkopuolelle jätettyjen asioiden suhteen sekä kertomisen viitekehys, jossa tulevaisuuden tietäminen aktualisoituu (vapaavuori ym. 125)

Sen jälkeen skenaarioiden pohjalta laaditaan organisaation oma visio eli tulevaisuuteen sijoitettava tahtotilan kuvaus

## 7 Tarve aikakriittisille GIS-järjestelmille

Toiminnan nopeusvaatimukset ja paineet turvallisuusalan kentältä vaativat järjestelmiä, joita voidaan nimittää aikakriittisiksi GIS-järjestelmiksi. Tämä tarkoittaa sitä, että järjestelmää ei niinkään käytetä jälkikäteiseen analyysiin - vaikka se tietenkin tuottaa myös tähän tehtävään vaadittavat paikkatiedot aikaleimoinen sekä tallentaa yksiköiden antamat muut tiedot. Pää-tarkoitus näillä järjestelminä on kuitenkin toimia operatiivisen päätöksenteon välineenä. Järjestelmän tulisi olla luotu siten, että siltä on heti löydettävissä eri tehtäviin tarvittavaa taustamateriaalia sekä kaikki lähes reaaliaikaiset tiedot meneillään olevasta operaatiosta.

Reaaliaikaisuus on kova haaste. Erityisesti pelastusalan ammattilaiset tietävät kuinka tärkeitä ovat ensimmäiset minuutin vammautuneen tai sairastuneen selviämisen kannalta, tai kuinka paljon merkitsee minuutti siihen pääseekö tulipalo valloilleen. Samoin tutkintaviranomaiset tietävät kuinka paljon rikoksen selvittämisen todennäköisyys laskee jos tekijöitä ei saada paikalta kiinni, ja kuinka paljon enemmän resursseja tutkinta vaatii. Tyypillisesti puhutaan minuuteista, ei kymmenistä minuuteista vaan pahimmillaan jopa sekunneista.

Yksityisellä sektorilla paikannusta käytetään paljon rajat ylittävässä liikenteessä paikantamalla tavaraeriä, laitteita ja esineitä. Julkisella sektorilla paikannusta käytetään usein tilannekuvien luomiseen. Molemmissa tapauksissa paikannuslaitteet saattavat liikkua myös kansallisvaltioiden rajojen yli, jolloin saattaa muodostua riskejä ja haasteita, joita paikantaja ei ole tähän asti kyennyt etukäteen arvioimaan.

Kansalliset viranomaiset (valtioneuvosto, puolustusvoimat, Poliisi, Tulli, Rajavartiolaitos) luovat maan sisällä omaan käyttöönsä erilaisia tilannekuvia. Kukin viranomainen tarvitsee vuorollaan tietoa muiden viranomaisten ydintoiminta-alueelta. Maan sisällä tarvittaisiin usein muun Euroopan tilannekuvaa ja päinvastoin. Tilanteiden kenttätason johtamiseen voidaan käyttää vain hyvin lähellä reaaliaikaa olevaa informaatiota. Toimenpiteistä päättämiseen tarvittava tieto pitää olla saatavissa lähes reaaliaikaisesti, jotta tarvittavat toimenpiteet tulee voida toteuttaa nopeasti.

Tilannekuva termiä käytetään hyvin yleisesti, mutta yleisesti hyväksyttyä määritelmää sille ei ole. Tilannekuvan käsitettä hahmotetaan yleensä sitä käyttävän joukon tai tiedon aikakriittisyyden perusteella. Tyypillisesti voidaan hahmottaa kaksi erityyppistä tilannekuvaa: Strategiseen johtamisen työkaluksi tarkoitettu tilannekuva, sekä toinen, oikeasti reaaliaikainen, operatiivisesti hyödynnettävissä oleva tilannekuva.

Operatiivisesta tilannekuvasta on esimerkkinä valtioneuvoston (2003) tilannekuva. ”Valtion johtamisen toimintaedellytysten kehittämisessä asetetaan etusijalle tilannekuva, jota tarvi-

taan yhteiskunnan elintärkeiden toimintojen johtamisessa.” Tässä tilannekuvassa tietoa kerätään laajasti jonka jälkeen sitä analysoidaan ja analyysin tulos on se tilannekuva joka toimitetaan edelleen päättäjille.

Edellä mainitussa lähteessä puhutaan erikseen reaaliaikaisesta tilannekuvasta, joka otetaan käyttöön poikkeustilanteissa. Tällainen muutos ottaa kuitenkin runsaasti aikaa, joten kysymyksessä voi olla vain pitkäkestoiset poikkeustilanteet.

Monesti operatiiviset viranomaisetkin tyytyvät tuottamaan vain tätä strategista tilannekuvaa ylemmän johdon käyttöön. Ympäristössämme tapahtuu kuitenkin koko ajan huumeiden, aseiden, ihmisten, rahan ja muun salakuljetusta sekä muuta toimintaa, joka vaatisi sekä kansallisesti että kansainvälisesti useiden eri viranomaisten toimia. Kuitenkin nämä yhdessä muodostavat valtavan harmaan talouden virran, Mikään strateginen johtaminen ei toimi kunnolla ilman operatiivisia toimia, ja operatiivinen toiminta tarvitsee aina kaiken mahdollisen reaaliaikaisen tiedon.

## 7.1 Tilannekuvan muodostamisen ongelmia

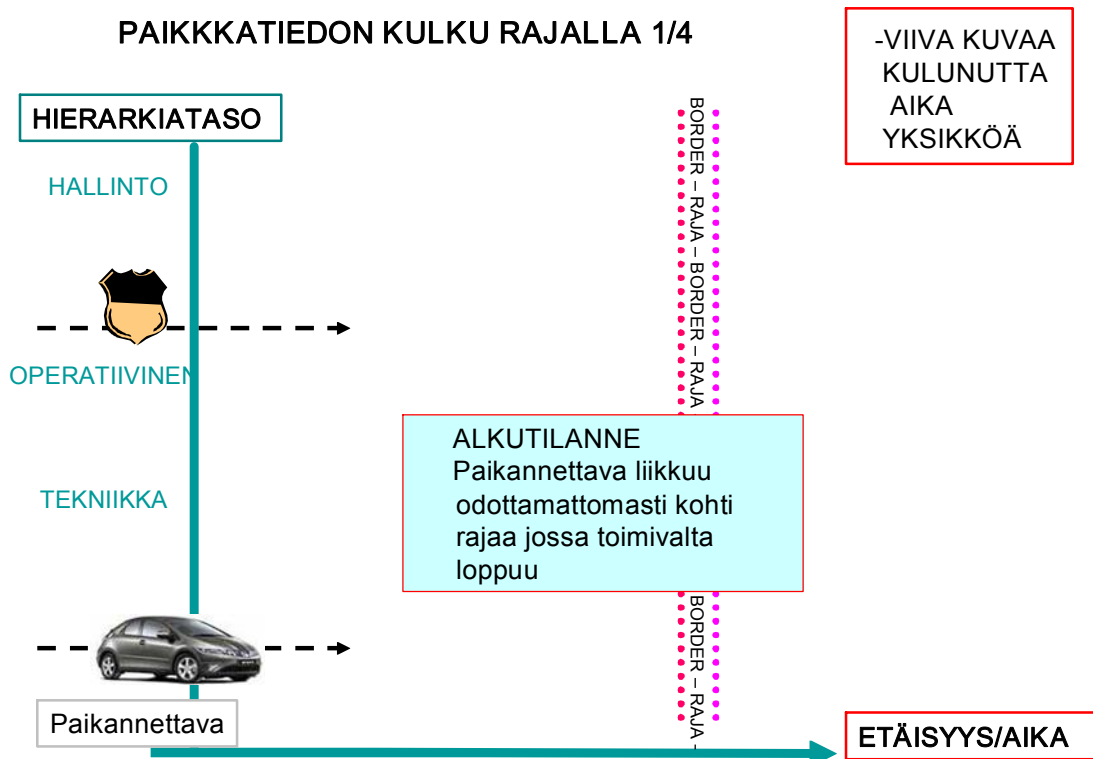
Euroopassa on eri viranomaisilla koko ajan satoja pieniä johonkin tehtävään liittyviä tilannekuvia. Näitä tilannekuvia ei varmasti aina tarvitsisi yhdistää, mutta tulisi olla olemassa järjestelmät, joilla se voitaisiin tarvittaessa tehdä hyvin nopeasti suuremman reaaliaikaisen tilannekuvan muodostamiseksi eri toimijoiden kesken. EU:n komission vetämä EURPSUR-hanke on luotu tähän tarpeeseen.

Strategisesta tilannekuvasta on vaikeaa muodostaa operatiivista tilannekuvaa, sen sijaan toiseen suuntaan toiminta on huomattavasti helpompi suorittaa.

Tällä hetkellä EU:n yhteisten tutkintaryhmien (Joint Investigation Team, JIT) ja yhteisten tullioperaatioiden (Joint Customs Operations, JCO) kaltaisiin välineisiin ei ilmeisesti turvauduta kovinkaan usein. Vuosina 2005 ja 2006 toteutettiin ainoastaan kaksi yhteistä tutkintaryhmää ja neljä yhteistä tullioperaatiota. (KOM 2007 781). Seitsemän jäsenvaltiota on mukana Lissabonissa sijaitsevan huumausaineasioissa toimivan merenkulun analysointi- ja toimintakeskuksen (MAOC-N) operatiivisessa toiminnassa. Mukana olevien jäsenvaltioiden lainvalvontaviranomaiset ja tuomioistuimet sekä meri- että ilma-aluksilla liikkuvat yksiköt tekevät tiivistä yhteistyötä taistelussa Atlantin ja Länsi-Afrikan kautta tapahtuvaa kokaiinin salakuljetusta vastaan. Ilma alukset ja laivat kuitenkin lastataan maalla.

Jo edellä luetusta saa käsityksen kuinka paljon erilaisia toimijoita logistiikkaan ja salakuljetuksen estämiseen liittyy. Ongelmaksi muodostuu eri toimijoiden välisen tiedonkulun hitaus.

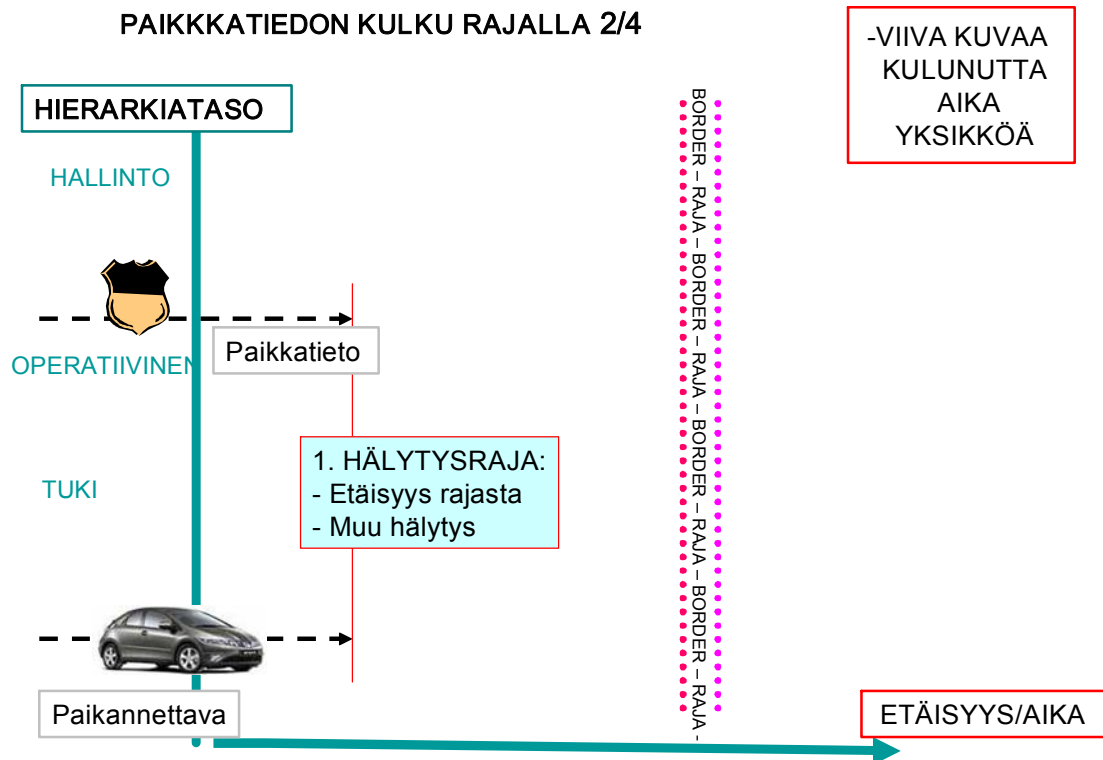
Parhaillaan EU on kehittämässä Euroopan yhteistä rajavalvontajärjestelmää (EUROSUR), jolla voidaan tulevaisuudessa auttaa jäsenvaltioita saamaan täydelliset tiedot tilanteesta ulkorajoillaan. Tilannetietoisuudella mitataan sitä, kuinka viranomaiset pystyvät havaitsemaan rajat ylittävää liikehdintää ja perustelemaan valvontatoimenpiteet. Sen avulla voidaan myös lisätä lainvalvontaviranomaisten kykyä reagoida. Reaktiokyvyllä mitataan sitä, kuinka paljon aikaa kuluu ennen kuin rajanylitysliikennettä päästään valvomaan ja ennen kuin epätavalliseen tilanteeseen pystytään reagoimaan asianmukaisella tavalla. Eurosurin tulisi tarjota yhteinen tekninen kehys, jonka avulla voidaan tehostaa päivittäistä yhteistyötä ja tietojenvaihtoa jäsenvaltioiden viranomaisten välillä ja helpottaa uusimman teknologian käyttöä rajavalvonnassa. Keskeisenä toimintatavoitteena tulisi olla tietojen nopeavaihtaminen (henkilötietoja lukuun ottamatta) nykyisten kansallisten ja EU:n järjestelmien kesken. (Euroopan yhteisöjen komissio. 2008). Ongelmanratkaisu tekniseen puoleen on siis tulossa, ratkaistavaksi jää vielä miten hallinnollinen puoli järjestetään niin, että mahdollistetaan tietojen lähes reaaliaikainen siirtäminen niitä tarvitseville.



Kuvio 3.

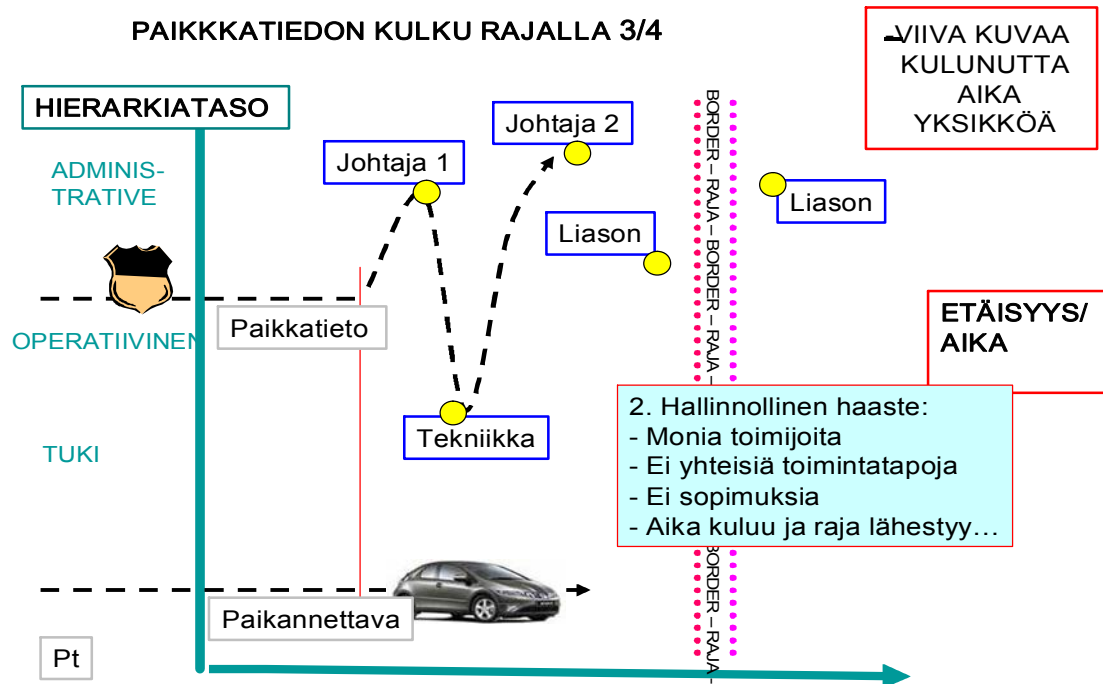
Kuvio 1:ssä on esitetty nykyisin yleinen tilanne, jossa selkeät pelisäännöt puuttuvat. Tekninen välineistö tuottaa tarvittavan tiedon mutta sitä hyödynnetään maksimaalisesti vain yhdellä toimialueella. Kuvassa olevan rajan ei välttämättä tarvitse olla valtakunnanraja, vaan se voi olla myös kahden toimintasektorin tai yksityisen ja julkisen toimijan välinen raja.





Kuvio 4.

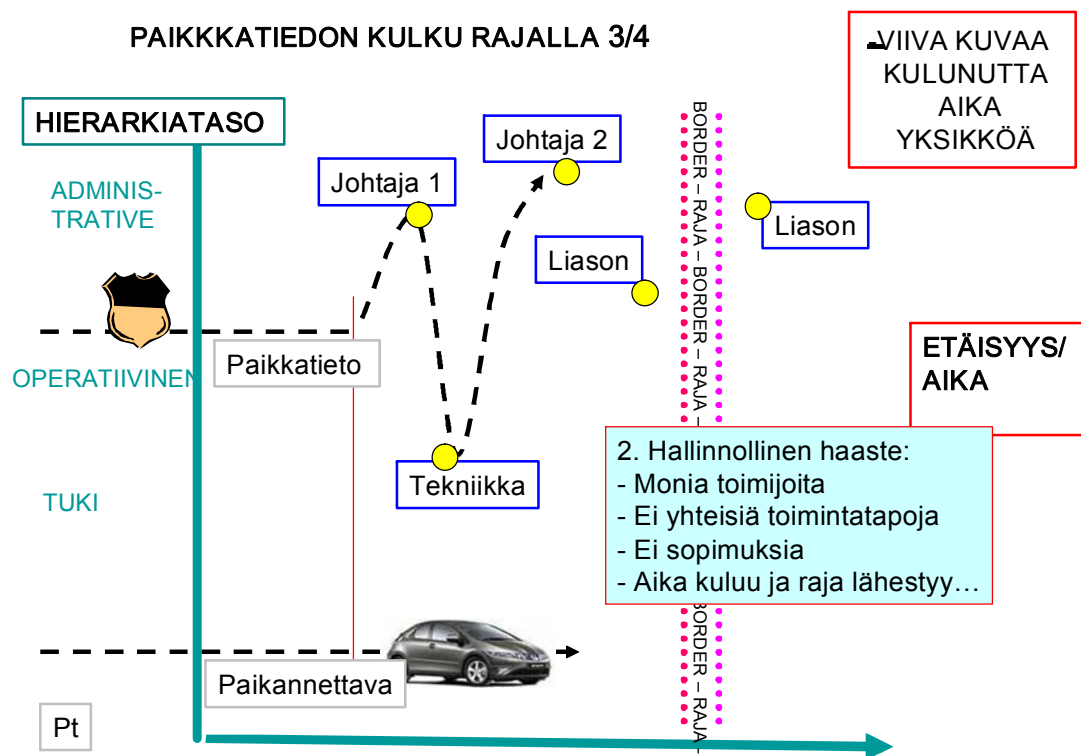
Kuviossa 2/4 Paikannettavan liikkumisesta voidaan todeta, että liikkuminen rajan yli ei ole enää pelkästään mahdollista, vaan alkaa käyttäytymisen perusteella näyttää jopa todennäköiseltä. Tilanne ei siis ole enää normaalitilanne, vaan poikkeamariski on selvästi kasvamassa. On tärkeää huomioida, että suurimmassa osassa nykyisiä järjestelmiä hälytys perustuu siihen, että paikannuttaja toteaa esimerkiksi näyttöpäätteeltään että kohde on siirtymässä väärälle alueelle. Hälytysraja on ylittynyt. operatiivinen henkilöstö alkaa miettiä miten poikkeamaan tullaan reagoimaan.



Kuvio 5.

Kuviossa 3 kohde on jo lähes rajalla. Operatiivinen henkilökunta ottaa yhteyttä omaan esimieheensä, jota kuvassa kuvaa johtaja1. Johtaja 1:ellä on käsitys siitä, että poikkeaman tehokas hallinta vaatii paikkatiedon siirtämistä rajan toiselle puolelle. Seuraava vaihe johtaja 1:ellä on ottaa yhteyttä tekniikkaan sen selvittämiseksi onko tieto teknisesti mahdollista siirtää rajan toiselle puolelle.

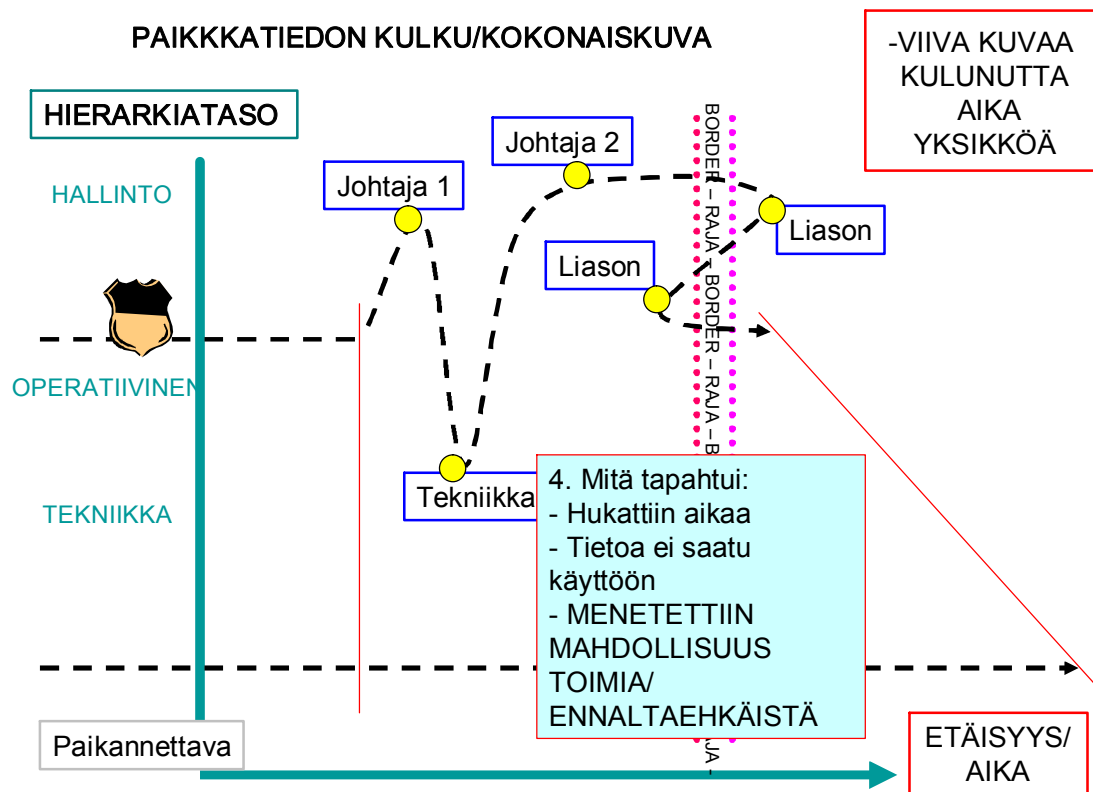
Siirrettäessä tietoa yhteistyökumppaneille saatetaan myös joutua tilanteeseen jossa järjestelmät puhuvat eri kieltä, eivätkä ymmärrä toisiaan. Samoin edistyneimmät toimijat käyttävät tietoturvan vuoksi salausta, jonka purkaminen toiselle osapuolelle voi olla mahdotonta vaikkakin salausavaimet saataisiin haltuun, koska sopivia ohjelmistoja salauksen purkuun ei ole käytettävissä. Teknisesti tiedonsiirto on todennäköisesti lähes aina mahdollista. Lähinnä on kysymys siitä kuinka paljon valmisteluja ja aikaa tiedon formaatin mahdollinen muuttaminen tai esimerkiksi salauksenpurku vaatii. Tämän jälkeen todennäköisesti on vielä operatiivista johtajaa ylempi hierarkiataso jolta kysytään virallinen lupa siirtää tieto. Tätä kuvaa kaaviossa johtaja 2. Hallinnon sisällä käydään asiaa hierarkiassa läpi, koska valmiita ei ole, tai ennakkosuunnitelmat edellyttävät vielä määrättyjä hyväksymismenettelyjä ennen kuin ne voidaan toteuttaa. Tarvittavien henkilöiden tavoittaminen vie aikaa.



Kuvio 6.

Tiedon siirtäminen muille toimijoille aiheuttaa viivettä, koska mutta sen siirtäminen rajan yli ei onnistu ilman erillistä sopimista hallinnollisia ja teknisistä asioista.

kuviossa 2 toisen päällikön hyväksynnän jälkeen tarvitaan vielä liason henkilöitä, joilla on tarvittavat kontaktit rajan toiselle puolelle. Tässä kuvatussa tapauksessa on kaiken kaikkiaan jo viisi erillistä kontaktia eri henkilöihin, jotta tietoa saataisiin eteenpäin. Vaikka kontaktit sujuisivatkin poikkeuksellisen nopeasti, vie jokainen niistä helposti useita minutteja, koska aina pitää siirtää myös tietoa kontekstista uusille henkilöille jo työvuorojenkin vaihtumisesta johtuen.



Kuvio 7.

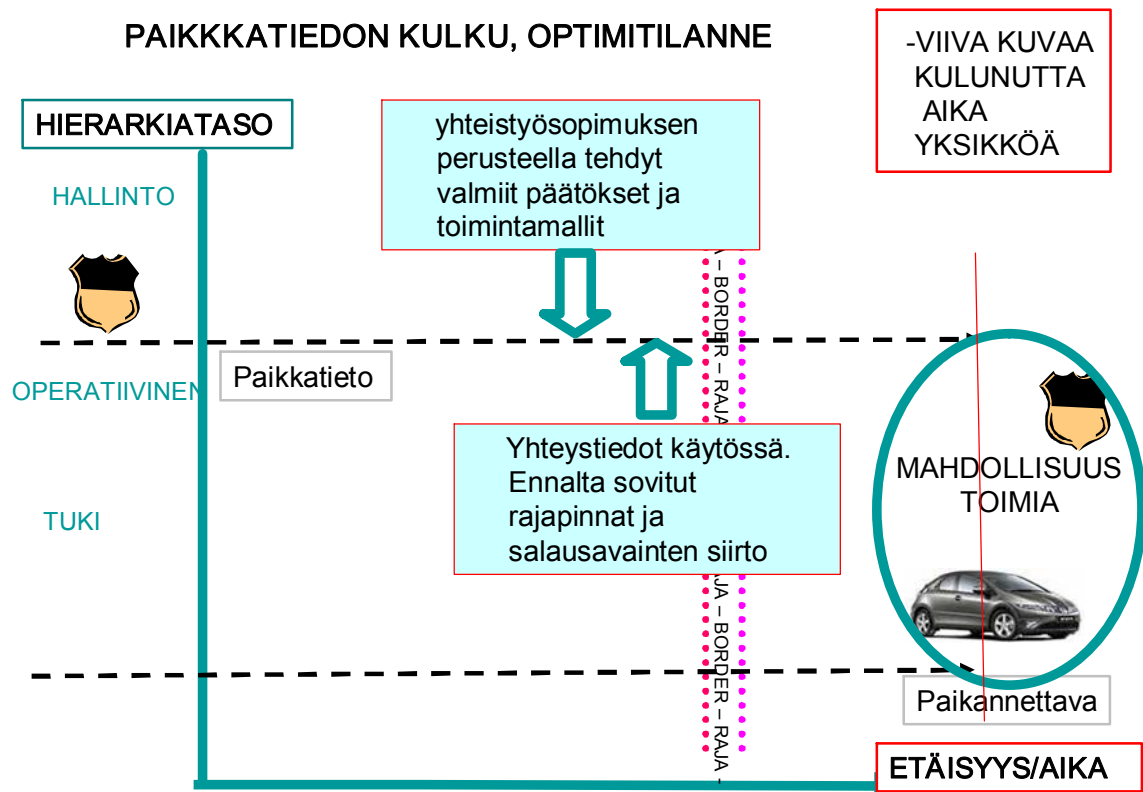
Kuviosta 5. ilmenee kuinka se ettei tieto välity tarpeeksi nopeasti sitä tarvitsevalle taholle aiheuttaa sen että mahdollisuudet jatkotoimenpiteille menetetään. Tiedon siirtyessä lopulta rajan toiselle puolelle, itse kohde on jo päässyt niin kauas, että ei-toivottu tapahtuma on jo voinut hallitsemattomasti käynnistyä.

Monet logistiikkaketjun ja turvallisuusalan operaatiot ovat erittäin aikakriittisiä. Jos tuotettavassa paikkatiedossa on liikaa viivettä, se auttaa vain tapahtuman jälkikäteiseen tarkasteluun, ei mahdollisen ei-toivotun tapahtuman estämiseen, joka olisi monesti taloudellisuuden ja turvallisuuden kannalta selkeästi paras vaihtoehto.

Suomessakin käytetään tärkeiden kuljetusten turvaamiseen paikannusta, jonka tuottama tieto on vain kyseisen yhtiön käytössä. Mahdollisessa hätätilanteessa tieto sitten otetaan järjestelmästä, kerrotaan puhelimella edelleen hälytyskeskukselle, joka välittää sen edelleen puhelimella poliisille tai palokunnalle, joka sitten kenties syöttää sen omaan paikajärjestelmäänsä. <miten kyseinen tiedonvälitysketju toimii jos tilanne onkin liikkuva, kuinka paljon operatiivista toimintaa aiheuttavaa viivettä aiheutuu, ja kuinka paljon virhemahdollisuudet lisääntyvät.

Tekniikan kehitys on huomioitu yksityisellä vartiointiliikepuolella, jossa jo kiivaasti tutkitaan GPS/GIS-järjestelmiin perustuvia tuotteita. Niitä käytettäisiin paitsi oman toiminnan tehos-

tamiseen myös palvelujen myyntiin yksityisille kansalaisille. Osa näistä palveluista on varmasti sellaisia, jotka eivät kuulu viranomaistoiminnan piiriin, mutta joukossa lienee myös tarpeita, joihin viranomaisten pitäisi kyetä vastaamaan.



Kuvio 8.

Kuviosta 6. ilmenee, että optimitalanteessa hallinnolliset päätökset ja yhteistyörakenteet on sovittu etukäteen jo operatiiviselle tasolle asti. Erilaisia skenaarioita on käyty läpi ja on sovittu että määriteltyjen olosuhteiden täytyessä ne voidaan ottaa suoraan käyttöön, konsulttimatta enää johtoa. Tuen puolella on rajapinnat ja yhteystiedot ja mahdollisten salausavainten siirto sovittu etukäteen, eikä aiheuta enää merkittävää viivettä paikkatiedon siirtoon. Sähköinen viesti kiertää maapallon valokaapeleissa muutamassa sekunnissa. Tieto kyllä kulkee riittävän nopeasti, kun hallinnolliset haasteet on voitettu.

## 7.2 EU-rajat ylittävä liikenne

Paikkatieto oli rautaesiripun kaatumiseen saakka monelta osin sotilastietoa ja siten myös salaista. On tutkimatta kuinka monen maan lainsäädännössä on vielä jäänteitä tältä ajalta jotka edelleen kieltävät määrätynlaisen tiedon siirtämisen valtakunnan rajojen yli.

Sotilassalaisuudet eivät ole toisaalta kadonneet minnekään ja vastakkainasettelua on edelleen suurvaltojen välillä. Onko esimerkiksi Venäjän lainsäädännössä vielä kohtia, jotka tekevät ilman Venäjän viranomaisen lupaa tapahtuvasta paikannuksesta lainvastaista?

Jos esimerkiksi GPS:n käyttö on kiellettyä tai luvanvaraista, luoko nykyinen käytäntö, että sitä kuitenkin salaa tehdään uusia riskejä. On täysin eri asia se, että joku toiminta on lainvastaista, mutta siihen ei käytännössä puututa, kuin se, että toiminta on selkeää ja perustuu lainsäädäntöön ja kansainvälisiin sopimuksiin.

Venäjällä on lukuisia esimerkkejä siitä, kuinka tarvittaessa voidaan käytäntöjä kiristää erilaisilla hallinnollisilla määräyksillä.

Lakipohjan puuttuminen saattaa antaa tilaa niin sanotulle kaasuhanadiplomatialle, eli kiristettään toimintaa jossain, jotta saavutettaisiin jossain muussa asiassa etua. Tämän vuoksi on tärkeää selvittää esimerkiksi se, voidaanko venäjällä GPS-paikannusta suorittava ja tiedon EU-alueelle lähettävä rekka takavarikoida?

Kun riskejä ei tiedetä, tai on tiedossa, että paikannuslaitteisto aiheuttaa riskin syyllistyä rikokseen valtion rajan ylityksen yhteydessä, paikannus jää helposti kokonaan tekemättä. Hankkeessa pyritään kartoittamaan riskejä ja pienentämään tai poistamaan ne kokonaan. Tämä voi tapahtua päätelaitteita ja järjestelmiä kehittämällä tai käyttökoulutuksen avulla.

Pääministeri Matti Vanhasen II hallituksen ohjelmassa (LVM. 2008. 7.1) todetaan liikenteestä, että tehokas liikennejärjestelmä ja logistiikka edistävät maan kilpailukykyä ja ylläpitävät hyvinvointia. sekä tukevat ilmastopolitiikkaa. Hallitus haluaa nimenomaan edistää informaatioteknologiaa hyödyntävien palvelujen käyttöönottoa liikenteessä.

SATERISK-projekti parantaa kilpailukykyä ja luo sitä kautta työtä sekä mukana olevissa yrityksissä että laajemmin turvallisuus- ja logistiikka-aloilla. Tarkoituksena on kilpailla toiminnan ja laitteiden laadulla kansainvälisillä markkinoilla. Hankkeen tulokset menevät mukana olevissa yrityksissä heti hyötykäyttöön, laitteiden ja palveluiden asiakkaat ovat jo olemassa. Riskiaroitusten tulokset ovat hyödynnettävissä tätä kautta myös yritysten markkinoinnissa.

Pienet tai keski suuret yritykset, joiden ydinliiketoimintaan satelliittipaikantaminen tai jokin siihen toimintaketjuun kuuluva osa oleellisesti kuuluu, omaavat erittäin rajalliset mahdollisuudet ostaa tai teettää kalliita tutkimuksia ja riskianalyyskejä paikannukseen liittyvistä riskeistä. Projektin kautta näiden yritysten on mahdollista muodostaa entistä kokonaisvaltaisempi kuva satelliittipaikantamiseen liittyvistä riskeistä.

Hallitsemalla satelliittipaikantamiseen liittyvät riskit, voivat satelliittipaikannusta toiminnassaan hyödyntävät yritykset saada suoraa liiketoiminnallista hyötyä. Osalla projektissa mukana olevista yrityksistä on tarkoituksena siirtää viranomais- ja sotilaspuolen paikannuksessa käytettäviä ratkaisuja myös yksityisen turva-alan käyttöön. Näin tehdään mahdolliseksi ratkaisujen kaksoiskäyttö.

Yksittäisten satelliittipaikannusta hyödyntävien tahojen oikeudelliset intressit saattavat toisaalta olla varsin erilaisia kuin valtio-osapuolten tai EU:n ja ESA:n. Näitä Galileoon liittyviä eri tasojen oikeusongelmia on toki tarkasteltu erilaisissa yhteyksissä tähänkin asti, mutta tasoja leikkaavaa tutkimusta on, epäilemättä sen haastavuudenkin vuoksi, ollut niukasti. Näin ollen kokonaisuudesta GALILEON oikeudellisista puitteista ei ole. Tämän projektin oikeudellisessa osuudessa olevassa työpaketissa pyritään osaltaan paikkaamaan tätä puutetta.

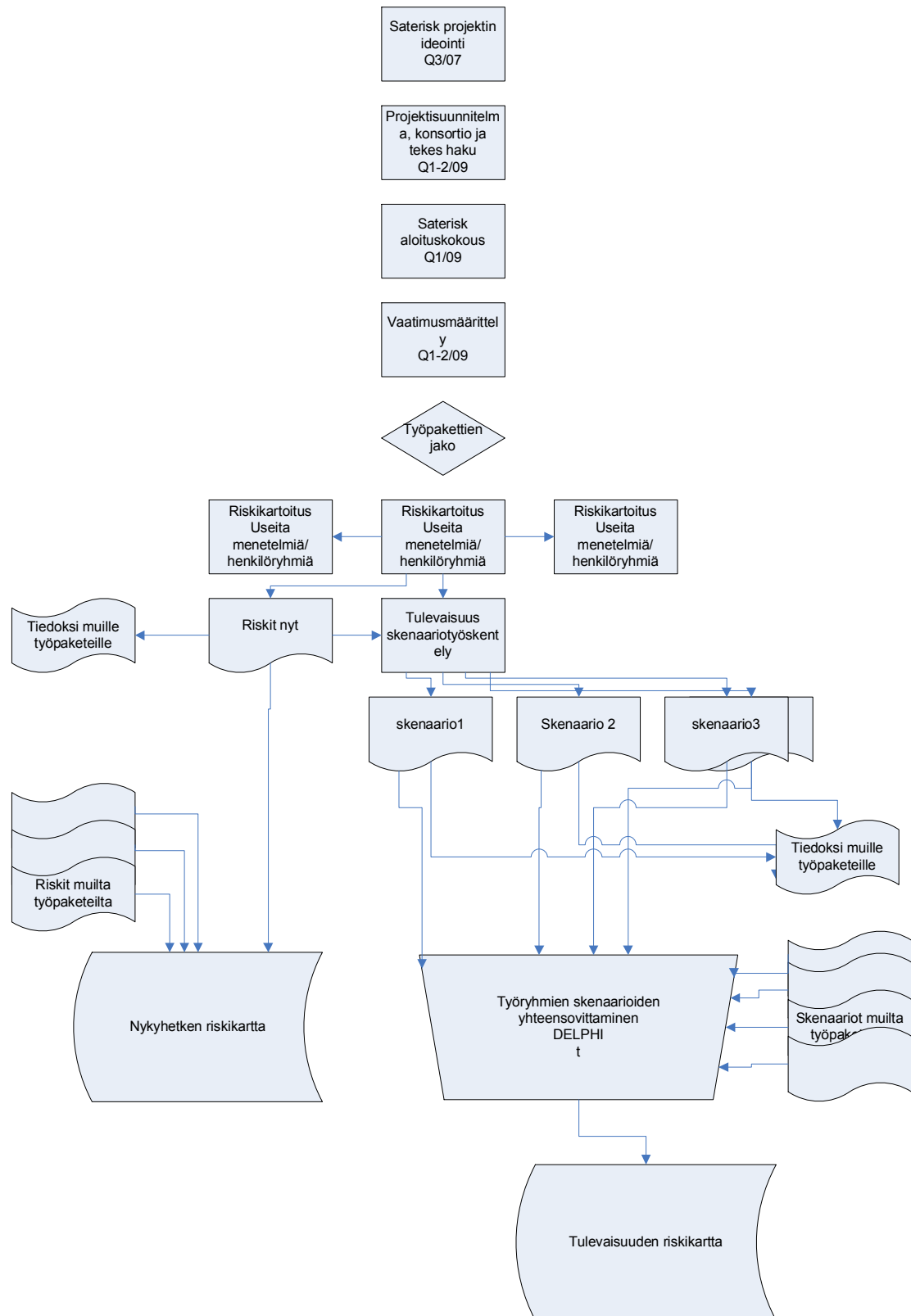
Todennäköisesti tulevaisuudessa osaa projektin tuloksista voidaan hyödyntää myös muuhun kuin turvallisuus- ja kuljetusalan paikannustoimintaan.

Verkottuminen projektiin osallistumista harkitsevien tahojen kesken on alkanut jo haettaessa partnereita tähän projektiin. Projektisuunnitelmaa kirjoitettaessa on selkeästi havaittu viitteitä ja tarvetta siihen, että projektiin osallistuvat tahot tulevat tekemään tulevaisuudessa yhteistyötä myös projektin päätyttyä.

Tämän projektin tulosten odotetaan selvittävän sekä riskit, että kustannukset ja hyödyt erilaisten käyttö- ja laiteskenaarioiden välillä.

Kuvio 9. Saterisk prosessi

SATERISK-projektin prosessi etenee kaaviona seuraavilla tavoilla, joita edellä on kuvattu.





### 7.3 Samantyyppisiä projekteja muualla maailmassa

Yhdysvalloissa on menossa FMCSA:n ( Federal Motor Carrier Safety Administration) CSA 2010 ( comprehensive Safety Analysis 2010) tutkimus jossa valtion ja yritysten tavoitteena on vähentää ammattiliikenteen kolareita, kuolonuhreja ja loukkaantumisia.

Kyseinen hanke tulee tutkimaan mm paikannuksen vaikutuksia seitsemän eri kategorian kautta, jotka ovat, vaarallinen ajotapa, väsynyt kuljettaja, ajajan fyysinen kunto, alkoholi, huumet, ajoneuvojen huolto, tavarantoimittajien lastaus ja kiinnitys, kolarit.

Tavoitteena on saada paljon lisää tietoa, jonka perusteella voidaan etsiä vaaralliset käytännöt ja puuttua näihin.

### 7.4 Tavoitteet, linjat ja odotettavissa olevat tulokset

Paikannusta tehdään maailmanlaajuisesti, mutta sitä ei ole lainsäädännössä useinkaan tarkasti määritelty. Tästä syystä SATERISK on enemmän riskikeskeinen kuin lainsäädäntökeskeinen. Useissa maissa, joissa paikannusta suoritetaan, on kuitenkin lainsäädäntöä, joka koskee yksityisyyden suojaa tai valtion turvallisuutta. Yritys ja varsinkin toisen maan viranomainen ei voi syyllistyä luvattomaan toimintaan toisen valtion alueella, sillä mahdollinen selkkaus voi johtaa keskusteluihin korkealla diplomaattisella tasolla eikä välttämättä siinä hengessä joka edesauttaisi tulevaisuudessa yhteistoimintaa.

Tämän vaatimusmäärittelyn tarkoitus on varmistaa, että SATERISK-projekti tuo viranomaispuolelle uutta tietoa, miten varmistaa toiminnan turvallisuus, laillisuus ja läpinäkyvyys. Keskeistä laillisuuspuolella on omien kansalaisten oikeusturva, sekä miten estää paikannuslaitteistoilla tapahtuva toisten valtioiden suvereniteetin loukkaukset.

Käytännön puolella taas on tarkoituksena saada käsitys järjestelmien haavoittuvuuksista, joita esimerkiksi rikolliset voisivat käyttää hyväksi. Tältä pohjalta nousevat taas ne uudet keinot joilla estää rikollisten vastatoimenpiteet. Tarkoitus on myös näin luoda perustietoa siitä mihin suuntaan tulevaisuudessa tehtäviä suurempia tilannekuvajärjestelmiä tulisi rakentaa

Yksityisellä puolella projektin avulla varmennetaan erilaisten toimijoiden mahdollisuuksia käyttää paikannus sovellutuksi ilman pelkoa tunnistamattomista oikeudellisista riskeistä. Esimerkiksi Venäjällä pienikin epäselvyys viranomaisten kanssa voi aiheuttaa paljon viivettä ja esimerkiksi kuorman pilaantumisen, tai pahimmillaan kuljetuskaluston joutumisen takavarikkoon.

Tässä vaatimusmäärittelyssä ei ole tarkoituksella menty tarkkoihin teknisiin, lainsäädännöllisiin ja käyttöä koskeviin vaatimuksiin. Sekä innovaatiot, että piilevät ongelmat sijaitsevat usein erilaisissa rajapinnoissa, ”ei kenenkään maalla”. Tällä määrittelyllä on pyritty saamaan liukuvia rajoja. Tarkoitus on että eri ryhmät tekevät samoja asioita, mutta hieman eri näkökulmista.

## 8 Seuraavat kehittämis- ja tutkimuskohteet

SATERISK-projektin aihepiiriä on tässä työssä voitu käsitellä vasta varsin pinnallisesti. Jo tässä vaiheessa on kirjoittajalle kuitenkin muodostunut käsitys siitä, että tämän aihepiirin jatko tarkastelulle on tilausta.

Tutkimusta tulee myöhemmässä vaiheessa jatkaa erilaisten verkkopaikannus teknologioiden suuntaan. Näitä voivat olla erilaiset yleiset radioverkot, kuten GSM ja virve, tai sitten hyvin pienet ja paikalliset esim. WLAN; BT, ZIG BEE teknologiaan perustuvat paikannus-sovellutukset. Varsinkin logistiikan puolella pienempien kollien RFID:t ilmoittautuvat kuljetusalustan paikannuslaitteelle joka sitten tulee toimimaan paikkatiedon lähteenä.

Uusien tekniikoiden tulo kuvaan mukaan avaa myös uusia laillisuuskysymyksiä, joihin tulee löytää vastauksia.

## Lähteet:

Airos, E. Korhonen, R. & Pulkkinen, T. 2007. satelliittipaikannusjärjestelmät. Puolustusvoimien tekninen tutkimuslaitos.

Anttila, P. 2000: Tutkimisen taito ja tiedon hankinta. Helsinki: Akatiimi

Beck, U. 1996. Risk Society. London: Sage

Brown, P. 2008. Number Of Factors May Impede Situational Awareness. Satellite Today, viitattu 15.3.2009.

<http://www.infowarmonitor.net/modules.php?op=modload&name=News&file=article&sid=2136>

Charmaz, K. 2006. Constructing Grounded Theory, London: Sage

Cohen, L., Manion, L. & Morrison, K. 2002. Research Methods in Education, London: Routledge Falmer.

Eduskunta. Prömin sopimus. Viitattu 21.4.2009

<http://217.71.145.20/TRIPviewer/show.asp?>

Elinkeinoelämän Keskusliitto, EK. 2009. rikosriskit-työkortti. Viitattu 29.3.2009  
tunniste=HE+243/2006&base=erhe&palvelin=www.eduskunta.fi&f=WOR

Elinkeinoelämän keskusliitto, EK. 2009 Pk -yrityksien riskienhallinta. 1998. viitattu 12.3.2009  
<http://www.pk-rh.com>

Euroopan yhteisöjen komissio. 2008. EUROSUR. Viitattu 21.5.2009  
<http://europa.eu/scadplus/leg/fi/lvb/l14579.htm>

Euroopan yhteisöjen komissio. 2007. huumausaineita koskeva EU:n tiedoksianto KOM 2007 781. viitattu 11.2.2009.  
[http://ec.europa.eu/prelex/detail\\_dossier\\_real.cfm?CL=fi&DosId=196512](http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=fi&DosId=196512)

Euroopan yhteisöjen komissio. 2006. Vihreä kirja satelliittinavigoinnin sovelluksista. Viitattu 23.4.2009 [http://www.tekes.fi/eu/fin/7po/yhteisty/liikenne/com\\_2006\\_gp\\_galileo\\_fi.pdf](http://www.tekes.fi/eu/fin/7po/yhteisty/liikenne/com_2006_gp_galileo_fi.pdf)

European Commission, 2003. The Galilei Project. Viitattu 23.4.2009.  
[http://ec.europa.eu/dgs/energy\\_transport/galileo/doc/galilei\\_brochure.pdf](http://ec.europa.eu/dgs/energy_transport/galileo/doc/galilei_brochure.pdf)

European Commission. 2008. EU energy and transport in figures

RIA Novosti. 21.10.2008. GPS to be banned in Russia. Viitattu 20.11.2008

<http://www.russia-ic.com/news/show/7268/>

Statistical pocketbook 2007/2008. viitattu 12.2.2008.

[http://bookshop.europa.eu/eubookshop/download.action?fileName=KOAB07001ENC\\_002.pdf&eubphfUid=575887&catalogNbr=KO-AB-07-001-ENC](http://bookshop.europa.eu/eubookshop/download.action?fileName=KOAB07001ENC_002.pdf&eubphfUid=575887&catalogNbr=KO-AB-07-001-ENC).

Elinkeinoelämän Keskusliitto, EK. 2009. rikosriskit-työkortti. Viitattu 29.3.2009

<http://www.pk-rh.fi/pdf/rikosriskit-tyokortti>

Elinkeinoelämän Keskusliitto, EK. 2009. SWOT. Viitattu 29.3.2009.

<http://www.pk-rh.fi/riskilajit/liikeriskit/liiketoiminnan-nelikenttaanalyysi-swot>

Elinkeinoelämän Keskusliitto, EK. 2001. yhteiskuntavastuu. Viitattu 22.3.2009

<http://www.ek.fi/arkisto/ekarchive/20010124-144202-178.pdf>

ESA. 2008. Galileo-projekti. Viitattu 30.1.2009

[http://www.esa.int/esaNA/GGG0H750NDC\\_galileo\\_0.html](http://www.esa.int/esaNA/GGG0H750NDC_galileo_0.html)

Federal Motor Carrier Safety Administration. 2004. Hazardous Materials Safety and Security Technology Field Operational Test. Viitattu 26.1.2009. <http://www.fmcsa.dot.gov/safety-security/hazmat/fot/eval-rpt-summary-part5.htm?printer=true>

Gibbons Media & Research, 2009. Compass/Beidou Will Be Complete by 2015. viitattu

15.3.2009. [http://www.insidegnss.com/node/1152#Baseband\\_Technologies\\_Inc\\_](http://www.insidegnss.com/node/1152#Baseband_Technologies_Inc_)

Grönfors, M. 1982. Kvalitatiiviset kenttätyömenetelmät. Juva: WSOY.

Heinonen, S. 2008. Riskikäsitteen moniulotteisuus tulevaisuudentutkimuksessa. Futura 4/2008, 5-16. Viitattu 11.2.2009.

[http://www.tem.fi/files/22698/Yhdyskuntien\\_kestava\\_kehitys.pdf](http://www.tem.fi/files/22698/Yhdyskuntien_kestava_kehitys.pdf)

Heiskanen, E. & Salo, J. 2007. Eettinen Johtaminen. Helsinki: Talentum.

Helsingin Navigaattorit. 2007. Pieni navigaatiosanasto. Viitattu 11.5.2009.

<http://personal.eunet.fi/pp/navis/sanasto.htm>.

Hirsijärvi, S. Remes, P. & Sajavaara, P. 2008. Tutki ja kirjoita.13. painos. Helsinki: Tammi

Kamppinen, M. Raivola, P. Jokinen, P. & Karlsson, H. 1995. Riskit yhteiskunnassa. Jyväskylä: Gaudeamus.

Keskurikopoliisi. 2008. Yrityksiin kohdistuvan ja niitä hyödyntävän

Rikollisuuden tilannekuva. Viitattu 20.4.2009.

[http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/files/Syksy%202008%20tilannekuva/\\$file/Syksy%202008%20tilannekuva.pdf](http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/files/Syksy%202008%20tilannekuva/$file/Syksy%202008%20tilannekuva.pdf)

Larsen, G. 2006. Why megatrends matter. Viitattu 12.3.2009

<http://www.cifs.dk/scripts/artikel.asp?id=1469>

Laki yksityisyyden suojasta työelämässä. SK 13.8.2004/759. viitattu 8.3.2009.

<http://www.finlex.fi>

Lakivaliokunnan mietintö n:o 24 hallituksen esityksestä telekuuntelua ja -valvontaa sekä teknistä tarkkailua koskevaksi lainsäädännöksi LaVM 24/1994

Liikenneministeriö (LVM). 2008. Vanhasen II-hallituksen hallitusohjelma: Liikenteestä, 7.1. viitattu 28.3.2009.

[http://www.lvm.fi/c/document\\_library/get\\_file?folderId=22164&name=DLFE-812.pdf](http://www.lvm.fi/c/document_library/get_file?folderId=22164&name=DLFE-812.pdf)

Mannermaa, M. 2008. Jokuveli. Porvoo: WSOY

Mannermaa, M. 2003. Teoksessa Vapaavuori, M. & Von Bruun, S. 2003. miten tutkimme tulevaisuutta. Tulevaisuuden tutkimuksen seura

Mannermaa, M. 1999. Tulevaisuuden hallinta. Porvoo: WSOY

Masini, E. 1993. Why Futures Studies. London: Grey

Mayhew, C. 2001. The detection and prevention of cargo theft. Australian Institute of Criminology. Viitattu 22.2.2009. <http://www.aic.gov.au/publications/tandi/ti214.pdf>

May, T. 1993. Social Research. Issues, Methods and Processes. Buckingham: Open University Press.

Ruutikainen, P. Inkinen, T. & Tapaninen, U. 2006. Suomen ja Venäjän välinen kuljetuslogistiikka. Turun Yliopisto. Viitattu 20.3.2009

<http://www.merikotka.fi/julkaisut/Kuljetuslogistiikka.pdf>

Meristö, T. 2003. Teoksessa Vapaavuori, M. & Von Bruun, S. 2003. miten tutkimme tulevaisuutta. Tulevaisuuden tutkimuksen seura

Märkälä, M. Jumpponen, J. Arposalo, A & Liedes, M. 2007 TRAKET - Transitoketjujen kilpailukyky -tutkimushankkeen yhteenveto. Lappeenrannan tekninen yliopisto.

[Http:www.lut.fi/en/NORDI/research/finished/traket/Documents/20070627\\_TRAKET\\_yhteenveto\\_fin.pdf](Http:www.lut.fi/en/NORDI/research/finished/traket/Documents/20070627_TRAKET_yhteenveto_fin.pdf)

Niiniluoto, I. 1983, Tieteellinen päättely ja selittäminen. Helsinki: Otava.

Opetushallitus. 2004. PESTE. Viitattu 24.2.2009.

<http://www.oph.fi/SubPage.asp?path=1,438,3086,3987,28363,28396,28397>

Pakkokeinolaki SK 30.4.1987/450 <http://www.finlex.fi>

Poliisilaki SK 7.4.1995/493 <http://www.finlex.fi>

Pölonen, P. 1997. Salaiset pakkokeinot. Vammala: Lakimiesliiton kustannus.

Sihvola, J. 1997. eDelfoi. Viitattu 19.4.2009.

[http://www.edelfoi.fi/fi/nd/delfoi/01\\_delfoi/02\\_teoria/014\\_pedadelfoi?materials:Open=951002&materials:selres=951002](http://www.edelfoi.fi/fi/nd/delfoi/01_delfoi/02_teoria/014_pedadelfoi?materials:Open=951002&materials:selres=951002)

Sisäasiainministeriö. 2006. Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi. Sisäasiainministeriön julkaisuja 15/2006

Sisäasiainministeriö. 2009. Yrityksiin kohdistuvan rikollisuuden tilannekuva. Viitattu 29.3.2009. <http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/pages/9713335D43ED3309C225730C00297606?opendocument>

Tekniikan Sanastokeskus. 2002. Paikannussanasto. Viitattu 3.1.2009

<Http://www.tsk.fi/tiedostot/pdf/paikannussanasto.pdf>

Transported Asset Protection Association (TAPA). 2009. TAPA FSR 2009. Freight Suppliers minimum security requirements. 1.1.2009. Viitattu 4.5.2009.

[http://tapaemea.com/download/public\\_fsr/2009\\_TAPA\\_FSR\\_Final.pdf](http://tapaemea.com/download/public_fsr/2009_TAPA_FSR_Final.pdf)

Tullihallitus, 2008. Jälleenvienti Venäjälle vuonna 2006. Kauppa 2008:M10.

Tupamäki, M. 1999. Valtion rikosoikeudellisen toimivallan ulottuvuus kansainvälisessä oikeudessa. Väitöskirja Helsingin yliopisto.

Turun käräjäoikeuden päätös 19.12.2008. 08/5361 R08/3030. Viitattu 2.3.2009  
<http://www.oikeus.fi/uploads/am45ea.pdf>.

TEM( työ- ja elinkeinoministeriö). 2008. kansallinen innovaatiostrategia. Viitattu 3.3.2009.  
[www.innovaatiostrategia.fi/files/download/Kansallinen\\_innovaatiostrategia\\_12062008.pdf](http://www.innovaatiostrategia.fi/files/download/Kansallinen_innovaatiostrategia_12062008.pdf)

USNO.(United States Naval Observatory) 2009. GPS-system. Viitattu 30.1.2009  
<http://tycho.usno.navy.mil/gpsinfo.html>

Uusikivi, T. 2006. Teknisestä tarkkailusta ja valvotusta läpilaskusta kansainvälisten sopimusten valossa. Poliisiammattikorkeakoulu: Poliisipäällystön tutkinto nro 8 opinnäytetyö

Valtioneuvosto periaatepäätös. 2006.Yhteiskunnan Elintärkeiden Toimintojen Turvaamisen Strategia. Viitattu 13.3.2009.  
[http://www.yett.fi/content/common/yett\\_strategiadokumentti.pdf](http://www.yett.fi/content/common/yett_strategiadokumentti.pdf)

Valtioneuvosto. 2006. Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi. Viitattu 24.4.2009  
[http://www.intermin.fi/intermin/biblio.nsf/8076DEF357461089C2257131002242F5/\\$file/152006.pdf](http://www.intermin.fi/intermin/biblio.nsf/8076DEF357461089C2257131002242F5/$file/152006.pdf)

Vaughan, E. 1997. Risk management. USA: John Wiley & Sons Inc

Vapaavuori, M. & Von Bruun, S. 2003. miten tutkimme tulevaisuutta. Tulevaisuuden tutkimuksen seura

Viestintävirasto. Mittauspöytäkirja häirintälaitteista, 04/2008.

Viikari, L.2007. The Environmental Element in Space Law: Assessing the Present and Charting the Future. Rovaniemi:University of Lapland Printing Centre

Wieggers, K. 2003. Software requirements. Washington: Microsoft Press.

**JULKAISEMATTOMAT LÄHTEET:**

Knuuttila, Juha, yliopettaja. Laurea, haastattelu

Laitinen, Ilkka, pääjohtaja, Frontex, haastattelu

Lindfors, Pentti radiotarkastusyksikön päällikkö, FICORA, haastattelu

Mäkinen, Tapio, myyntipäällikkö, EADS, haastattelu

Nurhonen, Pekka, ylitarkastaja, Haltik, haastattelu

Patama, Pasi, Kehityspäällikkö, TREVOC Oy

Rajamäki, Jyri, yliopettaja. Laurea, haastattelu

Vehmersalo. Kai, tulliylitarkastaja, Tulli, haastattelu

Öörni, Seppo, Liikenneneuvos Liikenne ja viestintäministeriö, haastattelu



## Liitteet:

Liite 1. SATERISK-projektin suunnitelma. Viitanen, J. Ojala, J & Tuomisto, J. 2008

Liite 2. TEKES-rahoituspäätös SATERISK-projektille

Liite 3. JAMMING DETECTION IN THE FUTURE NAVIGATION AND TRACKING SYSTEMS.

Happonen, M. Viitanen, J. Kokkonen, P. Ojala, J. & Rajamäki, J. 2009. Laurea

## Kuviot:

Kuvio 1. SATERISK-projektiin johtanut tapahtumaketju	8
Kuvio 2. Paikannuksen yleiskäsitteet	22
Kuvio 3. Paikkatiedon kulku $\frac{1}{4}$	47
Kuvio 4. Paikkatiedon kulku $\frac{2}{4}$	48
Kuvio 5. Paikkatiedon kulku $\frac{3}{4}$	49
Kuvio 6. Paikkatiedon kulku $\frac{4}{4}$	50
Kuvio 7. Paikkatiedon kulku/kokonaiskuva	51
Kuvio 8. Paikkatiedon kulku, optimitilanne	52
Kuvio 9. Saterisk prosessi	55

Liite 1: SATERISK-projektin suunnitelma

# SATERISK

Projektsuunnitelma (päivitetty 10.2.2009)

© Laurea -ammattikorkeakoulu 2008

## Tiivistelmä

Projektin ensimmäinen vaihe tuottaa riskianalyysin satelliittipaikannuksen vaikutuksista paikannuttajan ja paikannettavan riskeihin paikannuksen käytön, teknisten sovellutusten ja lainsäädännön osalta.

Toisessa vaiheessa tuotetaan kartoitus siitä, mitä tulevaisuuden seurantajärjestelmien ja uuden teknologian tulee mahdollistaa. Tarvitaanko uusia, kenties autonomisia tai interaktiivisia toimintamuotoja, joilla täytetään sekä turvallisuusalan, lainsäädännön, että yksityisyyden suojan edellytykset.

Projekti pyrkii tilanteeseen, jossa paikannukseen ja seurantaan liittyvät lait sekä niiden muodostama liiketoiminnallinen riski eivät estä m2m paikannusta valtiorajojen yli. Projektin aikana tehdyn tutkimustyön tuloksena suomalaiselle turva-alalle syntyy uutta kansainvälisen tason osaamista. Projekti tuo alalle myös uusia toimintamalleja ja ohjaa paikannusalan laite- ja järjestelmätoimittajien tuotekehitystä.

Paikannusta käytetään yleisesti tuottavuuden ja turvallisuuden parantamiseen. Länsimaissa yleisesti käytetty paikannusjärjestelmä GPS saa EU:n Galileosta lähivuosina kilpailijan. Galileon tulevaan paikantamiskäyttöön liittyviä ongelmia pitää kartoittaa nyt, kun se on vielä mahdollista. Projekti pyrkii myös ratkaisemaan ja ennaltaehkäisemään ongelmia GPS- ja Galileo -järjestelmissä uusien teknologisten ratkaisujen avulla.

Projektin asetelma satelliittipaikannuksen suhteen poikkeaa perinteisestä "first person use" tilanteesta, jossa paikannukseen liittyvää tietoa tarjotaan itse paikannuksen toteuttajalle (esim. ajoneuvonavigointi). Tässä projektissa paikannuksella tarkoitetaan etäältä tapahtuvaa valvontaa, optimointia tai seurantaa, jossa kohde on yhteistyöhaluinen, sivullinen tai yhteistyöhaluton.

Projekti sisältää myös erillisen oikeudellisen osion, jonka puitteissa tavoitteena on tarkastella Galileo-satelliittiin liittyviä monitahoisia oikeudellisia kysymyksiä monilla erilaisilla oikeuden tasoilla: kansainvälinen oikeus, eurooppaoikeus, ja valtioiden kansalliset oikeusjärjestykset. Tässä yhteydessä Saterisk- projektissa Venäjän lainsäädäntö tulee ottaa monellakin tasolla huomioon, monesta eri näkökulmasta. Lapin yliopiston ja erityisesti oikeustieteiden tiedekunnan yhteistyösuhteita venäläisiin tutkimuslaitoksiin ja muihin tahoihin voidaan käyttää hankkeen oikeudellisten kysymysten kartoittamiseksi ja selvittämiseksi.

## SISÄLLYS

1	Johdanto .....	Error! Bookmark not defined.
1.1	Projektin taustaa .....	Error! Bookmark not defined.
1.2	Projektin käyttöskenaario .....	Error! Bookmark not defined.
2	Projektin tavoitteet, linjat ja odotettavissa olevat tulokset	Error! Bookmark not defined.
3	Projektin työpaketit .....	Error! Bookmark not defined.
3.1	Työpaketti 1.....	Error! Bookmark not defined.
3.2	Työpaketti 2.....	Error! Bookmark not defined.
3.3	Työpaketti 3.....	Error! Bookmark not defined.
3.4	Työpaketti 4. ....	Error! Bookmark not defined.
4	Projektin aikataulutus.....	75
5	Käytettävissä olevat voimavarat ja organisaatio .....	Error! Bookmark not defined.
6	Budjetti ja rahoitus suunnitelma .....	Error! Bookmark not defined.
7	Projektin laadunvarmennus ja tulokset .....	Error! Bookmark not defined.
8	Projektin riskien arviointi.....	Error! Bookmark not defined.

1	Johdanto
1.1	Projektin taustaa

Satelliittipaikannus ja sen käyttö ovat yksi nopeimmin kasvavista toimialoista. Lissabonin strategian mukaisesti EU ([www.ESA.eu](http://www.ESA.eu)) tekee erittäin huomattavia panostuksia paikantamiseen liittyvien projektien toimintaan. Tästä yhtenä esimerkkinä on Galileo - satelliittipaikannusjärjestelmä. Suurin osa paikannuksesta on ”end user” paikannusta, eli palveluiden etsintää tai ajoneuvonavigointia, mutta paikannusta käytetään myös yleisesti tuottavuuden ja turvallisuuden parantamiseen.

Paikannusta käyttävät viranomaiset ja yksityinen turvallisuusala yleisesti, vaikka siitä arvioidaankin syntyvän riskejä. Tämänkaltaisia riskejä on yksittäisen toimijan erittäin vaikeata kartoittaa, ja monesti vain toivotaan että syntyvät riskit olisivat vaikutukseltaan vähäisempiä kuin ne, joita paikannuksella poistetaan tai pienennetään. Paikannuksesta syntyvät riskit, niiden todennäköisyys ja mahdolliset vaikutuksia tulee olla tiedossa.

Saterisk- projekti käsittelee satelliittipaikannusteknologiaa ja sen käyttöä, mutta myös informaation saattamista luotettavaan, helposti hyödynnettävään muotoon esimerkiksi tilannekuvan luomista varten. Tilannekuvaa tulevat erilaisten ulkoistamistoimintojen jatkuessa tarvitsemaan Suomessa satelliittipaikannusta suorittavien viranomaisten; Poliisin, Tullin, Puolustusvoimien ja Rajavartiolaitoksen lisäksi myös paikannustoimintaa suorittavat yksityiset safety- ja security- sektorien yritykset.

## 1.2. Projektin käyttöskenaario

Riskien kartoituksen tarve on ilmeinen ajatellen kokonaisia aloja, jotka hyödyntävät paikannus-sovellutuksia. Tässä projektissa tehtävän riskikartoituksen pääpainopiste on kuitenkin turva-alalla. Turva-alalla käytetään paikannusta ihmisten, ympäristön ja omaisuuden suojaamiseen, mutta myös tilannekuvasovellutuksiin.

Yksityisellä sektorilla paikannusta käytetään paljon rajat ylittävässä liikenteessä paikantamalla tavaraeriä, laitteita ja esineitä. Julkisella sektorilla paikannusta käytetään usein tilannekuvien luomiseen. Molemmissa tapauksissa paikannuslaitteet saattavat liikkua myös kansallisvaltioiden rajojen yli, jolloin saattaa muodostua riskejä ja haasteita, joita paikantaja ei ole tähän asti kyennyt etukäteen arvioimaan.

Kun riskejä ei tiedetä, tai on tiedossa, että paikannuslaitteisto aiheuttaa riskin syyllistyä rikokseen valtion rajan ylityksen yhteydessä, paikannus jää helposti kokonaan tekemättä. Hankkeessa pyritään kartoittamaan riskejä ja pienentämään tai poistamaan ne kokonaan. Tämä voi tapahtua päätelaitteita ja järjestelmiä kehittämällä tai käyttökoulutuksen avulla.

Hanke parantaa kilpailukykyä ja luo sitä kautta työtä sekä mukana olevissa yrityksissä että laajemmin turvallisuus- ja logistiikka-aloilla. Tarkoituksena on kilpailla toiminnan ja laitteiden laadulla kansainvälisillä markkinoilla. Hankkeen tulokset menevät mukana olevissa yrityksissä heti hyötykäyttöön, laitteiden ja palveluiden asiakkaat ovat jo olemassa. Riskikartoituksen tulokset ovat hyödynnettävissä tätä kautta myös yritysten markkinoinnissa.

Pienten tai keskisuurten yritysten, joiden ydinliiketoimintaan satelliittipaikantaminen tai jokin siihen toimintaketjuun kuuluva osa oleellisesti kuuluu, omaavat erittäin rajalliset mahdollisuudet ostaa tai teettää kalliita tutkimuksia ja riskianalyyskejä paikannukseen liittyvistä riskeistä. Projektin kautta näiden yritysten on mahdollista muodostaa entistä kokonaisvaltaisempi kuva satelliittipaikantamiseen liittyvistä riskeistä.

Hallitsemalla satelliittipaikantamiseen liittyvät riskit, voivat satelliittipaikannusta toiminnassaan hyödyntävät yritykset saada suoraa liiketoiminnallista hyötyä. Osalla projektissa mukana olevista yrityksistä on tarkoituksena siirtää viranomais- ja sotilaspuolen paikannuksessa käytettäviä ratkaisuja myös yksityisen turva-alan käyttöön. Näin tehdään mahdolliseksi ratkaisujen kaksoiskäyttö.

Yksittäisten satelliittipaikannusta hyödyntävien tahojen oikeudelliset intressit saattavat toisaalta olla varsin erilaisia kuin valtio-osapuolten tai EU:n ja ESA:n. Näitä Galileoon liittyviä eri tasojen oikeusongelmia on toki tarkasteltu erilaisissa yhteyksissä tähänkin asti, mutta tasoja leikkaavaa tutkimusta on (epäilemättä sen haastavuuden vuoksi) ollut niukasti. Näin ollen kokonaisesitystä Galileon oikeudellisista puitteista ei ole. Tämän projektin oikeudellisessa osuudessa olevassa työpaketissa pyritään osaltaan paikkaamaan tätä puutetta.

Todennäköisesti tulevaisuudessa osaa projektin tuloksista voidaan hyödyntää myös muuhun kuin turvallisuus- ja kuljetusalan paikannustoimintaan.

Verkottuminen projektiin osallistumista harkitsevien tahojen kesken on alkanut jo haettaessa partnereita tähän projektiin. Projektisuunnitelmaa kirjoitettaessa on selkeästi havaittu viitteitä ja tarvetta siihen, että projektiin osallistuvat tahot tulevat tekemään tulevaisuudessa yhteistyötä myös projektin päätyttyä.

## 2. Projektin tavoitteet, linjat ja odotettavissa olevat tulokset

Projektissa pyritään selvittämään tuoko kansainvälinen lainsäädäntö tai sen puuttuminen en-tuudestaan tuntemattomia tai tunnistamattomia riskejä paikantajan toimintaan. Riskien etsimisessä hyödynnetään mukana olevien eri turva-alan toimijoiden vankkaa osaamista. Projektissa tarkastelukulmana on paikannusta suorittavan tahon näkökulma.

Projektissa tullaan keskittymään enemmän riskeihin kuin lainsäädäntöön, koska regulaatio ei ole pysynyt teknisen kehityksen tahdissa. Paikannusta tehdään maailmanlaajuisesti, mutta sitä ei ole lainsäädännössä useinkaan tarkasti määritelty. Useissa maissa, joissa paikannusta suoritetaan, on kuitenkin lainsäädäntöä, joka koskee yksityisyyden suojaa tai valtion turvallisuutta. Viranomainen ei voi syyllistyä luvattomaan toimintaan toisen valtion alueella, sillä selkkaus voi johtaa keskusteluihin korkealla diplomaattisella tasolla.

Projektin avulla varmennetaan sekä julkisen että yksityisen sektorin toimijoiden mahdollisuuksia käyttää paikannussovellutuksia ilman pelkoa tunnistamattomista oikeudellisista riskeistä.

## 3. Projektin työpaketit

### 3.1 Työpaketti 1.

Projekti aloitetaan vaatimusmäärittelyllä, jota tehtäessä käytetään mm. ohjausryhmässä toimivien asiantuntijoiden ja ulkomaisten kontaktien apua. Näiden jälkeen eri käyttötapauksista toteutetaan (esim. kuva sivu 7) mallinnus, joka hyödyttää työpaketissa kaksi tehtävää riskianalyysia. Työpaketti yksi pitää sisällään myös projektin hallinnollisen puolen, tiedotukselliset seikat sekä syntyvien teknologisten tuotosten ensiarvioinnin.

Projektissa toimivat yhteistyöorganisaatiot ovat Laurea -ammattikorkeakoulu ja Lapin yliopiston oikeustieteiden tiedekunta. Projektin ulkomaisina yhteistyökumppaneina toimivat prof. Andrei Rybin / ITMO (IT-, mekaniikka- ja optiikkayliopisto) Pietarissa Venäjällä sekä H. Chen / Arizonan yliopiston Artificial intelligence laboratorio USA:ssa. Yhteistyötä tullaan myös tekemään tohtori

Mark Buttonin (University of Portsmouth, Institute of Criminal Justice Studies) sekä prof. Martin Gillin (Director, Perpetuity Research & Consultancy International Ltd) kanssa.

Projektin rahoituksessa mukana olevien yritysten ja yhteistyötahojen edustajien lisäksi projektin ohjausryhmässä toimivat äänivallattomina asiantuntijoina Kalle Pikkarainen / FICORA, Seppo Öörni / Liikenne ja Viestintäministeriö ja Erkki Väätäinen / Suomen Ulkoministeriö. Johtajatasolla käydyissä keskusteluissa projektille on myös luvattu edustetuilta tahoilta työresursseja.

Työpaketti yksi vastaa tiedottamisen lisäksi myös projektin laadunvalvonnasta. Laadunvalvontaan liittyy jatkuva ja tehokas tiedottaminen projektissa mukana olevien organisaatio- ja toimijatahojen välillä.

### 3.2 Työpaketti 2.

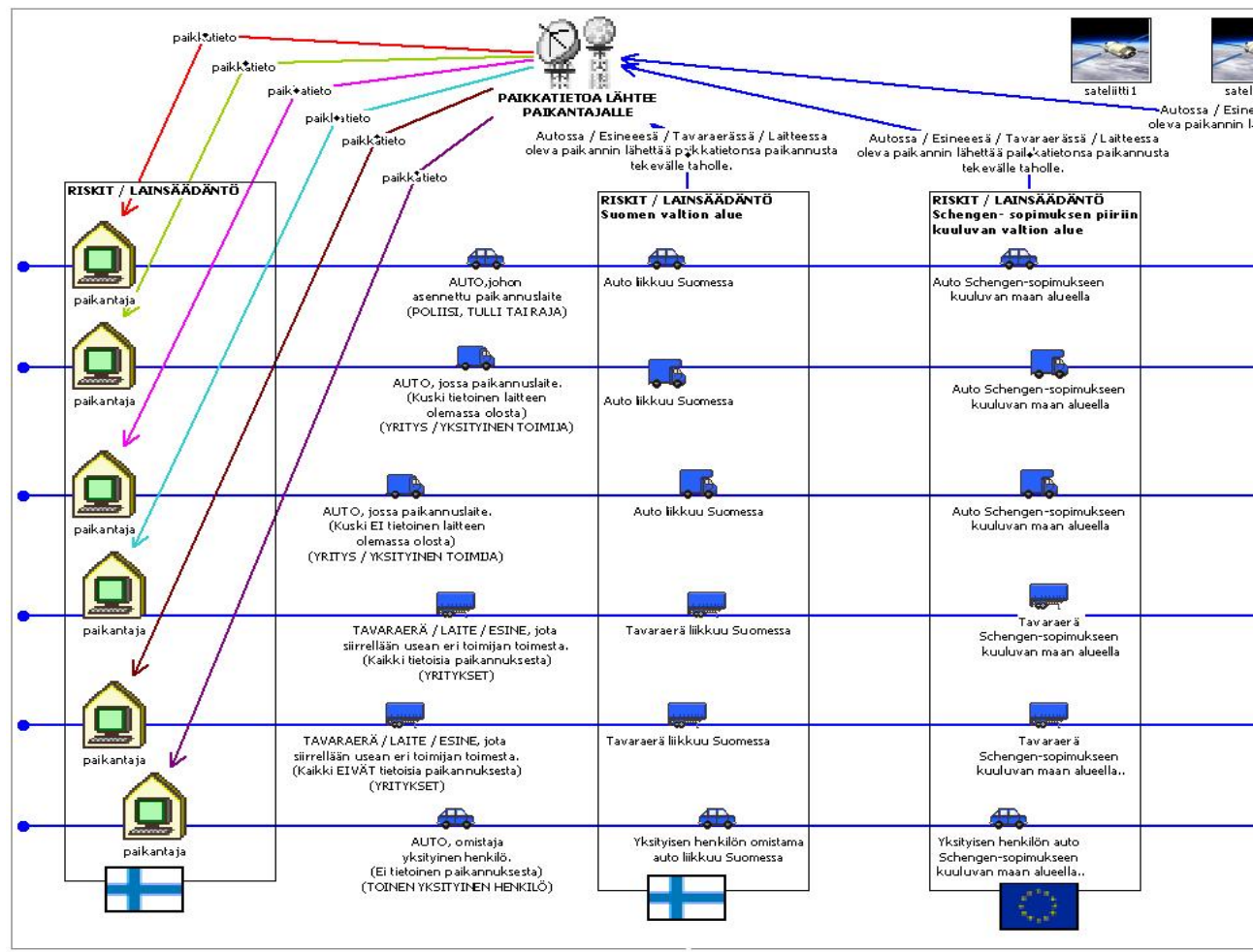
Riskianalyysi satelliittipaikannuksen vaikutuksista paikannuttajan ja paikannettavan oikeudelliseen asemaan ja sitä kautta riskeihin lainsäädännön, paikannuksen käytön ja teknisten sovelutusten kautta.

Vaikuttaako se, että paikannetaan kuljetuksessa olevaa arvokasta laitetta ajoneuvon kuljettajan tieteen vai siitä tietämättä? Onko sillä eroa, että toimiiko paikannuttajana viranomainen, yritys tai yksityinen henkilö?

Esimerkiksi; onko mahdollista, että paikannettavan kohteen seuranta vieraan maan alueella on kyseisen maan lakien mukaan rangaistavaa toimintaa? Telematikan tarjoamin keinoin paikannuksen kohde ja tiedon hyödyntäjä voivat olla eri valtioissa. Tiedon reaaliaikainen jakaminen voidaan toteuttaa kolmannen osapuolen kesken, sitä sen tarkemmin arvioimatta.

Kaikissa maissa on lähes poikkeuksetta lainsäädäntöä, joka koskee yksityisyyden suojaa tai valtion turvallisuutta. Mitä se voi aiheuttaa? Rikotaanko kuljettajan yksityisyyttä? Voiko paikakatieto joutua väärin käsiin? Pitäisikö tiedonsiirron yksityisyyden suojan nimissä olla salattua ja autentikoitua? Kuinka käsitellä ja tallentaa paikannuksesta satua tietoa? Mitä vaikutuksia sillä on, jos tieto on tuotettu mahdollisesti lainsäädäntöä rikkomalla?





### esimerkkitapaus 1:

Suomen viranomaisten seurantalaitteella Suomessa seuraama venäläinen huumausainekauppias liikkuu autollaan Schengen alueen läpi Moskovaan. Syyllistyykö suomalainen seurannan määrännyt ja siitä vastuussa oleva henkilö laittomaan tiedustelutoimintaa Venäjän federaation alueella, jos seuranta jatkettaisiin myös Venäjän valtion rajojen sisällä ilmoittamatta asiaa kyseisen maan viranomaisten edustajalle?

### esimerkkitapaus 2:

Suomesta lähtevä rekka, jonka kuorma sisältää arvokasta elektroniikkaa. Kuljetuksesta vastaava liike seuraa satelliittipaikannuksen avulla rekan kulkemista Viron kautta Venäjälle tavaravastaanottajalle. Kuljettaja on joko tietoinen paikannuksesta tai sitten ei ole tietoinen kuljetuksen paikannuksesta. Onko kyseisellä seikalla vaikutusta arvioitaessa paikannustietoa saavan yrityksen toimintaa?

Seurantälähetin tietää oman paikkansa metrien tarkkuudella, mutta nykyiset taustajärjestelmät eivät kuitenkaan reagoi kansallisvaltioiden rajojen ylityksiin komentamalla lähetintä pois päältä tai sellaiseen toimintamoodiin, jolla ei rikota em. maan lakeja.

Mitä riskejä satelliittipaikannuksesta aiheutuvat riskit voivat aiheuttaa yrityksen liiketoiminnan kannalta siten, että ne muodostuvat liiketoimintariskeiksi?

Ensimmäisessä vaiheessa on mukana käytön ja lainsäädännön lisäksi myös järjestelmien tekniikka ja niiden haavoittuvuudet, sekä kartoitus satelliittipaikannuksen häirintälaitteiden käytön nykytilasta.

2.työpaketti osa 1.	2.työpaketti osa 2.	2.työpaketti osa 3.
<b>LAINSAADÄNTÖ:</b>	<b>KÄYTTÄMINEN:</b>	<b>TEKNIikka:</b>
Regulaatio	käyttötavat	autentikointi
Yksityisyydensuoja	käyttökulttuuri	salaus
Säännökset	valvonta	eheys
Sopimukset	ominaisuudet	oikeudellisuus
Tulkinta	rekisterit	häirintäalttius
Puutteellisuus	tallennukset	yhteensopivuus
olemassa olo	koulutus	toimivuus

Osaamista näiden riskien kartoittamiseen haetaan mukana olevilta yhtiöiltä, mutta myös mukana olevien viranomaisten taajuusvalvontaviranomaisen Ficora (Viestintävirasto) osaamisesta.

### 3.3 Työpaketti 3.

Nykyiset seurantalaitteet tuottavat paikkatietoa yleensä NMAE:formaattissa ja sitä lähetetään edelleen paikantajan karttajärjestelmään lähes riippumatta siitä missä tai millaisissa olosuhteissa laitteistoa käytetään.

Toisen vaiheen tavoitteena on luoda asiantuntijoiden yhteinen näkemys siitä, mitä uusia, kenties autonomisia tai interaktiivisia toimintamuotoja laitteissa ja järjestelmissä tulee olla, jotka täyttävät sekä turvallisuuden, lainsäädännön, että yksityisyydensuojan vaatimukset.

Laitteiden ja järjestelmien suorittamien analyysien autonomisten ratkaisujen tulee tukea turvallisuusalan toimijoiden työntekeä. Paikannuksen nykyisin toteuttavat sensorit eivät sisällä useinkaan autentikointia tai salausta. Onko mahdollista luoda järjestelmälle autonominen tietoisuus laittoman tilan kohtaamisesta?

Työpaketti 3 täydentyy työpaketti 2. valmistumisen jälkeen.

osa 1. satelliittijärjestelmän ratkaisut

osa 2. päätelaitteiden uudet ratkaisut

osa 3. taustajärjestelmien uudet ratkaisut

### 3.4 Työpaketti 4.

Erillisessä oikeudellisessa osassa pyritään tarkastelemaan Galileoohon liittyviä oikeudellisia kysymyksiä. Galileo on oikeudellisesti varsin monimutkainen konstruktio jo EU:n ja ESA:n välillä. Sen rooli uraauurtavana public-private partnership -hankkeena tuo sekin mukanaan merkittäviä oikeudellisia haasteita. Toisaalta yksityisen ja julkisen sektorin rajanveto Galileon yhteydessä on jo sinänsä vaikeaa; yksittäinen toimija voi toimia toisaalta yksityisessä roolissa, toisaalta myös julkisen vallan harjoittajana. Kansainvälisen oikeuden näkökulmasta julkisen vallan harjoittamisen ja yksityisluontoisen esim. taloudellisen toiminnan erottelu on merkittävää erityisesti oikeudellisissa konflikteissa, joissa kansainvälisen oikeuden subjektit (erit. valtiot) voivat immuniteettiinsa vedoten kieltäytyä ylipäätään osallistumasta oikeusprosesseihin - eivät välttämättä kuitenkaan, milloin kyseessä ei ole valtiovallan harjoittaminen vaan valtiojohtoinen liiketoiminta. Vaikka immuniteettisuoja ei osoittautuisikaan ongelmaksi, ratkaisujen täytäntöönpano voi olla vaikeaa, jopa mahdotonta.

On selvää, että taloudellisesti ja poliittisesti erittäin merkittävässä Galileon kaltaisissa hankkeissa järjestelmän oikeudellinen ennakoitavuus on kuitenkin erittäin tärkeää kaikkien kannalta. Erityisen merkittävää se on yksityisen sektorin näkökulmasta. Tässä suhteessa olennaisinta on toimivien - ja toiminnaltaan riittävästi ennakoitavissa olevien - riitojenratkaisu- ja varsinkin riitojenekäisymekanismin olemassaolo. Oikeudellisten riitojen syntyä estää osaltaan tietenkin järjestelmän oikeudellinen toimivuus ja kattavuus ylipäätään.

Jo tällä hetkellä hyvin perustavanlaatuiset, koko Galileon toimintaan liittyvät kysymykset ovat kuitenkin osoittautuneet haasteellisiksi, esimerkiksi EU:n ja ESA:n välinen satelliittipaikannusjärjestelmää koskeva päätöksenteko ja järjestelmän ylätasoon oikeudellinen kokonaisrakenne. Paikannusjärjestelmän käytännön toiminnassa tulee nousemaan esiin vielä lukuisia yksityiskohtaisempia oikeudellisia kysymyksiä, koskien esimerkiksi yksityisyydensuojaa, sopimussitovuutta, kuljetusoikeutta, oikeusinformatiikkaa, erilaisia vastuukysymyksiä, valtiosuvereniteettiin liittyviä näkökohtia ja valtiosopimusoikeutta.

Epäilemättä Galileo tulee johtamaan vielä täysin ennakoimattomiinkin oikeudellisiin ongelmiin. Tämän projektin puitteissa on tavoitteena tarkastella tähän mittavaan hankkeeseen

liittyviä erilaisia oikeudellisten kysymysten tasoja, niiden välisiä yhteyksiä ja haasteita, sekä tarjota mahdollisuuksien mukaan oikeudellisia ratkaisuvaihtoehtoja olemassa oleviin ja tulevaisuudessa konkretisoituihin ongelmiin.

Saterisk- projektissa Venäjän oikeus tulee ottaa monellakin tasolla huomioon monesta eri näkökulmasta. Kansainvälisen oikeuden alalla yksi tärkeimpiä venäläisiä tutkimuslaitoksia on Kansojen ystävyysyliopisto Moskovassa, jonka kanssa Lapin yliopiston OTK:lla on yhteistyösopimus. Avaruusoikeuteen erikoistuneen professorin G.P.Zkukovin arvio kv-avaruusoikeuden kehitystendensseistä 1990- ja 2000-luvuilla saattaa olla hyvinkin relevantti hankkeen kannalta. Zkukovin mukaan kv- avaruusoikeus etenee kansallisen lainsäädännön tasolla, mutta ei niinkään kansainvälisen oikeuden tasolla, eikä esim. YK:n avaruussopimus v.1967 ole viime vuosina saanut riittävästi huomiota osakseen.

LY:n OTK:n yhteistyöpartnereista toinen varteenotettava tämän hankkeen kannalta on Venäjän tiedeakatemian Valtio- ja oikeuslaitos, jossa mm. on äskettäin tutkittu avaruudesta käsin tapahtuvaa merenkulun ohjausta. Laitoksella on pitkät perinteet avaruusoikeudesta, mutta myös vankkaa asiantuntemusta esim. ulkomaankaupan ja yritystoiminnan juridiikasta ja kaikilta oikeuden aloilta. Laitoksen asiantuntijat osallistuvat Venäjän lainsäädännön valmisteluun kaikilla tasoilla.

Lapin yliopistolla on myös tiivistä tutkimusyhteistyötä venäläisten yliopistojen kanssa, mm. suomalainen opiskelija on tekemässä tohtorinväitöskirjatutkimusta kaksoistutkintona taloudellisesta rikollisuudesta Venäjällä ja Suomessa. Hankkeen turva-aspektiin löytyy muitakin kontakteja OTK:n henkilöstöltä Venäjälle, mm. Niznij Novgorodin Turvallisuusakatemiaan. Venäjän oikeuteen liittyviä pro gradu-tutkimuksia on myös käynnistynyt suomalaisen liike-elämän kanssa tiiviissä yhteistyössä mm. rakentamisen ja metsätalouden alalla, mitkä ovat Saterisk-projektin kannalta kiinnostavia. Lapin yliopiston ja Oulun yliopiston yhteistyönä v.2009 alkaa kahdeksan Luoteis-Venäjällä olevan yliopiston kanssa rajat ylittävä yliopistollinen koulutusyhteistyö (BCBU - Barents Cross Border University ) neljällä maisteriohjelmalla, joista mm. vertailevan sosiaalityön ohjelma on Saterisk-projektille mielenkiintoinen sovellutuskenttä esim. dementoituneiden henkilöiden valvontajärjestelmien osalta.

#### 4 Projektin aikataulutus

VAIHE	kevät/09	syksy/09	kevät/10	syksy/10	kevät/11
tp 1. valmistelu, järjestely ja laadunvarmennus, VAATIVUUSMÄÄRITTELY, tehdään keväät09	1	1,5	1	1,5	1
2 tp. osa 1 riskianalyysi lainsäädäntö	5				
2 tp. osa 2. riskianalyysi käyttäminen	2	3			
2 tp. osa 3. riskianalyysi tekniikka		5			
kaupallisten sovellustusten suunnittelu		1	1,5		
väliraportti työpaketeista 2 (osat 1-3)		1	4		
kaupallisten sovellustusten testaus			1	1	
3 tp. osa 1. sateliittijärjestelmän ratkaisut			5		
3 tp. osa 2. päätelaitteiden uudet ratkaisut				5	
3 tp. osa 3. taustajärjestelmien uudet ratkaisut				5	
4 tp. Oikeudellinen osio (Lapin yliopisto OTK)					
projektin loppuraportti				2	6
ensimmäiset kaupalliset sovellutukset myynnissä				1	1,5
projektinhallinto (sisältyy tp 1)					

**Rahoituksen kautta henkilötyökuukautta (htk)  
yhteensä:**

**8      11,5      12,5      15,5      8,5**

Projektin eri vaiheiden kohdalla esitetty luku kuvastaa arvioita kyseiseen toimintaan käytettyä työajasta henkilötyökuukausina

Kyseisissä luvuissa ei ole huomioitu projektissa mukana olevien yritysten siihen asettamia työpanostuksia.

Projektin tiettyyn vaiheeseen erityisesti osallistuvat yritykset:

Projektin aloitukseen ja ensimmäiseen vaiheen riskikartoitukseen (osa tp 1), jossa malliesimerkkien kautta kartoitetaan mahdolliset potentiaaliset riskit (poa), osallistuvat sekä kaikki yritykset (paikannusketjun toimijat), että asiantuntijat.

VAIHE	kevät/09	syksy/09	kevät/10	syksy/10	kevät/11
tp 1. valmistelu, järjestely, laadunvarmennus ja vaativuusmäärittely kevät09	Laurea	Laurea	Laurea	Laurea	Laurea
2 tp. osa 1 riskianalyysi lainsäädäntö	Lapin YO Ficora LVM UM				
2 tp. osa 2. riskianalyysi käyttäminen	Ficora LVM Loomis Trevoc Portalify Tulli	Ficora LVM Loomis Trevoc Portalify Tulli			
2 tp. osa 3. riskianalyysi tekniikka		Ficora EADS Trevoc Tulli			
kaupallisten sovellustusten suunnittelu		EADS Trevoc Portalify Loomis	EADS Trevoc Portalify Loomis		
väliraportti työpaketeista 2 (osat 1-3)		Laurea Lapin YO	Laurea Lapin YO		
kaupallisten sovellustusten testaus			EADS Portalify Trevoc Loomis Tulli	EADS Portalify Trevoc Loomis Tulli	
3 tp. osa 1. sateliittijärjestelmän ratkaisut			EADS		
3 tp. osa 2. päätelaitteiden uudet ratkaisut			EADS Trevoc		
3 tp. osa 3. taustajärjestelmien uudet ratkaisut				Portalify	
4 tp. Oikeudellinen osio	Lapin yliopisto OTK	Lapin yliopisto OTK	Lapin yliopisto OTK	Lapin yliopisto OTK	Lapin yliopisto OTK
projektin loppuraportti				Laurea Lapin YO	Laurea Lapin YO
ensimmäiset kaupalliset sovellutukset myynnissä					
Projektinhallinto	Laurea	Laurea	Laurea	Laurea	Laurea

## 5 Käytettävissä olevat voimavarat ja organisaatio

Laurea -ammattikorkeakoulu: Suomen neljänneksi suurin monialainen ammattikorkeakoulu, joka toimii Uudellamaalla. Laurean erityisosaamisalueet ovat hyvinvointi, palveluliiketoiminta ja yhteiskuntavastuu.

Lapin yliopisto, oikeustieteiden tiedekunta: Lapin yliopisto on kansainvälinen opetuksen ja tutkimuksen keskus, jonka yksi osa on oikeustieteiden tiedekunta. Yliopiston tutkimus on vahvaa eri aloilla, kuten oikeuslingvistiikassa, oikeusinformatiikassa ja avaruusoikeudessa. Yliopisto koordinoi myös yli sadan arktisen tutkimus- ja koulutusinstituution verkostoa.

EADS: Kansainvälinen ilmailu ja puolustusalan suuryritys

Fastrax: Maailmanlaajuisesti toimittaa OEM GPS -vastaanottimet ja -paikantimet, satelliittipaikantimet ja -antennit.

Trevoc Oy: EU-viranomaisille teknisen tiedustelun laitteita valmistava Pk-yritys.

Loomis: Erikoistunut kaupan ja pankkien rahahuoltoon, arvokuljetuksiin, käteisturvapalveluihin sekä tietotallenteiden säilytykseen, alan suuri kansainvälinen toimija.

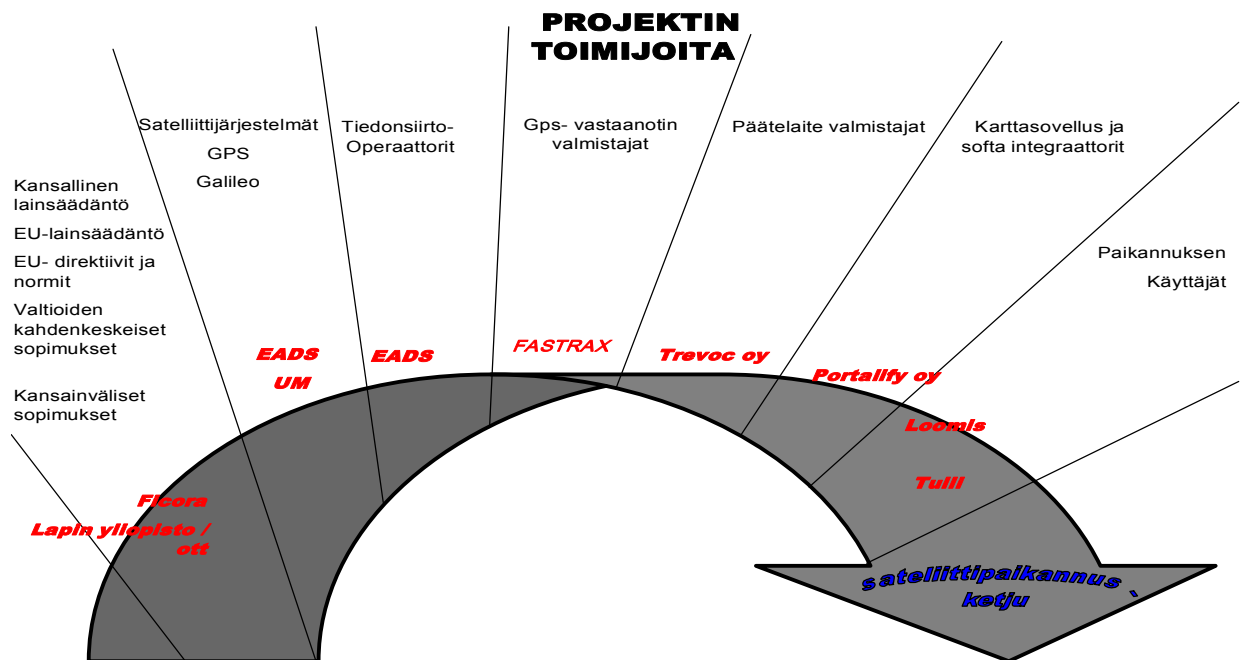
TULLI: Koko maan kattava EU:n sisä- ja ulkokaupan verotus-, valvonta- ja palveluorganisaatio, joka toteuttaa EU:n yhteistä tullipolitiikkaa.

Ficora: Suomen taajuus ja radiovalvonta viranomaisen

UM: Suomen ulkoministeriö, vastaa mm. NSA tehtävistä

Saterisk- projektin osallistuvat tahot kattavat kaikki satelliittipaikannusketjun osa-alueet.

Galileo- satelliittien valmistuksessa mukana olevasta EADS:stä paikannuksen security- sovelluksia käyttävin kuljetusliikkeisiin.



Projekti toteutetaan kahden tutkimusorganisaation yhteistyönä. Yhteistyöorganisaatiot ovat Laurea -ammattikorkeakoulu ja Lapin yliopiston oikeustieteiden tiedekunta. Ulkomaisina yhteistyökumppaneina ovat ITMO (IT-, mekaniikka- ja optiikkayliopisto) Pietarissa Venäjällä ja Arizonan yliopiston Artificial intelligence laboratorio USA:ssa.

Projektin koordinaattorina ja koko projektin vastuullisena johtajana toimii yliopettaja, TkT Jyri Rajamäki Laurea- ammattikorkeakoulusta. Projektiin rahaa sijoittavat yritykset tulevat olemaan mukana projektin johtoryhmätyöskentelyssä seuraavankaltaisesti:

Jäsenet:

Äänivallaton jäsen, projektipäällikkö ja esittelijä:

yliopettaja, KTL Juha Knuuttila Laurea- ammattikorkeakoulusta

Projektin tutkimusresurssit muodostavat organisaatioittain seuraavat:

Laurea -ammattikorkeakoulu

yliopettaja, TkT Jyri Rajamäki

yliopettaja, KTL Juha Knuuttila



Laurea voi myös käyttää muita omia asiantuntijoita sekä opiskelijaresursseja soveltuvin osin. Projektissa voidaan myös hyödyntää Laurea Leppävaarassa toimivia T&K laboratorioita. Opetuksessa ja kaikissa laboratorioissa noudatetaan Laureassa kehitettyä LbD (Learning by Developing) -ongelmaratkaisupohjaista oppimismallia. LbD on läpikäynyt kansainvälisen raadin tekemän arvioinnin viime syys-talvena.

Lapin yliopiston oikeustieteiden tiedekunta

OTT Lotta Viikari

KTT, OTL Leena Lehtinen assistentteineen

## 6 Budjetti ja rahoitus suunnitelma

Budjetti:

Palkat		166600
Henkilösivukustannukset		83300
Yleiskustannukset		124900
Matkat		20000
Aineet ja tarvikkeet		19150
Laiteostot/vuokrat		0
Ostettavat palvelu		20000
Muut kustannukset		0
	YHTEENSÄ	<b>434000</b>

KAIKKI YHTEENSÄ: 434 000 euroa

Rahoitussuunnitelma:

<i>Rahoittaja</i>	<i>Tuen muoto</i>	<i>euroa</i>	<i>%</i>
Tekes	AVUSTUS	260400	60
<u>Laurea AMK</u>	<u>Oma rahoitus</u>	<u>59 600</u>	<u>13,8</u>
EADS Secure Networks oy	Yksityinen rahoitus	45 000	10,4
Tullihallitus	Muu julkinen rahoitus	30 000	6,9
<u>Trevoc oy</u>	<u>Yksityinen rahoitus</u>	<u>15 000</u>	<u>3,5</u>
Loomis Suomi oy	Yksityinen rahoitus	15 000	3,5
Portalify oy	Yksityinen rahoitus	9 000	2,1
	Yksityinen rahoitus		
<b>YHTEENSÄ</b>		<b>434000</b>	<b>100</b>

Rahoituspanoksen lisäksi seuraavien asiantuntijatahojen kanssa on neuvoteltu ja he ovat luvanneet työpanostaan Saterisk-projektin toteuttamiseen:

Liikenne- ja viestintäministeriö / liikenneneuvos Seppo Öörni

Ulkoasiainministeriö, Hallinnollinen osasto, turvallisuusyksikkö / turv.pääl. (NSA) Erkki Väättäinen

Viestintävirasto (Flicora) / radioverkkoasiantuntija Kalle Pikkarainen

(Fastrax: Maailmanlaajuisesti toimittaa OEM GPS -vastaanottimet ja -paikantimet, satelliitti-paikantimet ja -antennit.)

## 7 Projektin laadunvarmennus ja tulokset

Projektin laadunvarmennuksesta vastaa projektipäällikkö yliopettaja Juha Knuuttila Laurea-ammattikorkeakoulusta. Laadunvarmennus toteutetaan erillisen suunnitelman mukaisesti, jossa on hahmoteltu laadunvarmennuksen toteuttamisperiaatteita, tiedon keräämistä, tulosten analysointia ja raportointia.

Laadunvarmennus toteutetaan projektissa mukana oleville yrityksille ja asiantuntija organisaatioille suunnattuina arviointi- ja palautekyselyinä ja projektissa tutkimusorganisaatioina olevien osalta jatkuvana itsearviointina.

Laadunvalvontaan liittyy jatkuva ja tehokas tiedottaminen projektissa mukana olevien organisaatio- ja toimijatahojen välillä.

## 8 Projektin riskien arviointi

Seuraavien seikkojen on arvioitu muodostavan projektin onnistumiselle riskeiksi. Näihin riskeihin on varauduttu taulukossa ilmenevin keinoin.

RISKI	RISKIIN VARAUTUMINEN
Yhteistoiminta tutkimuslaitosten ja yritysten välillä	Jatkuva ja tehokas yhteydenpito. Molemmilla määritellyt ja resurssoidut avainhenkilöt
Yrityspuolen toimijat eivät riittävän sitoutuneita	Sitouttaminen, yritysten sijoitettu rahapanos riittävä ja kilpailija mahdollista ottaa tilalle.
Avainhenkilöiden poistuminen (henkilö-riski)	Huolellinen rekrytointi ja varahenkilöjärjestelmä. Kaikki tärkeä osaaminen, asiat ja tiedot usean henkilön hallussa.
Mukana olevien yritysten kiinnostuksen kohteiden erilaisuus	Varmistetaan riskianalyysin tulosten käyttökelpoisuuden riittävästä yleisyydestä. Huomioidaan uusien näkemyksiä ja ratkaisuja suunniteltaessa koko paikannusketjun toimijat. Hyödynnetään yritysten erilaisuutta vertailunäkökohtana.
Henkilöresurssien riittämättömyys työpakettien toteuttamisessa	Laureassa runsaasti korkeatasoisia osaajia sekä opettajina, että ylemmän amk tutkinnon opiskelijoina turvallisuusjohtamisen sekä teknisen tietoturvallisuuden ja tietotekniikan aloilla vahvana reservinä.
Tiedon keräämisen epäonnistuminen	Useita viranomaisia ja toimijoita, joilla tarvittavat kotimaiset ja kansainväliset kontaktit, jotka kattavat koko arvoketjun.
Aikataulun venyminen	Huolellinen valmistelu ja järjestely aloitus. Aikataulutettu projektisuunnitelma, jossa useita suunniteltuja mittauspisteitä
Tulosten vaikea saavuttaminen	Realistisesti asetetut tavoitteet, jotka jaettu pienemmiksi osatavoitteiksi

Lähteitä:

Euroopan talous- ja sosiaalikomitean lausunto aiheesta: Vihreä kirja satelliittinavigoinnin sovelluksista KOM(2006) 769 lopullinen

Saatavana internetistä:

<URL:<http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=fi&docnr=989&year=2007>>

Laki yksityisyyden suojasta työelämässä. SK 13.8.2004/759

Saatavana internetistä: <URL:<http://www.finlex.fi>

LaVM 24/1994 Lakivaliokunnan mietintö n:o 24 hallituksen esityksestä telekuuntelua ja -valvontaa sekä teknistä tarkkailua koskevaksi lainsäädännöksi

Pakkokeinolaki SK 30.4.1987/450

Saatavana internetistä: <URL:<http://www.finlex.fi>

Pk -yrityksien riskienhallinta. 1998. Saatavana internetistä:

<URL:<http://www.pk-rh.com>>

Poliisilaki SK 7.4.1995/493

Saatavana internetistä: <URL:<http://www.finlex.fi>

Prümin sopimus

Saatavana internetistä:

<URL:<http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+243/2006&base=erhe&paivelin=www.eduskunta.fi&f=WORD>>

Pölönen, Pasi (1997) Salaiset pakkokeinot. Kauppakaari Oy, Lakimiesliiton kustannus, Vammalan kirjapaino Oy, Vammala.

The Galilei Project / GALILEO Design Consolidation © European Commission, 2003

Saatavana internetistä:

<URL:[http://ec.europa.eu/dgs/energy\\_transport/galileo/doc/galilei\\_brochure.pdf](http://ec.europa.eu/dgs/energy_transport/galileo/doc/galilei_brochure.pdf)>

Tupamäki, Matti (1999) Valtion rikosoikeudellisen toimivallan ulottuvuus kansainvälisessä oikeudessa. Väitöskirja Helsingin yliopisto 1999

Uusikivi, Toni (2006) Teknisestä tarkkailusta ja valvotusta läpilaskusta kansainvälisten sopimusten valossa. Poliisiammattikorkeakoulu Poliisipäälystön tutkinto nro 8 opinnäytetyö

Viestintäviraston mittauspöytäkirja häirintälaitteista, 04/2008. (Viranomaisjulkinen)

VIHREÄ KIRJA satelliittinavigoinnin sovelluksista. EUROOPAN YHTEISÖJEN KOMISSIO Bryssel KOM(2006) yyy lopullinen (komission esittämä)

Saatavana internetistä:

<URL:[http://www.tekes.fi/eu/fin/7po/yhteistyo/liikenne/com\\_2006\\_gp\\_galileo\\_fi.pdf](http://www.tekes.fi/eu/fin/7po/yhteistyo/liikenne/com_2006_gp_galileo_fi.pdf)>

Viikari, Lotta (2007) The Environmental Element in Space Law: Assessing the Present and Charting the Future. University of Lapland Printing Centre. Rovaniemi 2007.

## Liite 2, TEKES-rahoituspäätös SATERISK-projektille



p 10050

7.4.2009

Dnro 1203/31/08

Tekesin talouspalvelut

Laurea-ammattikorkeakoulu Oy  
Laurea Leppävaara  
Ratatie 22

01300 VANTAA

Rahoituspäätös nro 940/08, päätöspvm 14.11.2008  
Vastuuhenkilönne Jyri Rajamäki

## MAKSATUSPÄÄTÖS

Tekes ilmoittaa tehneensä seuraavan maksatuspäätöksen:

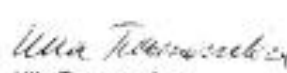
	EUR
Myönnetty avustusta	260.400,00
Maksettu aikaisemmin	0,00
Kustannusjakso	1.9.2008 - 31.12.2008
Hyväksytyt kustannukset	23.449,00
Maksetaan eränä A 1	14.069,00
Momentti	32.20.40.1/08
Tilille 800017-70367168	
Pankkiville/viesti SATERISK	

**Lainkohdat:** Valtioneuvoston asetus tutkimus-, kehittämis- ja innovaatiotoiminnan rahoituksesta (298/2008) 15 § sekä valtionavustuslain (688/2001) 37 §.

**Muutoksenhaku:** Tähän päätökseen saa hakea oikaisua Tekesiltä. Oikaisuvaatimusosoitus on liitteenä.

Helsingissä, 7.4.2009

  
Kimmo Kanto  
teknologiajohtaja

  
Ulla Tuomenoksa  
tarkastaja

LKP	Tatili	Vv	Kun	Euko	Kohde	EUR
82302	3220401	08	49			D 14.069,00
19981						K 14.069,00

utu

## OIKAISUVAATIMUSOsoitus

Tokes - teknologian ja innovaatioiden kehittämiskeskuksen antamaan päätökseen saa siihen tyytymätön asianosainen hakea muutosta vaatimalla oikaisua. Oikaisuvaatimus tehdään kirjallisesti ja se on tehtävä 30 päivän kuluessa Tekesin päätöksen tiedoksisaantipäivästä, sitä päivää lukuunottamatta. Tiedoksiantopäivän osoittaa tiedoksianto- tai -saanti-todistus. Mikäli päätös toimitetaan postitse, asianosaisen katsotaan saaneen päätöksestä tiedon seitsemäntenä päivänä siitä, kun päätös on annettu postin välittäväksi.

Oikaisuvaatimuksessa on ilmoitettava

- oikaisuvaatimuksen esittäjän nimi
- päätös, johon haetaan oikaisua
- millä kohdin päätökseen haetaan oikaisua ja mitä muutoksia siihen vaaditaan tehtäväksi
- perusteet, joilla oikaisua vaaditaan.

Oikaisuvaatimuksen esittäjän laillisen edustajan tai asiamiehen on allekirjoitettava oikaisukirjelmä. Asiamiehen on liitettävä kirjelmään valtakirja.

Oikaisuvaatimus on toimitettava määräajassa virka-aikana klo 8.00 – 16.15 Tekesin kirjaamoon. Omalla vastuulla vaatimuksen voi lähettää postin tai lähetin välityksellä, telekopiona tai sähköpostitse (kirjaamo@tokes.fi) niin ajoissa, että se ehtii perille määräajan viimeisenä päivänä virka-aikana. Myöhästyneet oikaisuvaatimukset jätetään tutkimatta.

### Liite 3: Jamming detection in the future navigation and tracking systems

M. Happonen, J. Viitanen, P. Kokkonen, J. Ojala, J. Rajamäki, 2009

#### Abstract

Currently, satellite navigation and tracking have become everyday routine and they are still growing while EU's new satellite system Galileo will be operative in 2013. Positioning, navigation and tracking are used to decrease risks especially in logistics and to optimize work flow, but does it always work that way? Can international legislation about tracking, or lack of it, cause problems when doing tracking abroad? With technical aspects, are your tracking systems good enough to increase the security of your crown jewel or are you just giving extra hints to thieves? For answering these questions, the SATERISK research project was started in 2008. It aims at a situation where laws on positioning and tracking and the financial risks posed by their usage will not prevent the use of m2m tracking across state and union borders. Essential part of the project is to study signal interference in tracking and find ways to improve tracking devices and user habits in the future to avoid them. This paper focuses mainly on that topic.

Index Terms—Navigation, positioning, signal interference, tracking, jamming

#### INTRODUCTION

Satellite navigation and tracking have become everyday routine nowadays and many security instances use GPS with no risk analysis. Popularity of satellite navigation still grows while Russian Glonass is re-established and EU's new satellite tracking system Galileo becomes operational in 2013. Navigation and tracking is used to decrease risks especially in logistics and to optimize work flow, but does it always work that way? Military uses of positioning have always been heavily protected, but in civil applications security issues and possibility for signal interference are too often ignored. This is one of the main reasons why SATERISK project is founded. At the moment SATERISK project is in relatively early phase and first main tasks are to make risk assessment and requirement specification. Preliminary risk assessment has supported assumption that knowledge of signal interference and counter measures for them are needed and therefore they are essential part of SATERISK project. Due to early phase of the SATERISK project, this paper is mainly theoretical and hands-on results are still forthcoming.



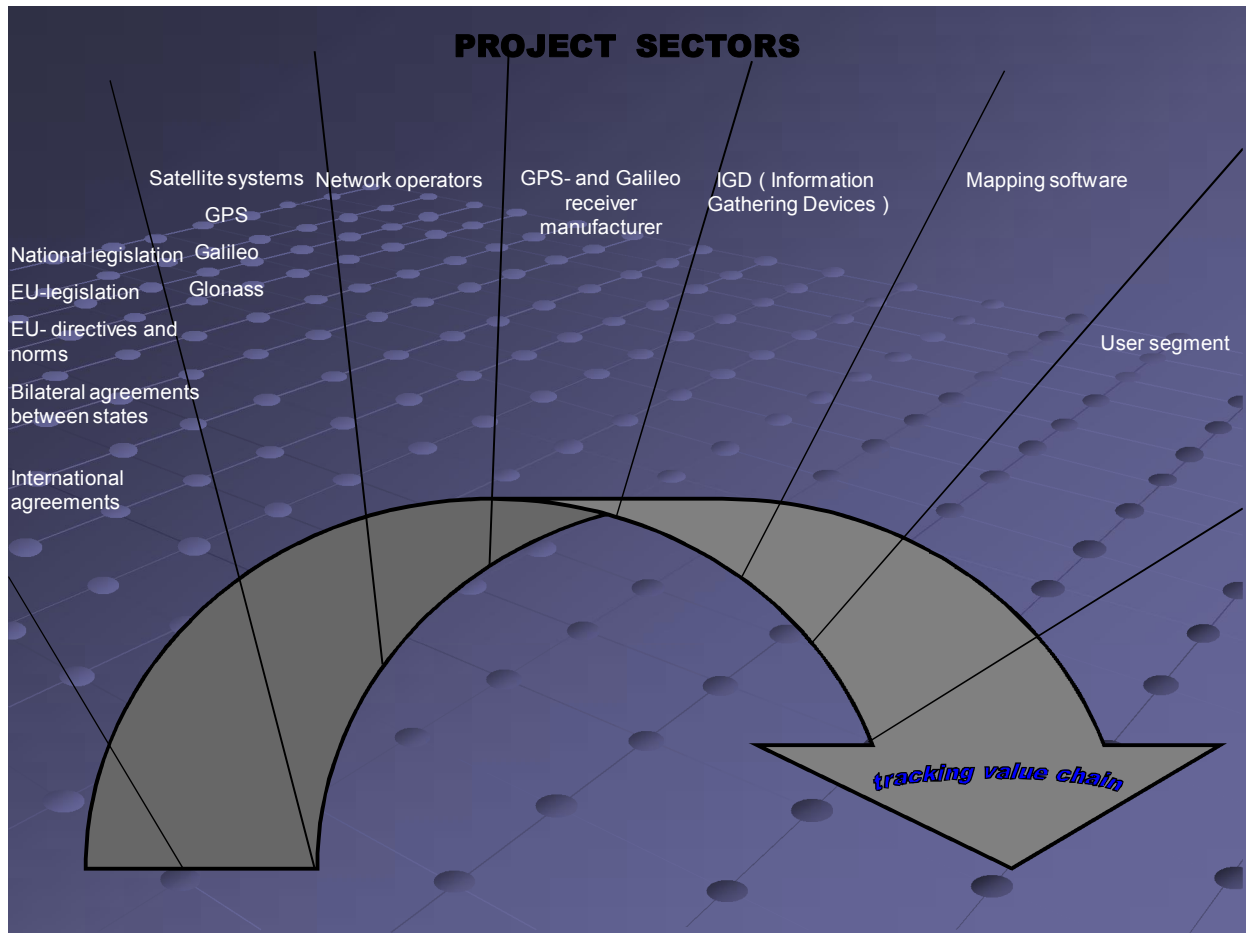
## SATERISK

SATERISK is a research project, which aims at a situation where laws on positioning and tracking will not prevent the use of so-called m2m (machine to machine) tracking devices across state and union borders.

The project aims to bring new, international level know-how to the European security field. The project will also create new methods and development paths for positioning and tracking systems. The widely used US-based GPS (Global Positioning System) satellite positioning system will soon get an EU counterpart and rival from the Galileo [1]. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system can be charted. The project also aims to offer technological solutions to issues that rise while the project is ongoing.

SATERISK is a joint research project of universities, public organizations and private companies with regard to positioning, navigation and tracking systems, as shown in Figure 1. The aim of the project is to evaluate risks and the technical and legislative needs for positioning and tracking here and now, as well as in the future. However, this paper is a technical one and therefore legislation part is reduced. Technical issues are mainly studied by Laurea University of Applied Sciences and they are covering, for example, security, fail resistance and high usability. Despite confirmed intentional signal interference cases in tracking have been really rare, there have been some events, where usage of jamming devices have been documented.

Figure 1, Project sectors



## SIGNAL INTERFERENCE

Tracking devices can be interfered in several ways and each of them has their own counter measures. GPS (like any other satellite navigation system) frequencies are commonly known and therefore easily disturbed. Similarly, tracking device transmissions are as easily stopped by causing noise to GSM and 3G frequency. More sophisticated way to interrupt tracking transmission is to use fake base station, when no other signals are disturbed. This makes interference detection much more challenging.

Another way to nullify tracking system is to use fake satellites (so called pseudo-satellites or pseudolites). Instead of jamming, pseudolites imitate satellite signal. Corrupted satellite data causes wrong positioning for tracking devices.

One, theoretical way to prevent tracking is to use electromagnetic pulse (EMP) device. EMP devices are expensive and developed for military use. There are no reports about using any EMP device to disrupt tracking.

Naturally all interference isn't intentional. Other electrical equipment could cause errors especially for inadequately shielded devices. This problem is easily avoidable by using better shielding and components. Therefore unintentional interference is not taken part in this document.

Targets and reasons for interference vary a lot. Although SATERISK-project is mostly focused on reliability of tracking devices on motor vehicles, results of the project are also usable in other environments, too. For example in aviation satellite positioning is gaining ground from traditional radio positioning and even radar. Satellite positioning is used to reduce distances between airplanes caused by slowness of radar. So satellite positioning will reduce costs and improve efficiency, especially in approach and landing [2]. Another special case is plan to use positioning to road toll and taxation systems. Positioning based road toll system have been under development by several private companies and one advantage in this system is that road tolls accumulates with driven kilometres. Finnish ministry of transportation and communications also has preliminary plans to bill car insurance and car taxes by driven kilometres [3]. This scenario still has some issues to be solved, where false positioning is one of them. These scenarios about aviation and road tolls are not represented any further in this document.

## TECHNICAL ASPECTS

In October 2007, there was an attempted robbery of cash truck near the Finnish city of Turku. The police took 11 men into custody, all of them allegedly members of an international gang. The robbers were equipped with assault rifles, explosives, bullet-proof vests, masks and a jamming device capable of jamming GSM phones, GPS devices and also TETRA phones on very limited range [4]. So, there really is a need to know if your assets are target of intentional electromagnetic interferences (IEMI) and jamming [5-7]. Small, 5 meter radius GPS/GSM jammers are easily buyable and prizes start from 50 € [8].

The technical approach on the SATERISK project considers e.g. authentication, jamming detection and necessary encryption. On some occasions it is necessary to use strong encryption to hide position from public for own protection (e.g. money transports) especially if network operators are not trusted, while in other circumstances it is vital to get authenticity of position [Data protection vs. data authentication] (e.g. in aviation).

International co-operation is needed between authorities to create tracking transmission standards with necessary encryption. Standards are needed when changing encrypted position information abroad. Trust management will play an essential role in these exercises.

One of the main technical tasks is to provide information about intentional and accidental interference of the tracking signal. This information will help to provide better tracking and positioning devices. It also helps to find counter measures for interference.

## DETECTION

Intentional and unintentional interference is difficult to separate from each other in some occasions, for example when tracking device enters to tunnel or to a parking lot. If interference is caused by natural causes, there is not much to do for it. Only possible counteraction is to log these locations to tracker and later tracking administrator may approve these positions as “clarified” positioning error areas.

On the other hand, if satellite signal is lost suddenly, especially in open environment, it is most likely caused by intentional jamming. Intentional jamming is relatively easy to detect, if data about natural interference positions is available, but otherwise it’s close to lucky guess to separate them.

Frequency jamming isn’t the best way to interfere tracking signal. Using pseudolites instead of jammers may mislead tracking personnel much easier [9]. Pseudolites can be modified from GPS transeivers, but the better ones are built entirely for creating fraud satellite signal. Nowadays, some tracking devices, especially in aviation, can identify pseudolites and ignore their signals. However, interfering devices get better all the time and better algorithms and countermeasures are needed.

Jamming of GSM signal is relatively easy to spot, because of the wide coverage of signal. If the GSM signal is interrupted, reason is either broken mobile device, base station failure or intentional jamming. In crowded areas, base stations usually cover part of each other’s area and therefore lose of signal most likely is prove of jamming.

While detection of GSM jamming is one of the easiest to spot, usage of the fake base station is one of the hardest. Fake base stations captures all signals of mobile phones, speech, sms and data, and user of fake base station may decide, if the signal is passed through, decoded and opened, interfered or even changed and then forwarded. Every base station has its own unique identification, so called cell id. If cell id codes are known and stored in tracking devices local database, device can compare current cell id with cell ids of current tracking area. This will need more sophisticated tracking device, because connection to the server isn’t certain in GSM interference situations.

## COUNTER MEASURES

The most important feature in tracking devices is reliability in all environments [10]. Therefore countermeasures for interference have to be found and tested. The most important counter action to interference is immediate alarm to the local unit. Especially on transportation of valuable goods it's vital to get alarm to target unit. Next alarm information should be sent to the backup units.

To prevent unwanted incidents, it is very important that the information provided by the tracking system is very near real time. The priority of security system is to prevent, not to help investigation afterwards.

Some standard counter actions for interference can be decided, but they still need to be tested beforehand. If tracking device transmissions are interrupted, device should start to work as a logger. Recorded data will be sent to server, when connection is enabled again. Possibility to use alternative communication methods have to be researched. Alternative methods could be TETRA phone, wlan or other similar wireless solution.

Pseudolites have to be recognized and ignored. Best knowledge about pseudo-satellites is probably in NASA (for example because of Mars navigation) and in aviation industry, where the risks are the biggest. However, exact information about pseudo-satellites is likely confidential, because of obvious security issues.

If satellite signal is jammed, alternative ways to locate tracking device have to be found. One possible solution is to use gsm base station positioning. This will give quite good estimate about position, until satellite connection is re-established. In aviation, there always needs to be radar or radio positioning as a backup system, especially, when flying in instrumental meteorological condition (IMC).

If both, satellite information and device transmission are jammed, there basically isn't way to get position information. Then tracking device should go to passive mode and run periodical tests until connections are enabled again.

## FUTURE WORK AND FINAL WORDS

Like early in the paper stated, SATERISK project have just lately begun and there are lots of research work to be done. Although SATERISK get some funding from Finnish research support centre (TEKES), it is relatively small player in positioning field. Main effort is done to improve

knowledge of the possible risks regard to positioning and tracking. This knowledge will point out new features needed in tracking systems and in the future those features need to be tested. SATERISK project needs to find balance between security and usability of tracking as a security device. After all, user is one of the main risks in technical system and therefore also user habits need to be charted.

Possible changes to international legislation and regulations need lots of work and it's better to leave for professionals of that topic. Communication security has to be improved, but that is likely made with already existing solutions.

In general, SATERISK project is also trying to look in the future by finding future scenarios of the risks and benefits. Reliability, error recovery and avoidance of human err are challenging goals, but they still are worth trying.

Positioning and tracking systems do not automatically decrease, but can actually create risks and therefore a risk assessment is needed before using them. In the history of IT, today's solutions have often turned out to be tomorrow's problems. Whether this is applicable and/or avoidable regarding Galileo?

## REFERENCES

OPINION of the European Economic and Social Committee on the Green Paper on Satellite Navigation Applications COM(2006) 769 final, Available:

<http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=en&docnr=989&year=2007>

Tekniikka&talous magazine 7.12.2008, available in Finnish:

<http://www.tekniikkatalous.fi/ict/article194088.ece>

Parliament of Finland, YmVL 12/2008, online document (in Finnish) Available:

[http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ymvl\\_12\\_2008\\_p.shtml](http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ymvl_12_2008_p.shtml)

(Helsingin Sanomat/International edition, 2007, October 2) Available:

<http://www.hs.fi/english/article/Two+Swedish+gang+members+still+at+large+after+attempted+robbery+of+cash+truck+near+Turku+on+W.ednesday/1135231511615>

T. Olsen, B. Forssell, "Susceptibility of Some Civil GPS Receivers", GPS World (2003), Available: <http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=43432>

D. Månsson, Intentional electromagnetic interference (IEMI): Susceptibility investigations and classification of civilian systems and equipment. Doctoral thesis, Uppsala: Uppsala University, University Library (2008), Available: <http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-9264>

D. Månsson, T. Nilsson, R. Thottappillil and M. Bäckström, "Susceptibility of GPS Receivers and Wireless Cameras to a single Radiated UWB Pulse", Proceedings of EMC Europe, Barcelona, Spain (2006).

TAYX -online catalogue, Available: <http://www.tayx.co.uk/default.html>

GPS Pseudolite rover project. Available: <http://sun-valley.stanford.edu/users/rover/>

O. Pozzobon1, C. Wullems1, K Kubik, "Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services" Journal of Global Positioning Systems (2004) Vol. 3, No. 1-2: 200-207, Available: