LAUREA

Recognizing risks of satellite-based tracking

Happonen, Markus

2010 Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

RECOGNIZING RISKS OF SATELLITE-BASED TRACKING

Markus Happonen
Thesis work for masters' degree in ICT
May 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma

Markus Happonen

Satelliittipaikannuksen riskien tunnistaminen

Toukokuu 2010 Sivumäärä 45

Satelliittipaikannus on yleistynyt nopeasti sotilaskäytöstä aivan jokapäiväiseksi avuksi autoilusta lasten vahtimiseen. Vaikka uuden teknologian käyttö on yleistynyt voimakkaasti, ei sen sisältämiin vaaroihin ole paneuduttu riittävästi. Paikannusta käytetään yleisesti tuottavuuden ja turvallisuuden parantamiseen, mutta väärinkäytettynä paikannus tarjoaa ennemminkin työkaluja rikollisille. Tämän vuoksi vuoden 2008 lopussa aloitettiin SATERISK-projekti.

SATERISK-projektin tarkoituksena on selvittää satelliittipaikannuksen käyttöön liittyviä riskejä, sekä suunnitella ja toteuttaa vastatoimia niihin. Osaltaan projekti liittyy eurooppalaisen GALILEO-projektin mahdollistamiin muutoksiin, vaikka pääpaino onkin paikannuslaitteissa sekä taustajärjestelmissä.

Projektin ensimmäinen vaihe tuotti projektisuunnitelman mukaisesti riskianalyysin ja tämä päättötyö on luonnollinen jatko sille. Tässä työssä on paneuduttu esittelemään SATERISK-projektiin liittyviä konferenssitöitä, joissa kirjoittaja on ollut osallisena. Lähestymistapa on ollut pitkälti tekninen, sillä kirjoittajan taustasta johtuen esimerkiksi lakiosuus on erittäin rajoitettu.

Päättötyön ensimmäinen julkaisu liittyy signaalinhäirintään sekä sen vastatoimiin. Kaikki häirintä ei luonnollisesti ole tahallista, vaan esimerkiksi maasto ja tunnelit voivat aiheuttaa katkoksia. Näistä tilanteista toipuminen, sekä sopivat vastatoimenpiteet ovat erittäin tärkeitä mm. arvokuljetuksissa.

Toisessa ja kolmannessa julkaisussa on keskitytty organisaation välisen tiedonkulun haasteisiin paikannettaessa. Kyseinen ongelma liittyy eritoten kansainväliseen viranomaisyhteistyöhön, mutta myös useammassa maassa toimivat logistiikkayhtiöt ovat vastaavan haasteet edessä.

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

Laurea University of Applied Sciences
Leppävaara
ICT Programme

Markus Happonen

Recognizing risks of satellite-based tracking

May 2010 Pages 45

Abstract

Within last two decades, popularity of the satellite-based navigation has boomed from military application to common aid in driving and safety equipment for children. People have become even too dependent of technical aid while risk of their usage is too often forgotten. Especially this is serious risk in companies and public sector, where positioning and tracking is used to improve security and productivity. To avoid these problems SATERISK-project was found.

Goal for the project is to search risks about satellite-based navigation and also find solutions for them. Project has small part in GALILEO project development, while main part of the project focuses on tracking devices and backend software.

The requirements analysis was the first phase of SATERISK-project and this thesis is natural continuum for it. This thesis focuses to present those publications done for the SATERISK-project, where thesis writer have had a part. Personal approach for the task is mainly technical due to writer's background and therefore for example juridical part is really limited.

First publication in the thesis is about signal interference and countermeasures for them. All interference is not intentional, but for example terrain and road tunnels may cause signal loss. Therefore recovery and countermeasures for these situations should be considered beforehand. It is absolutely important to know, if the interference is manmade or unintentional, especially in transportation of valuable goods.

Second and third publications were about time critical data communication between multinational organizations. This problem is common in law enforcement environment. Criminals are working more often abroad due the European integration, but law enforcement authorities do not have common protocols and procedures, how to pass information between each other. Especially machine to machine (M2M) communication is not researched yet.

Key words: Requirement analysis, Galileo, GPS, Risk, GIS, Tracking, SATERISK

PREFACE

The thesis work is going to present three publications that were made as a part of the SATERISK-project. It also gives a picture about satellite-based navigation and tracking applications. I was fortunate to get this possibility to work along this project. In the project, I was able to use my previous knowledge about satellite-based navigation and I also gained huge amount of information about the topic. It gave me many new points of view to the wide area of satellite-based navigation and it will certainly help me in the future in my work and also in my hobbies.

Satellite-based navigation is also rapidly developing topic and different uses for navigation are invented nearly daily basis. Especially GPS-based road toll applications are getting more popular (Iltalehti 2010). It has been a great opportunity to do an interesting work and study about everyday technologies for tomorrow.

The work has been performed under guidance of Dr. Jyri Rajamäki, who also works as a part of the SATERISK project. His spirit, skill to encourage and new ideas have been great help for the project and also for my thesis work. I feel lucky to have such a professional as a tutor and coworker. I am also very grateful for him about offering me this possibility to have a part in this marvelous project.

I would like to thank the Finnish Funding Agency for Technology and Innovation, TEKES, about providing funding for SATERISK-project. Without this, the entire project would be cancelled or reduced. The project has so far been interesting and motivating to learn more about satellite-based tracking. My special thanks to all SATERISK-team for co-operation. Your different background and many ideas have been so fruitful and your spirit has kicked me forward in my work. SATERISK-project also made it possible to participate to the conferences by providing funding for these trips. My special thanks for this.

I would also like to LAUREAs teachers and personnel. Your professional attitude and skills have provided really good learning environment. Also, all other co-authors of the publications have my special gratitude.

I also like to thank my fellow students to provide workgroups where they provided their experiences from different fields of ICT sector. Especially I like to thank my colleague and fellow student Jouni Viitanen, who had great contribution for my decision to apply Laurea University of Applied Sciences. Mr. Viitanen also played essential part when inventing

SATERISK-project and finding proper funding for it. Without him, I wouldn’t be able to do this interesting thesis.

Also my family, friends and relatives deserve my gratitude for their support not only during good days, but also when things were not going that smoothly. Last but not least I would like to thank my employer for flexibility and giving me possibility to study.

Table of Content

LIST OF PUBLICATIONS

This thesis consists of an introduction and the following three publications, which are preferred by [P1]-[P3] in the text:

[P1] M. Happonen, J. Viitanen, P. Kokkonen, J. Ojala & J. Rajamäki, “Jamming detection in the future navigation and tracking systems”, In proceedings of the 16th Saint Petersburg International Conference of Integrated Navigation Systems, St. Petersburg, Russia, May 2009. ISBN 978-5-900780-69-6, pp. 314-317

[P2] J. Viitanen, M. Happonen, P. Patama & J. Rajamäki, “International and transorganizational information flow of tracking data”, in proceedings of the 8th WSEAS International Conference on Information Security and Privacy (ISP ’09), Puerto de la Cruz, Tenerife, Spain, December 2009. ISBN 978-960-474-143-4, pp. 111-115

[P3] J. Viitanen, M. Happonen, P. Patama & J. Rajamäki, “Near border Procedures for Tracking Information”, WSEAS TRANSACTIONS ON SYSTEMS, Issue 3, Volume 9, March 2010. ISSN 1109-2777, pp. 223-232

LIST OF ABBREVIATIONS & SYMBOLS

A-GPS = Assisted GPS, satellite-based positioning method aided by mobile networks
3G = common name for third generation mobile networks
CII = critical information infrastructure
CIIP = critical information infrastructure protection
DSA = Designated Security Authority
EGNOS = European Geostationary Navigation Overlay Service
EU = European Union
Europol = European Law Enforcement Organization.
FICORA = Finnish Communication Regulatory Authority
Frontex = European Union's agency for external border security.
GALILEO = Joint European satellite-based navigation system. Due to major delays it is currently only in early test phase. Planned to be fully operational around 2013 (ESA – Navigation - The future – Galileo 2009).
GIS = Geographical Information System
GLONASS = (*GLObalnaja* NAvigatsionnaja Sputnikovaja Sistema). Russian satellite-based based navigation system. Currently being reinstalled and should be fully operational in near future.
GNSS= Global Navigation Satellite System
GPS=Global Positioning system. Satellite-based global positioning system operated by Navstar
GPRS = 3rd generation mobile network
GSM = 2nd generation mobile network
IGD= Information Gathering Device
IRNSS = Indian Regional Navigational Satellite System
LEA = Law Enforcement Authority. Common name for law enforcement authorities, including for example: police, customs and border guard.
M2M= Machine to Machine. Data gathering method were humans are not directly involved.
MIL-STD= NATO based military standard
NASA = National Aeronautics and Space Administration
NMEA = (National Marine Electronics Association) Organization that created popularly used positioning protocol, also named NMEA.
NCSA = National Communication Authority
NSA = National Security Authority
SATERISK = Joint project to detect and counter SATEllite-based positioning RISKs. Main participants are LAUREA University of Applies Sciences and University of Lapland. [KTS.]
TCP/IP = Transfer control protocol/Internet Protocol

TEKES = the Finnish Funding Agency for Technology and Innovation. Tekes is the main public funding organization for research, development and innovation in Finland. Tekes provides funding for SATERISK-project.
TETRA = (Terrestrial Trunked Radio) Professional Mobile radio, widely used by law enforcement
VPN = (Virtual Private Network) Encryption device to the TCP/IP networks.
WAN = Wide Area Network
WLAN = Wireless TCP/IP Network
WSEAS = World Scientific and Engineering Academy and Society

1 INTRODUCTION

Within last decade, satellite-based navigation has become available tool for every consumer. Satellite-based navigation has been integrated to the boats, airplanes, luxury cars and now even to the mobile phones. Still, risks and misuse of satellite-based navigation have been almost forgotten. Therefore SATERISK project was found. This paper is a part of a SATERISK-project and basically continuum to MBA Jouni Viitanen's thesis work "requirement analysis of the SATERISK-project" (Viitanen 2009).

This paper is going to summarize and represent 3 publications where the publisher has taken a part. It is going to present some basics about satellite-based navigation and also some basics about tracking applications. Main task for the thesis work is to point out essential and too often forgotten risks in satellite-based navigation and tracking applications. The first publication is researching issues about tracking interference, while second focuses to problems on multiorganizational tracking information flows. The third publication is based to the second one. However, it is wider and published in WSEAS TRANSACTIONS ON SYSTEMS, Issue 3, Volume 9, March 2010.

SATERISK-project has started as a special work relating to Jouni Viitanens and Jussi Ojalas studies. It was shortly found to be exciting and needed research topic and therefore was introduced also to the Finnish Funding Agency for Technology and Innovation TEKES. After negotiations, TEKES gave part of the funding for SATERISK. Jouni Viitanen also made his thesis work about the topic and he has taken part to the publications. The thesis work proved need for further examination about the topic.

Main goal for the thesis was to create more information to the SATERISK-project. My personal effort to the project was to get more familiar with signal interference and also create possible risk scenarios and countermeasures for them. This topic was presented at conference held in St. Petersburg. Also the second publication had same kind of approach, but this time topic was tracking related multiorganizational information flow. Also this publication was presented in conference, this time held in Puerto de la Cruz, Spain.

The most important task for this paper is to present these works done for the SATERISK project, where writer have had a part. Mainly these works are conference papers and presentations, but also proposed journal is also included. Main goal for these papers and presentations were to get publicity for a project and also get new approach and feedback from the audience.

As a result for the research, more information was gathered for the SATERISK-project. Also new risk scenarios were created and some possible solutions were found. Also need for international co-operation came essential. The thesis work will point out need for further research about the topic. The publications will point out lack of co-operation between law enforcement authorities.

In this thesis work, scope of the study is presented first. After that, general information about navigation, SATERISK and problems are presented. Third major topic is short presentation of the publications and discussion about results and further studies.

2 SCOPE AND STRUCTURE OF THE STUDY

2.1 Scope, objectives and methods

Objective of the study was to find possible risk scenarios and bottlenecks in satellite-based tracking. The work was done under SATERISK-project and due to personal background, approach is mainly technical. The scope of the study was to find new approach and points of view to the topic of general interest. Although the work was mainly theoretical, it is based to practical experience and to real scenarios. Also the results of the study should be usable in the field of tracking in the future. Main questions this work concentrates to answer are:

- Are electronic countermeasures and other similar interference providing risks to the tracking and how there could be avoided
- What are the main issues in international or in multiorganizational tracking applications
- What steps are required to create commonly used doctrines in tracking

Main goal of the study is to gain knowledge to the project and help to find possible solutions to everyday tracking applications.

Publication [P1] was made using design research method. Goal for the publication was to create guidelines for better tracking devices with error recovery and jamming detection. Also new operational procedures were considered in the publication.

Publications [P2] and [P3] were done using constructive research method. Goal for the papers were to point out the problems and to find possible solutions for multiorganizational tracking.

2.2 Structure and schedule

Saterisk project were founded on the second half of the year 2008 (Viitanen 2009). Personal studies about thesis work started in the beginning of year 2009, although in the beginning, development was relatively slow. Main part of the work in SATERISK project have been data gathering, creating contact and participant networks and finishing requirement analysis (Viitanen 2009). SATERISK-project has so far provided couple of conference papers, where I have been one of the writers. Conference papers and participations are introduced more thoroughly in chapter 2.3. As a part of the thesis work, I have taken part to conferences and gathered information during year 2009.

2.3 Contribution of the Author:

Publication [P1] is based on the analysis of the risks of intentional and unintentional countermeasures for tracking applications. The presentation based to the publication was given in 16th Saint Petersburg International conference on integrated navigation systems. The author was part of the research group as a student and author's contribution to the publication is approximately 65%. Author was sole presenter of the paper in conference.

Publication [P2] were written for and presented in the 8th WSEAS international conference on Information Security and Privacy (ISP `09), in Puerto de La Cruz, Spain. The author was part of the research group as a student and author's contribution to the publication is approximately 35%. Author was companied with a teacher and fellow researcher in the conference.

Publication [P3] was written to a journal, relating to 8th WSEAS conference. The publication was published in WSEAS Transactions on Systems, Issue 3, Volume 9, March 2010 (ISSN 1109-2777). The author was part of the research group as a student and researcher. The author's contribution to the publication is approximately 40%.

The co-authors have seen these descriptions of contributions, and agree with the author.

3 NAVIGATION

Navigation has always been a great issue for human kind. Still, less than fifty years ago, first satellite-based navigation systems have been developed. Also the most common satellite-based navigation system (GPS), were found on the seventies (Standford University – News release, 1995). In the beginning satellite-based navigation and tracking were reserved for military applications and civil use were restricted. In earlier days, GPS satellite signal was

also disturbed in civil applications to reduce accuracy to about 100 meters. This, although were removed shortly after end of the cold war in 1993 (Standford University – News release, 1995).

Within last two decades satellite-based navigation has become every day tool also in civil world. Time period is relatively short and therefore our dependency of it is quite impressing. Aviation, maritime transport and nowadays even everyday car ride is either based or aided by satellite-based navigation.

Another common civil use for satellite-based navigation is to use it as a tracking aid. Nowadays, tracking is used in logistic companies and navigation is an everyday tool for every consumer, but are we already even too dependent about technical aids. When parents are using tracking devices to protect their children privacy is always compromised. And is it possible to use tracking devices against the targets? Then, protection aid would become a threat instead.

Although in many applications satellite-based navigation is only method to do positioning, in more critical applications positioning is secured with more reliable method. For example in aviation, radio positioning is still commonly used method and excluding some exceptions always an alternative method.

4 POSITIONING

Satellite-based navigation is based to a comparison of at least four (or in some cases three, when altitude information is lost) satellites. Satellites have a specific clock in them and therefore distances between tracking unit and satellite is computed from the difference of satellite times. Also additional information is sent, like position of the satellite and ephemerides. Principle of satellite-based navigation is presented on figure 1.

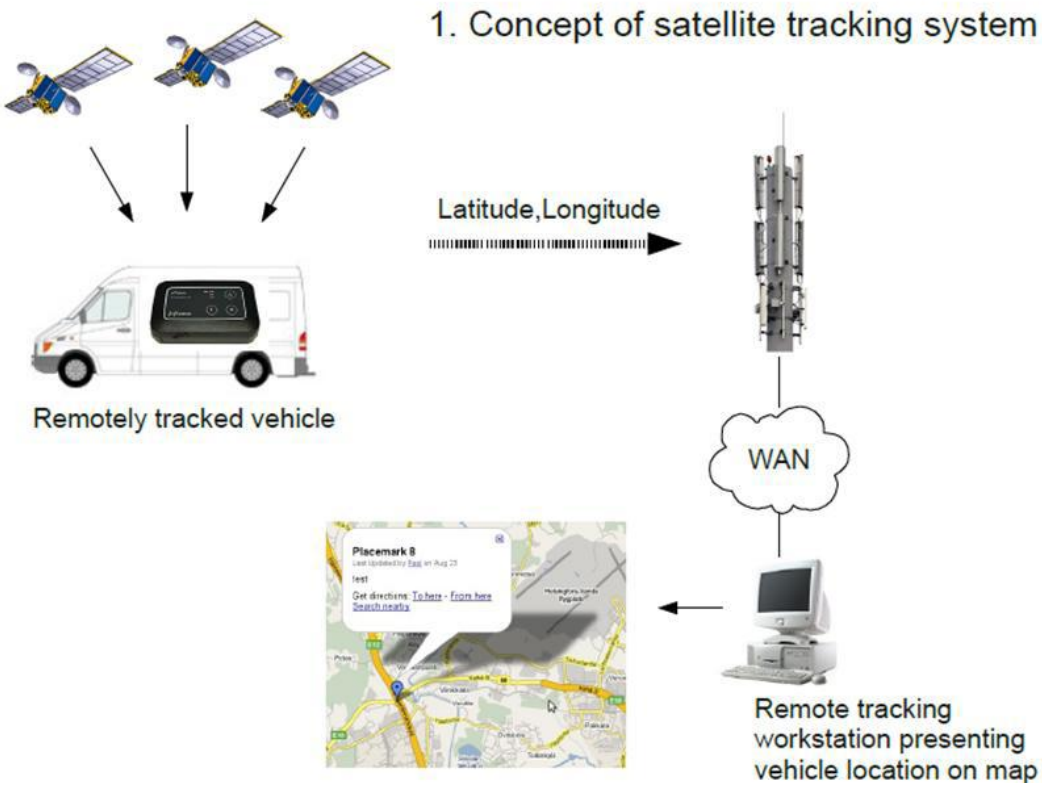

Figure 1. Satellite-based tracking system

Satellite-based tracking systems may wary, but the principle remains the same, whether it is about GPS, GLONASS, GALILEO or similar. The accuracy of the satellite systems depends about accuracy of the clock, possible bouncing signal, distance from the satellite and weather. To reduce false positions necessary amount of the satellites are needed. Currently 24 GPS satellites are on orbit and in use, while four satellites are as spare ones (Garmin – What is GPS).

5 RISKS

The most common risk for satellite-based navigation and tracking is lack of the satellite signal. All the interference is not intentional, but caused by natural reasons. Some interference still is manmade. Nowadays, there have been documented cases where criminals have used signal interference devices. In the future, when GPS based road tolls probably come more common (Findarticles – technology, 2008), also willingness to interrupt satellite signal to avoid taxes increases.

Necessary countermeasures for interference need to be found. Because interfering device is almost impossible to find, the active countermeasures should be done in tracking devices. In Finland controlling radio frequencies belongs to Finnish Communications Regulatory Authority, FICORA, but naturally their ways to prevent signal interference is really limited. So

therefore, police is the only authority to have even slightest possibility to catch anybody from using such a device.

6 SATERISK-PROJECT

Saterisk project started on late 2008 as on special student work, namely done by students Jouni Viitanen and Jussi Ojala. Shortly after presenting work to the teachers, value and idea of the paper was noticed and decision to upgrade work to multiorganizational project was made. Decision was made to create student led research project. After negotiations with the Finnish Funding Agency for Technology and Innovation (TEKES), University of Lapland, and companies from the private sector, SATERISK-project was found. SATERISK-project sectors are presented in figure 2.

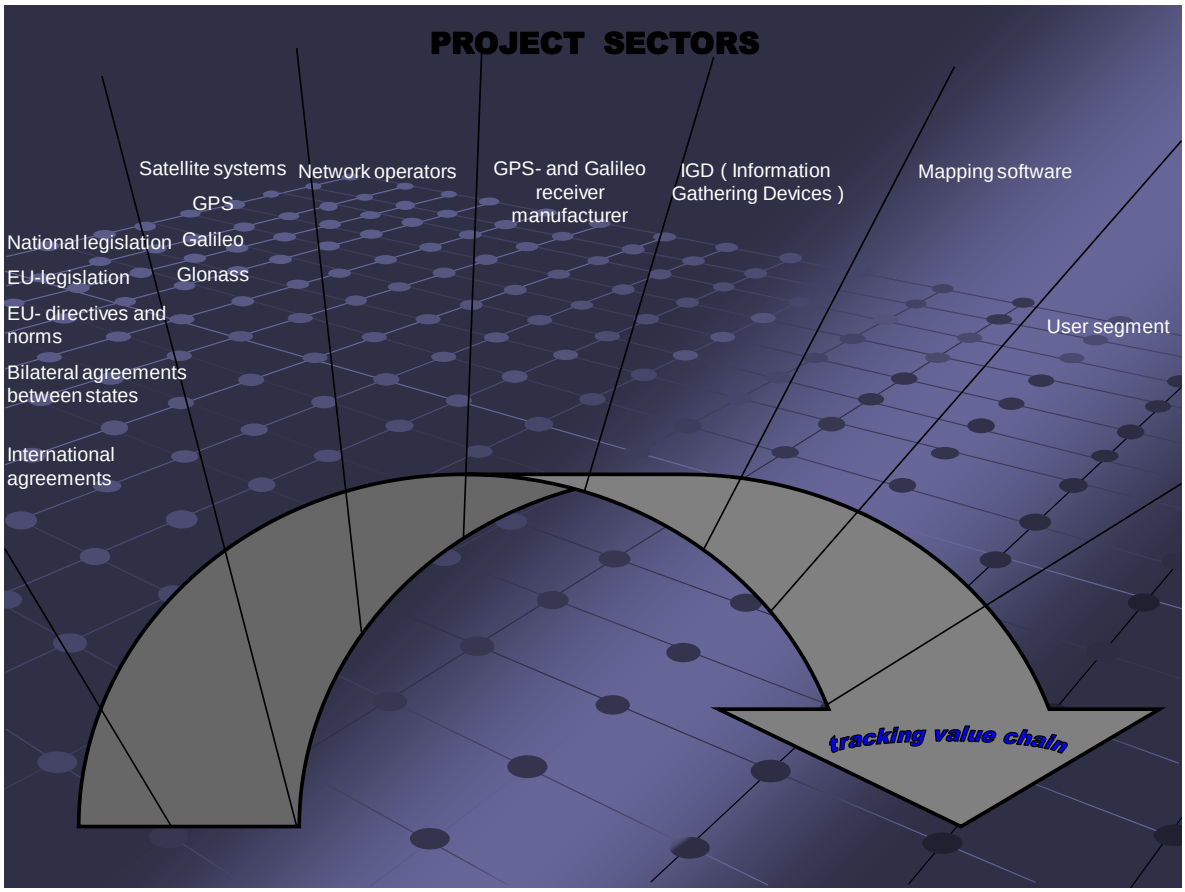

Figure 2. SATERISK project sectors

SATERISK project was found to search possible risk scenarios in satellite-based navigation and tracking applications. Within last decade usage of satellite-based tracking application have boomed, but only little research about risks and setbacks are done. Saterisk project have legislation part, done by University of Lapland. University of Lapland also has close contact with Russian counterpart and therefore comparison between legislation is easily done.

Technical part of the project is coordinated by Laurea University of Applied Sciences and future scenarios are built by information from private sector, too.

7 SUMMARY OF PUBLICATIONS

7.1 Jamming detection in the future navigation and tracking systems

This publication examines the possible risks and counter measures for intentional and unintentional signal interference. Also possibility to interrupt signal and use it criminally against the target is considered in this publication. Misuse of the tracking signal is one key factor in SATERISK and therefore is should not be skipped.

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. While usage of navigation and tracking applications has increased, risk for misuse of position information has increased as well.

Tracking devices can be interfered in several ways and each of them has their own countermeasures. When satellite navigation is interrupted, alternative positioning methods, like mobile networks base station, should be used. False satellites (so called pseudolites) should be ignored. When transmitting signal of tracking device is blocked, should device use alternative transmission method, if available? If no other transmission method is available, tracking unit should work as a logger and send positions afterwards.

All the interference is not intentional. Tunnels and other manmade structures may cause signal interference, as well as terrain. However, in some cases this is hard to separate. In these cases position should be registered to the device or mapping server to avoid possible problems in the area in the future.

Countermeasures for interference also depend about, if the target is aware of the tracking. For example in case of transportation of valuable goods, driver should always be alarmed first in case of interference. The driver is the best person to estimate, if the interference is caused by natural reasons (for example tunnel) or is the interference human made. The driver also is first to do necessary countermeasures in case of attack. After all, the most important countermeasure for interference is reliability in all environments (O. Pozzobon, etc, 2004).

7.2 International and transorganizational information flow of tracking data

This publication presents problems about border crossing tracking. European integration has opened borders and this advantage is widely used by criminals. Therefore transmitting tracking and other status information between nations and different organizations should become every day business. Goal of the publication was to find possible bottle necks in co-operation between organizations and authorities. The publication also tries to find administrative and technical solutions to improve multi-organizational tracking solutions.

In border crossing tracking, time is a key factor. After all, preventing is always more effective than repairing damages (EK – risk management, 1998). However, it is also more difficult than crisis management. Therefore necessary doctrines and atomization is needed.

Nowadays, Law Enforcement Authorities (LEA) happens to be hierarchical and therefore information goes through many unnecessary levels. The knowledge might be created in lower parts of the organization, but for spreading out, it usually must first go to the top, and only from there it can spread. This causes latency which in some cases might be critical. Also, dependency of certain employees may cause vulnerabilities to information flow.

To prevent time consuming decision making process, necessary procedures and doctrines are needed in advance. A doctrine will give an advice, how to proceed in any given situation. Doctrines should be installed as doctrine libraries to the tracking system so, that no human effort is needed to proceed. This, however, creates some technical needs, which are the second part of the publication.

Many of the tracking solutions are designed to work as a standalone system and therefore they have problems to communicate with other similar systems. Even in cases, where common protocol and communication channel exist, possibility to send so called metadata is still missing. Metadata consist essential status information about the target: model, is the target dangerous, armed, etc.

To get proper interfaces, protocols and transmission methods, many international meetings and workshops are needed. Workshops should be organized by European joint organization, like Europol or Frontex, to get necessary value for it. Also mobile development should be taken care of. Therefore, SMS transmission should be used as a backup, when doing tracking abroad.

Another technical challenge is to plan secure network topology for data transmission. All data transfer is encrypted and protected with virtual private network (VPN), but should tracking

information be also encrypted inside private network to prevent information flows? If so, common private key, public key encryption could be used.

In the future, doctrine libraries and technical platform needs to be tested and lots of meetings are required. Also funding might become an issue for the project.

7.3 Near border procedures for tracking information

This publication is a journal, based to the publication [P2]. The publication was published in WSEAS journal (WSEAS – Journals, 2010). The journal approached exchange of tracking information more widely. Also the risks are considered more thoroughly. Also satellite-based tracking in general is explained more comprehensively.

7.4 Discussion of the Publications

In general, risks around satellite-based navigation is a huge field and therefore lots of the tasks are yet undone. This thesis and SATERISK-project in general covers only a little of the topic and therefore more research work and co-operation is required. The project needs more participants to provide more information.

Especially the first publication shows, how the adaptability of the criminals is a challenge for law enforcement and logistics companies. Self learning devices are required to face interference and countermeasures are required to be planned beforehand. Countermeasures depend a lot about current case and if the driver of the tracked vehicle is aware of the device.

More tests are required and development work on tracking devices and background system is essential. Also A-GPS and any other aid should be considered, although also they have same restrictions about jamming.

The second and the third publication showed up risks about tracking solutions between organizations. It also brought up a problem between publicity of the academic research and providing tools for law enforcement agencies. It is natural, that all the used tools should not be published because it would give too much help for criminals to countermeasure them. On the other hand research work, especially when doing it as an academic project, should be open and under critique.

International co-operation is everyday business in police work, through Europol and Interpol. Still, technical co-operation is really limited and should be used more often. Criminals are

getting more and more international, so why police operations should be limited by national borders in integrating Europe?

8 DISCUSSION AND CONCLUSIONS

Topic in general is really interesting and it has multiple aspects. Administrational and technical frames create own limitations for applications and legislation should not be forgotten. In fact, legislation may cause biggest paradigm also in this topic, because only one side obeys the rules. We need to share information, but also limit information about exact applications to the authorities. Balance between public studies and private or governmental interests may cause problems in some cases.

In the future, conferences, workshops and international administrative meetings are required to provide possibilities to offer international level tracking applications with limited and acknowledged risks. Work between different sectors should be more encouraged to get several points of view and so create more solid and working solutions. Changes in the future have to be considered in beforehand. For example 4G, GALILEO and alternative positioning methods need research beforehand.

Too much reliability to some technology should be considered as a risk. GPS signal is interruptible and in crisis situation probably not available. Also the future of the entire GPS has been questioned, GPS satellites have only certain lifetime and need to be replaced (GIS conference – papers, 2005). One solution for GPS dependency is forthcoming European positioning system, GALILEO. Timetable of the project have been postponed several times, but cancellation of the project doesn't seem likely.

Also other positioning methods should be considered. Base stations of the mobile phones are used already as a backup and also WLAN positioning is under research. For example Ekahau is distributing challenging indoor positioning system, which has been proved to be quite reliable. (Ekahau, 2010)

In the future more workshops, conferences and meeting are required. Although SATERISK-project is found to gather information about risks and countermeasures in satellite-based tracking and navigation, it should not try to solve every problem. When creating solutions and procedures, It should first be tested locally, then nationally and finally EU-level. Some backup from European authority, like Frontex or Europol is required, but they are more willing to adapt already working solutions than principles with no proof of concept.

In general, satellite-based tracking is used to protect valuables and to get better situation awareness. When using satellite-based tracking especially in multinational environment, standard procedures are essential to get work done. Unfortunately world is full of bad examples of this. For example, lack of situation awareness was also one of the main issues when organizing search of the remains in Air France flight 447. False information, multinational search force with no common procedures and not working lead caused long delays for operation. (Hellenberg, 2009)

SATERISK project have had a good start and has got a good feedback in conferences, but lot of the work is still to be done and many different points of view will be found before project is over. We are in a right road, but have long way to go.

REFERENCES

EK - risk management, 1998, Confederation of Finnish Industries EK, Pk -risk management. http://www.pk-rh.com, (18.10.2009)

Ekahau, 2010, http://www.ekahau.com, (06.04.2010)

ESA – Navigation – The future – Galileo, http://www.esa.int/esaNA/galileo.html, (02.02.2010)

Findarticles – technology, 2008, http://findarticles.com/p/articles/mi_m0BPW/is_10_13/ai_n27578121/, (10.04.2010)

Garmin – What is GPS, http://www.garmin.com/aboutgps, (20.02.2010)

GIS conference – papers, 2005, http://gisconference.cas.psu.edu/2005/proceedings/4_tues_1030.pdf, (11.04.2010)

T. Hellenberg, Pelastustieto magazine, "Tilannetietous on kriisinhallinnan nro 1" (Situation awareness is number one in crisis management), Palo- ja pelastustieto ry, 06/2009 (in Finnish)

Iltalehti magazine, "Slovakiassa siirryttiin Ison Veljen valvontaan" (Slovakia uses "big brother" in road tolls), Article is in Finnish, (29.1.2010)

O. Pozzobon, 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.

Standford University – News release, 1995 http://news.stanford.edu/pr/95/950613Arc5183.html, (20.03.2010)

J. Viitanen "Requirement analysis of the SATERISK-project" Thesis work, done for Laurea University of Applied Scienses, 2009

WSEAS – Journals, 2010, http://www.worldses.org/journals/systems/systems-2010.htm, (06.04.2010)

CONTENT OF THE APPENDICES

Appendix 1: Publication [P1], Jamming Detection in the Future Navigation and Tracking Systems

Appendix 2: Publication [P2], International and Transorganizational Information Flow of Tracking Data

Appendix 3: Publication [P3], Near Border Procedures for Tracking Information

PUBLICATION [P1]: M. HAPPONEN, J. VIITANEN, P. KOKKONEN, J. OJALA & J. RAJAMÄKI, “JAMMING DETECTION IN THE FUTURE NAVIGATION AND TRACKING SYSTEMS”, IN PROCEEDINGS OF THE 16TH SAINT PETERSBURG INTERNATIONAL CONFERENCE OF INTEGRATED NAVIGATION SYSTEMS, ST. PETERSBURG, RUSSIA, MAY 2009. ISBN 978-5-900780-69-6, PP. 314-317

JAMMING DETECTION IN THE FUTURE NAVIGATION AND TRACKING SYSTEMS

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

Laurea Leppävaara, Vanha maantie 9, FI-02650 Espoo, Finland

markus.happonen@laurea.fi

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. An 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 and/or GLONASS with no risk analysis. Popularity of satellite navigation still grows while Russian GLONASS is re-established and the EU:s new satellite tracking system Galileo will become operational in 2013. Also, China and India are preparing their own satellite navigation systems Beidou and IRNSS.

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 found. At the moment SATERISK project is in a relatively early phase and the 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 (SATEllite positioning RISKs) is a Finnish 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) and Russian based GLOSNASS (Globalnaja navigatsionnaja sputnikovaja sistema) satellite positioning systems 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 SATERISK 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 on the whole tracking value chain, 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 the 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.

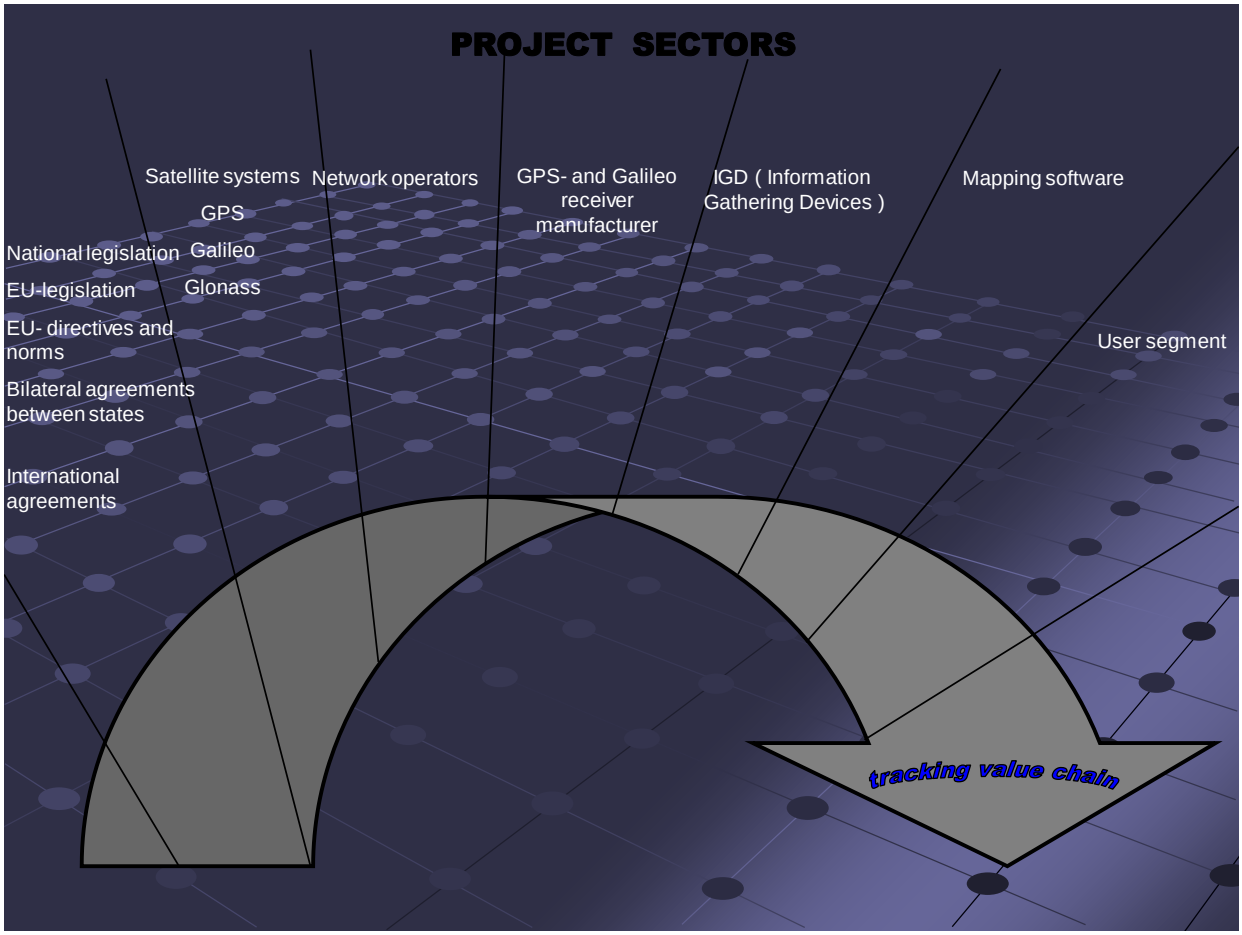

Figure 1, Project sectors

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 a 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 civil tracking systems.

Naturally all interference is not 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 handled 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 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 the 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 systems have been under development by several private companies and one advantage in this system is that road tolls accumulate with driven kilometres. Finnish ministry of transportation and communications has also 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 a 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

In some occasions, it is difficult to separate intentional and unintentional interference from each other, for example, when a tracking device enters a tunnel or 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 the 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 is close to lucky guess to separate them.

Frequency jamming is not 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 transceivers, 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 are getting better all the time, and better algorithms and countermeasures are needed for detecting them.

Jamming of GSM signal is relatively easy to spot, because of the wide coverage of signal. If the GSM signal is interrupted, the reason is a broken mobile device, a 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, the usage of a fake base station is one of the hardest. Fake base stations capture all signals of mobile phones, speech, SMS and data, and the user of a 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, the device can compare current cell ID with cell IDs of current tracking area. This will need a more sophisticated tracking device, because connection to the server is not 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 counteraction to 1interference is an immediate alarm to the local unit. Especially, with regard to transportation of valuable goods it is 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 will be very near to real time. The priority of security system should be to prevent incidents and crimes, not to help their investigation afterwards.

Some standard counteractions for interference can be decided, but they still need to be tested beforehand. If tracking device transmissions are interrupted, the 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 another 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 the 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 systems are jammed; there basically is no 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

As stated earlier in the paper, the SATERISK project has just lately begun and there is lots of research work to be done. Although SATERISK gets some funding from the Finnish Funding Agency for Technology and Innovation (TEKES), it is a relatively small player in the field of positioning. The main goal of the project is to improve knowledge of the possible risks regard to positioning and tracking. This knowledge will point out new features needed with regard to tracking devices and background systems. In the future these features need to be tested as a part of the project. The SATERISK project needs to find balance between security and usability of tracking as a security device. After all, users themselves are one of the main risks with regard to technical system and therefore also user habits need to be charted.

Possible changes to international legislation and regulations need lots of work, but it is better to leave these questions for the professionals of that topic. The juridical part of the project will be researched in University of Lapland. Communication security has to be improved, but that is likely made with already existing solutions.

In general, the SATERISK project is trying to look into the future by finding forthcoming 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 risks, but can actually create them and therefore a risk assessment is needed before using them. When looking at the history of ICT, today's solutions have often turned out to be tomorrow's problems. Is this applicable and/or avoidable regarding Galileo?

REFERENCES

[1] 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
[2] Tekniikka&talous magazine 7.12.2008, available in Finnish:
http://www.tekniikkatalous.fi/ict/article194088.ece
[3] Parliament of Finland, YmVL 12/2008, online document (in Finnish) Available:
http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ymvl_12_2008_p.shtml
[4] (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+Wednesday/1135231511615
[5] T. Olsen, B. Forssell, "Susceptibility of Some Civil GPS Receivers", GPS World (2003), Available:
http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=43432
[6] 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
[7] 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).
[8] TAYX –online catalogue, Available: http://www.tayx.co.uk/default.html
[9] GPS Pseudolite rover project. Available: http://sun-valley.standford.edu/users/rover/
[10] 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:

PUBLICATION [P2]: J. VIITANEN, M. HAPPONEN, P. PATAMA & J. RAJAMÄKI, “INTERNATIONAL AND TRANSORGANIZATIONAL INFORMATION FLOW OF TRACKING DATA”, IN PROCEEDINGS OF THE 8TH WSEAS INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY (ISP ’09), PUERTO DE LA CRUZ, TENERIFE, SPAIN, DECEMBER 2009. ISBN 978-960-474-143-4, PP 111-115

International and Transorganizational Information Flow of Tracking Data

JOUNI VIITANEN, MARKUS HAPPONEN, PASI PATAMA & JYRI RAJAMÄKI
Laurea Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9,
FI 02650 Espoo, FINLAND
Corresponding Author: jouni.viitanen@laurea.fi, www.laurea.fi

Abstract: - European integration has increased transport of the illegal goods and criminals. Therefore transmitting tracking and other status information between nations and different organizations should become every day business. The goal of the paper is to find possible bottle necks in international co-operation between authorities and to find possible solutions for them. Following area can be considered as a part of the SATERISK project [1] that aims at a situation where laws on positioning and tracking and the financial risks posed by their usage will not prevent the use of machine-to-machine (m2m) tracking across state and union borders. The target of the paper is to present administrative and technical solutions to improve multi-organizational tracking solutions. Namely, make it possible to create timely situational picture in joint in multinational and inter agency operations. This paper will provide guidance for preparing appropriate plans and doctrine proposals for joint operations and training. Also, technical solutions and bottlenecks are briefly covered in this paper.

Key-Words: - Navigation, Positioning, Interfaces, Tracking, Doctrines.

1 Introduction

In the past decade, tracking have become essential and valuable tool for authorities to prevent and examine crimes [2]. At the same time, criminal nature and organized crime have internationalized, mostly due to European integration. The change has been rabid and therefore law enforcement authorities (LEA) have failed to create protocols and procedures to deal international tracking issues. This paper addresses the problems of LEA with regard to cross-border operations and explains how they differ from other operations. It focuses on the operational level of action and addresses issues across the range of LEA operations. Its goal is to reveal the need for technical help and doctrinal guidance focused on tasks on or over borders. It examines the special considerations required when conducting operations in or over the complex modern border environment. Many of these problems are also present in other than nation state borders, but also in other governmental borders.

It is always more efficient to prevent than to repair damages [3]. Unfortunately, preventing is even more difficult than crisis management, due to information- and time criticalness. Currently, the Geographical Information System (GIS) is mostly used for analyzing thing after they had happened or trying to make logistics more efficient, but not for preventing unwanted thing from happening.

The military has got used to utilize GIS-systems. Also, some LEA-authorities are good at this, but the trouble lies on the borders, being it a nation-state or juridical border.

The European Council held a special meeting on 15 and 16 October 1999 in Tampere on the creation of an area of freedom, security and justice in the European Union. The meeting called for joint investigation teams to be set up without delay with a view to combating trafficking in drugs and human beings, as well as terrorism. In the year 2005 and 2006, there were only two join investigation groups [4]. And these were investigation teams, trying to find out what happened, although in the long run that will also help in prevention.

2 Administrative Challenges

When something illegal has happened, it is mandatory for the LEA-authorities to act and failing to act may result legal actions. But failing to get or share the information from or with the partners is in many cases a volunteer action, although the information would prevent something unwanted. Also, sharing the information is often a complicated legal issue. Therefore in many cases, not sharing the information is much easier and safer choice for the officers' own well being.

Today, LEA agencies are using more tracking technology than ever before. Early systems were point to point systems, where the surveillance team was receiving the information through point to point radio communication. Nowadays, systems are running more on network (GSM&TCP/IP) based, and they can send and receive the information basically anywhere. These days, technical tracking is used in smaller and smaller cases.

Many cross-border joint ventures are targeted at some big incidents, although smaller separate cases together are creating the biggest flow. That means that all the cases cannot go through the same hierarchical command system, because there are too much of cases. Boarders are creating delay for LEA as shown in Fig. 1, and thereupon a crime preventing work will often change into an investigating one.

Border is a part that forms the outer edge of something [6]. It is a very thin line, and if LEA officers want to be successful, they need a lot of information about both sides of the border. The big question is how to overcome those problems described in Fig. 1.

The exchange of information with people from other organizations during crisis situations is often done informally. These contacts are not institutionalized, but are established on a personal basis. Information is shared more easily with people that one knows and trusts. [7] But could it be generally accepted that real time information sharing in law enforcement between parties is based on personal contacts? Unfortunately, in many cases this is the only way to change metadata about the properties and status of the target. If the information

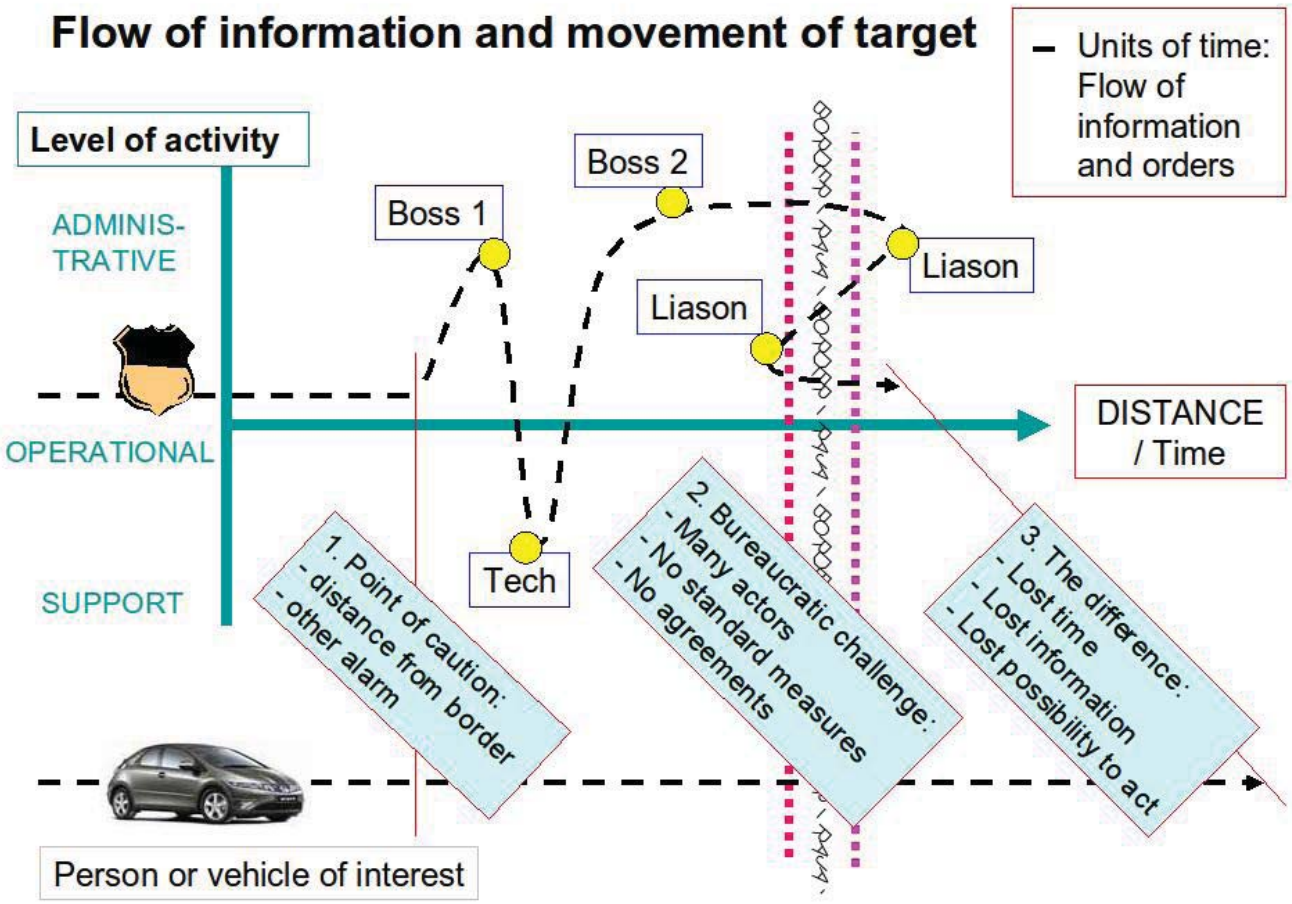

Fig. 1. Informal flow on boarder [5]

exchange is based completely on personal contacts, it is clear that technology can create only limited help. Another bad thing is that in the same time you get to be very dependant of key persons. Absenteeism or loss of a key individual who cannot be readily replaced should not be a threat to public safety.

In the EU-level, LEA organizations are changing information. Europol is the European Law Enforcement Organization which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organized crime. Europol's task is to handle criminal intelligence. [8] Europol works mainly on a political level, because at the operational level the pursuit of Europol is simply too slow. Therefore, some principles agreed beforehand are needed. Currently, the change of information LEA organizations helps just in the case of investigation or in statistics, but not at the operational level.

3 Auto Release for Doctrines

There are hundreds of tracking operations going on in Europe every moment. They are carried out within small proprietary teams. The teams know where the contraband comes, and where it is going. They have the big picture how to investigate, but they don't have the real-time big picture how to prevent. This leads to inefficiency.

In traditional organizations, knowledge tends to flow along organizational lines, from the top to the down. The knowledge might be created in lower parts of the organization, but for spreading out, it usually must first go to the top, and only from there it can spread. This pattern seldom results in making knowledge available after a timely fashion and where it is needed most. Also, dependency of certain employees may cause vulnerabilities to information flow.

Preventing crimes is very time critical business, and law enforcement authorities are usually very traditional and hierarchical organizations. This seems to be a trouble combination, although a long tradition also has good points of view. The time criticality has forced to created shortcuts for the normal operational information passing most of the hierarchy. In most cases, information is send and used in timely manner. Information can flow across organizational lines, reaching the right people who can use it in such a way that best serves the goal of the organization in question.

But if the case is such as not repeating itself constantly, e.g. a case dealing with a boarder that you don't cross every day, you might end up in situation, that you don't have shortcuts anymore. Then the information will start to go up and down the ladders of hierarchy and the moment is lost.

A doctrine is defined as a principle of law established through past decisions, a statement of fundamental government policy especially in international relations or a military principle or set of strategies [9]. The normal way of LEA to go is to create doctrines. A doctrine will give you advice how to proceed in any given situation. In any organization there are lot of doctrines, the problem is to remember of find them. Now people are asking advice from their superiors and consuming precision time as in the picture.

Our answer is to combine tracking systems and situational awareness systems with doctrine libraries. To successfully execute this, we need a lot more information from the target than just the position. We need real time status and profile information to combine the threat to right doctrine. Unfortunately, many systems are only producing the positioning; there is no profile or status information in the message. This situation must be changed.

4. Technical Challenge

Tracking applications have usually been organizational or national, although some commercial devices are nowadays more widely in use. Many of the tracking solution providers offer integrated systems, where tracking devices and mapping software are combined. Traditionally these systems are designed to be standalone services with no proper way to communicate with other mapping systems. If some interface and protocol exist, possibility to send properties and status information; so called metadata, is still missing. Differences in devices, protocols and background systems have caused problems for international co-operation, simply because of lack of the commonly agreed interfaces.

Although standardization of the mapping software and transmission protocols is not necessary, some common translation to pass information is needed. Exchange of information should be automated between computers. This information flow should be based to organizational doctrine libraries, created beforehand.

A special conference or workshop for technical specialists is thereby needed. Workshop should be organized by a European joint organization, such as Europol or Frontex; EU's agency for external border security [10]. This would give weight for decisions

and also reduce financial arguments. When building up multinational tracking data exchange system, costs are small when compared to benefits of international co-operation of authorities.

Main goal for the technical meeting is to find suitable way to share tracking information abroad with no delays. Certain protocols and operation procedures are needed. Possibility to adopt already existing methods, e.g. from military, should be considered. Currently the National Marine Electronics Association (NMEA) protocol is used in some international sharing. [11] But for real time surveillance it is not sufficient; because NMEA does not provide possibility to send metadata.

Transmission protocol is not the only issue in multinational tracking network. Also, the applied network topology has to be decided. One possible topology is presented in Fig. 2. Today, criminals applies more and more technology [12]. So, all data transfer is encrypted and protected with virtual private network (VPN). A question to sort out is that should the tracking information be encrypted also inside private network? If so, the easiest way is to use common public and private key solution. All the public keys should be stored into the one server connectible in the private network.

When connection to the other LEA authority is needed, transmitting server acquires needed public keys from dedicated server, encrypts and sends messages to the receiver. When the receiving server gets new encrypted message, it automatically decrypts data (if transmitting server is in "allowed" list) and ask permission to create new target to the map, if it does not already exist. If data transmission is nearly on daily basis, auto-permission procedure should be used.

Second main topic for international consortium is to find reliable ways to change additional information during the tracking. This, so called metadata contains necessary information about target and therefore should be transmitted also to the foreign authorities. Metadata is information about target, such as for example details about target vehicle, possible risks of the target (target being. armed?) and preferred actions against target. Like always in such operations, all data should be encrypted. All metadata should be sent among spatial information.

5. Future Work and Final Words

Today, many of the suggested solutions in our paper exist only on the drawing board. Therefore they need lots of testing and international cooperation. Technical and administrational meetings are required to build up international (or at least EU-wide) network system to handle tracking information flow. Some already existing working principles can be adopted e.g. from military, and therefore the usage of existing know-how should be considered. Especially, a common language for the metadata, such as the military standard MIL-STD 2525 in military side, should make it possible to apply doctrine libraries. Because of different legislation, even EU Member States must have little different doctrine libraries until united EU

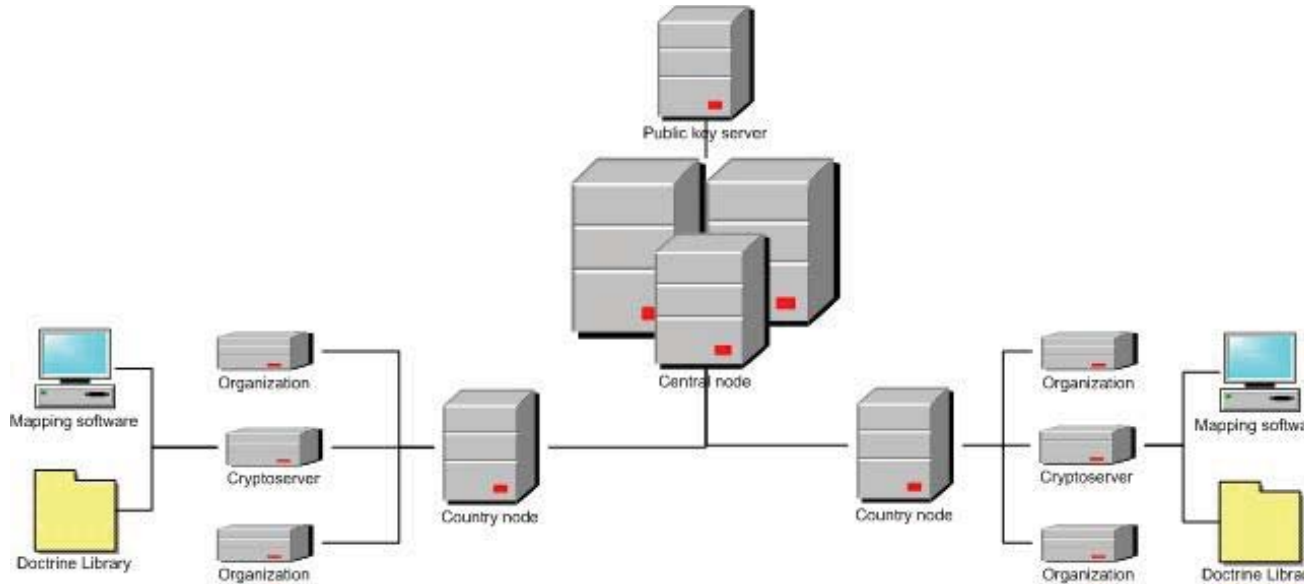

Fig. 2. Network topology

legislation is achieved. However, the main principles and the language should be the same.

Building up a new multinational tracking information system needs lots of political, administrational and technical decisions. It also needs lots of effort and time. Many bottlenecks and possible problems still need to be solved. However, co-operation is the key element for better results.

References:

[1] www.saterisk.com
[2] Viitanen, J., "Planning and requirement analysis of the SATERISK ‐ project", Master thesis, Laurea University of Applied Sciences, Espoo 2009. (In Finnish)
[3] Risk Management in SMEs, http://www.pk-rh.fi/en-1
[4] COM(2007)781. COMMUNICATION FROM THE COMMISSION on the 2007 Progress Review of the implementation of the EU Action Plan on Drugs (2005-2008) http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=196512
[5] Viitanen, J. Presentation, Situation Scope I Seminar, Helsinki 20.-21. Nov., 2008.
[6] http://www.answers.com/topic/border
[7] Muhren, W., Jaarva, M.-M., Rintakoski, K. & Sundqvist, J., "Information sharing and interoperability in national, cross-border and international crisis management", Crisis Management Initiative, Tilburg University, Crisis Management Centre Finland & Elisa Ltd., June 2008. http://www.cmi.fi/files/ Interoperability_report.pdf
[8]. http://www.europol.europa.eu
[9] http://www.merriam-webster.com/dictionary/doctrine
[10] http://www.frontex.europa.eu
[11] http://www.nmea.org
[12] Happonen, M., Kokkonen, P., Viitanen, J., Ojala, J. & Rajamäki, J., "Jamming Detection in the Future Navigation and Tracking Systems", in Proceedings of the 16th Saint Petersburg International Conference on Integrated Navigation Systems, 25 - 27 May, 2009 Saint Petersburg, Russia.

PUBLICATION [P3]: J. VIITANEN, M. HAPPONEN, P. PATAMA & J. RAJAMÄKI, “NEAR BORDER PROCEDURES FOR TRACKING INFORMATION”, WSEAS TRANSACTIONS ON SYSTEMS, ISSUE 3, VOLUME 9, MARCH 2010. ISSN 1109-2777, PP. 223-232

Near Border Procedures for Tracking Information

JOUNI VIITANEN, MARKUS HAPPONEN, PASI PATAMA & JYRI RAJAMÄKI
Laurea Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9,
FI 02650 Espoo,
FINLAND
Corresponding Author: jouni.viitanen@laurea.fi, www.laurea.fi

Abstract: - European integration has increased the transport of illegal goods and other criminal activity. Therefore the transmitting of tracking and other status information between nations and different organizations should become an everyday business. The goal of this paper is to find possible bottle necks in international cooperation between authorities and to find possible solutions for them. The following area can be considered as a part of the Finnish SATERISK research project that aims for 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. The target of the paper is to present administrative and technical solutions to improve multi-organizational tracking solutions. Namely, the goal is to make it possible to create a timely situational picture in joint multinational and interagency operations. This paper will provide guidance for preparing appropriate plans and doctrine proposals for joint operations and training. Also technical solutions and bottlenecks are briefly covered in this paper.

Key-Words: - Borders, Doctrines, Interfaces, Navigation, Positioning, Satellite navigations, Tracking.

1 Introduction

In the past decade, tracking has become an essential and valuable tool for authorities to prevent and investigate crimes [1]. At the same time, criminal nature and organized crime have internationalized, mostly due to European integration. Within the last decade, criminals have also become more technically oriented. Some countermeasures for tracking applications have been found from the hands of the criminals [2], and therefore international cooperation between officials becomes even more vital.

The change has been rabid and therefore law enforcement authorities (LEA) have failed to create protocols and procedures to deal with international tracking issues. This paper addresses the problems of LEA with regard to cross-border operations and explains how they differ from other operations. It focuses on the operational level of action and addresses issues across the range of LEA operations. Its goal is to reveal the need for technical help and doctrinal guidance focused on tasks on or over borders. It examines the special considerations required when conducting operations in or over the complex modern border environment. Many of these problems are also present in non-national or state borders, but also in other governmental borders.

It is always more efficient to prevent than to repair damages [3]. Unfortunately, preventing is even more difficult than crisis management, due to information and time criticality [4]. Currently, the Geographical Information System (GIS) is mostly used for analyzing situations after they have happened or trying to make logistics more efficient, but not for preventing unwanted events from happening.

The military has become accustomed to utilizing GIS. Also, some LEA are good at this, but the trouble remains on the borders, be it a nation-state or juridical border. The European Council held a special meeting on 15 and 16 October 1999 in

Tampere on the creation of an area of freedom, security and justice in the European Union. The meeting called for joint investigation teams to be set up without delay with a view to combat the

trafficking in drugs and human beings, as well as terrorism. In 2005 and 2006, there were only two joint investigation groups [5]. These were post-event investigation teams, trying to find out what happened, although in the long run that will also help with prevention.

2 SATERISK Project

SATERISK (SATEllite positioning RISKs) is a Finnish research project, which aims at a situation where laws on positioning and tracking will allow the use of so-called m2m (machine to machine) tracking devices across state and union borders. [6]

The project aims to bring new know-how on an international level 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) and Russian-based GLOSNASS (Globalnaja navigatsionnaja sputnikovaja sistema) satellite positioning systems will soon get an EU counterpart and rival from Galileo [7]. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. The SATERISK project also aims to offer technological solutions to issues that arise 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 on the whole tracking value chain, as shown in Fig. 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. This paper is mostly focused on the international co-operability. Technical issues are mainly studied by Laurea University of Applied Sciences, for example, security [8], fail resistance and high usability. A concept of satellite tracking system is shown in Fig. 2.

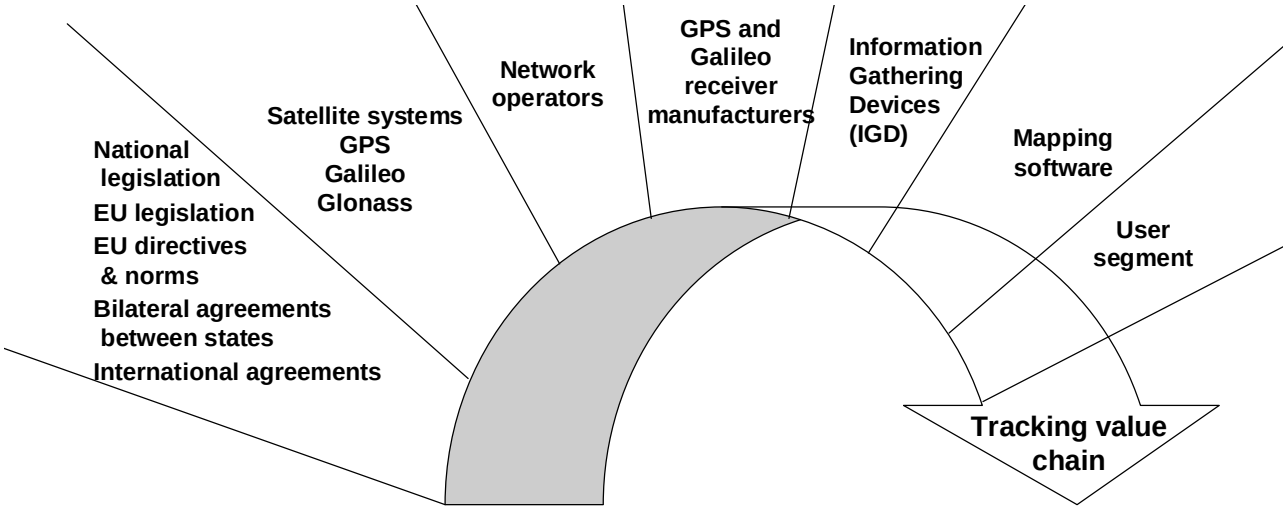

Fig. 1 Sectors of SATERISK project

3 Administrative challenges

When something illegal has happened, it is mandatory for the LEA to act, and failing to act may result in legal actions. Failing to obtain or share the information from or with the partners, however, is in many cases a volunteer action, although the information could prevent something unwanted. Also, sharing the information is often a complicated legal issue. Therefore in many cases, not sharing the information is a much easier and safer choice for the officers' own well being.

Today, LEA are using more tracking technology than ever before. Early systems were point-to-point systems, where the surveillance team was receiving the information through point-to-point radio communication. Nowadays, more systems are network-based (GSM & TCP/IP), and users can send and receive the information basically anywhere. These days, technical tracking is used in fewer and fewer cases.

Many cross-border joint ventures are targeted at some big incidents, although smaller separate cases together are creating the biggest flow. That means that all the cases cannot go through the same hierarchical command system, because there are too many cases. Borders often create delays for LEA as shown in figures 1-4, and therefore a crime preventing work will often change into an investigation.

In Fig. 3 there is a normal real-time tracking situation, where the local LEA is getting the target's position in near real-time, only with a few seconds delay.

Fig. 4 presents the point when the LEA starts to be worried that the target might go across the border,

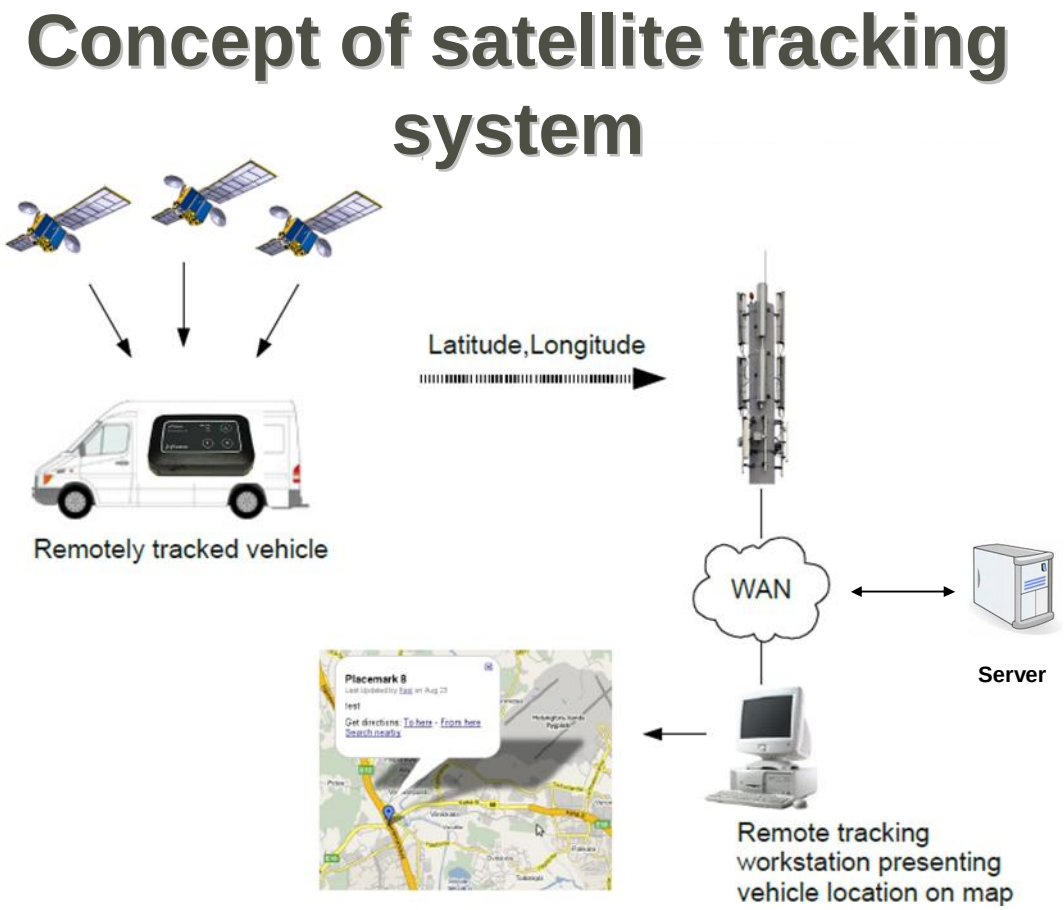

Fig. 2 Concept of satellite tracking system

but the tracking is still near real-time. A border is a very thin line, and if LEA officers want to be successful, they need timely information about both sides of the border. Border guards are very seldom responsible for tracking, so in many cases they do not have the information.

After the target crosses the border (Fig. 5), the trouble starts. The target's timeline is still straight-forward, but now the LEA starts to use time in discussions with superiors to find out how to proceed in the new situation. There is still no information on the border or on the other side.

The exchange of information with people from other organizations during crisis situations is often done informally. These contacts are not institutionalized, but are established on a personal

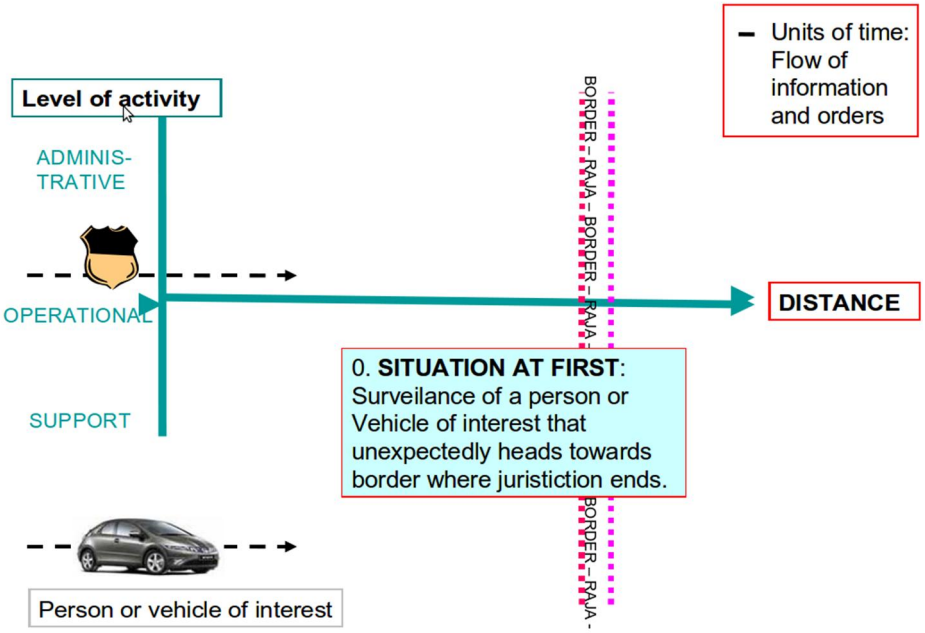

Fig. 3 Flow of information and movement of target – Start situation [9]

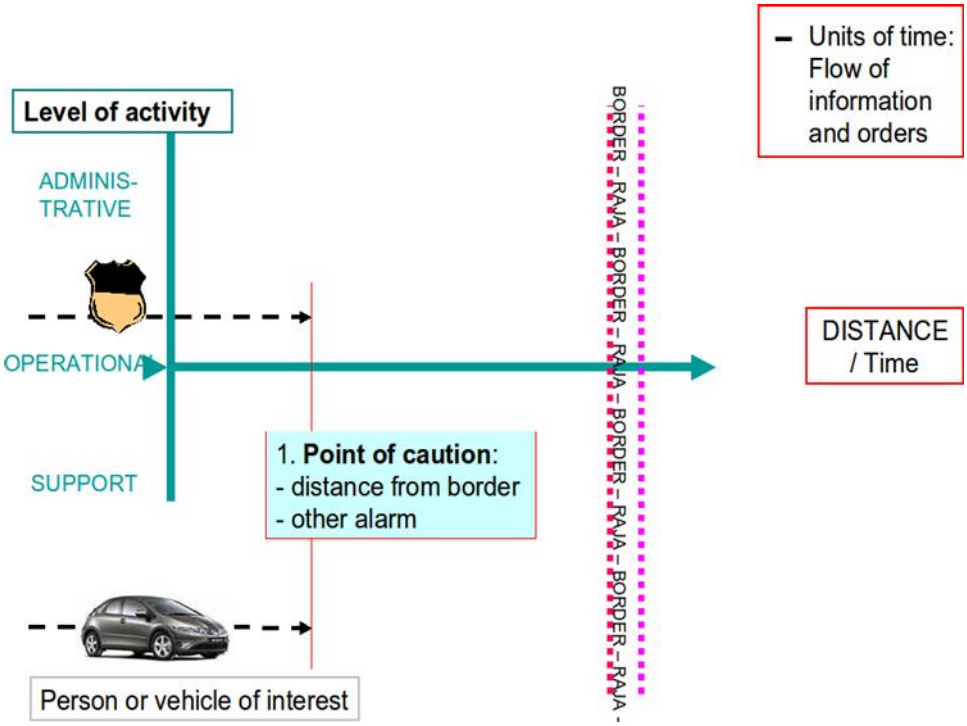

Fig. 4 Flow of information and movement of target – Point of caution [9]

basis. Information is shared more easily with people that one knows and trusts [10]. Is it accepteable that real-time information sharing in law enforcement between parties is based on personal contacts? Nowadays it is commonly the only way to change metadata about the properties and status of the target. If the information exchange is based completely on personal contacts, it is clear that technology can create only limited help. Another disadvantage is dependency of the key persons. Absenteeism or loss of a key individual who cannot be readily replaced should not be a threat to public safety.

The real-time tracking might be still on, but the

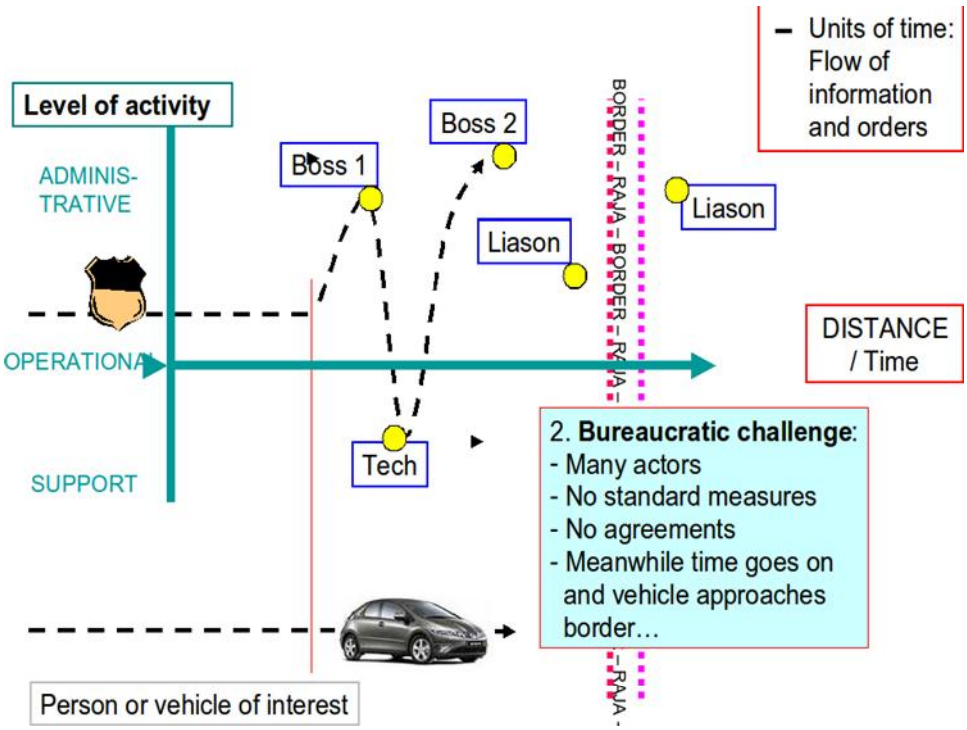

Fig. 5 Flow of information and movement of target – Bureaucratic challenge [9]

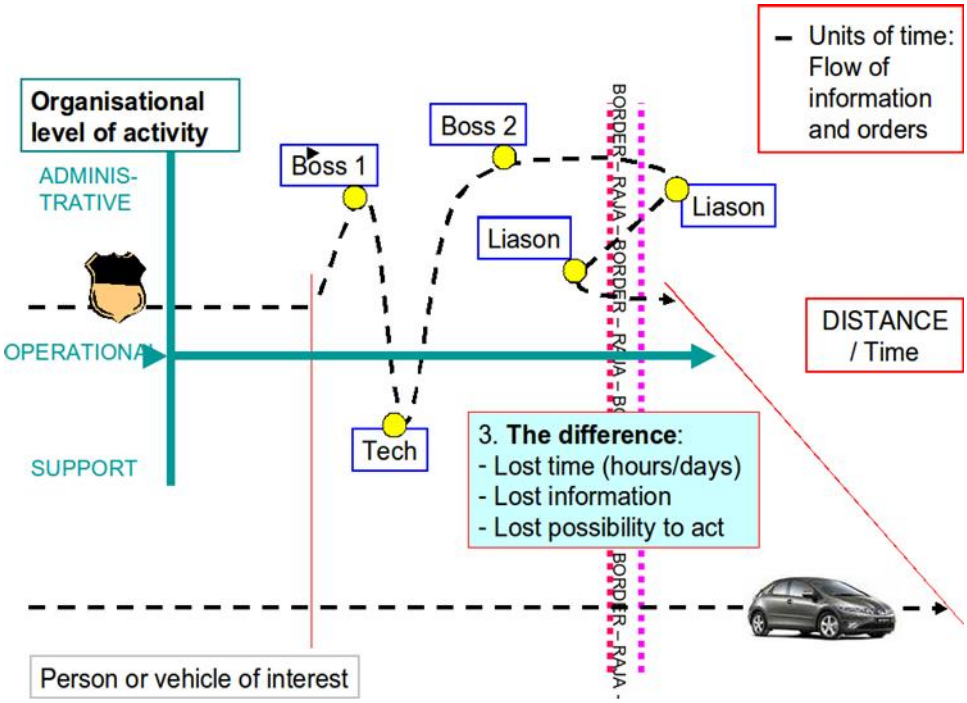

Fig. 6 Flow of information and movement of target – Information is lagging [9]

target is over the border and the information stays on the wrong side of the border as seen in Fig. 6. Tracking information is often most critically needed by LEA near the target. In this scenario is not there where it is needed.

At the EU-level, LEA organizations are exchanging information. “EUROPOL is the European Law Enforcement Organization which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organized crime.” EUROPOL’s task is to handle criminal intelligence. [11] EUROPOL works mainly on a political level because at the operational level the pursuit of Europol is simply too slow. Therefore, some principles agreed to beforehand are needed. Currently, the change of information between LEA organizations helps just in the case of investigation or in statistics, but not at the operational level.

There are hundreds of tracking operations going on in Europe at every moment. Operations are done with small proprietary teams. The teams know where the contraband comes from and where it is going, and so they have the big picture about the situation. This is essential for investigation purposes, but it doesn’t provide the real-time big picture required to prevent incidents. This leads to inefficiencies and ineffectiveness. Fig. 7 presents the worst case scenario, where as the situation progresses, the possibility to act is lost.

4 Auto Release for Doctrines

In traditional organizations, knowledge tends to flow along organizational lines, from the top to bottom. The knowledge might be created in lower parts of the organization, but for spreading horizontally, it usually must first go to the top, and only from there can it spread. This pattern seldom results in making knowledge available in a timely fashion and in the places where it is needed most. Also, dependency on certain employees may cause vulnerabilities to information flow.

Preventing crimes is a very time-critical business, and law enforcement authorities are usually very traditional and hierarchical organizations. This seems to be a troublesome combination, although a long tradition also provides some positive aspects. The time-criticality has forced officers to create shortcuts for the normal operational information, bypassing most of the hierarchy. In most cases, information sent in this way is received and used in a timely manner. Information can flow across organizational lines, reaching the right people who can use it in such a way that best serves the goal of the organization in question.

However, if the situation is not very common,

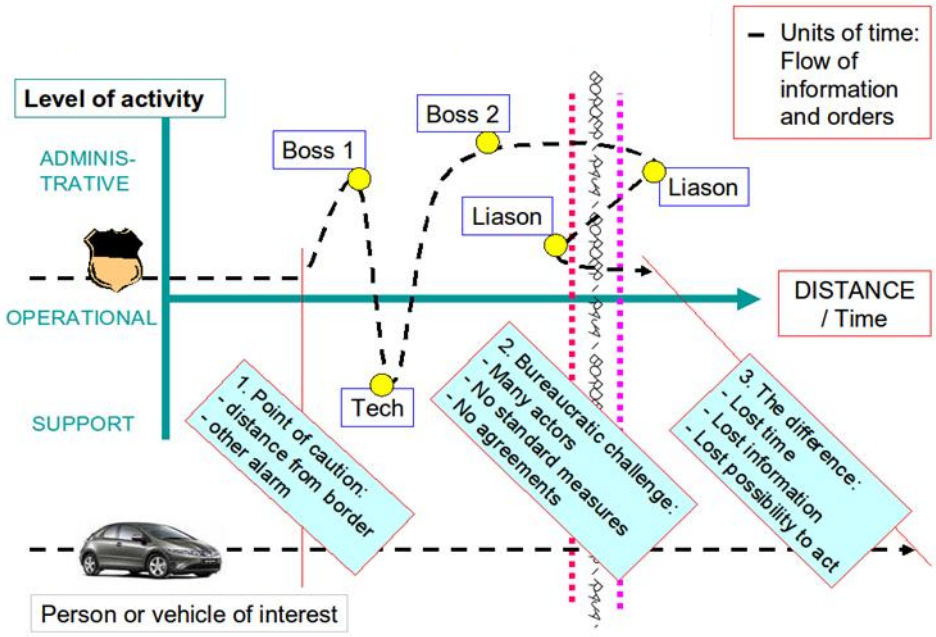

Fig. 7 Flow of information and movement of target – Lost possibility to react [9]

e.g. a case dealing with a border that you do not cross every day, you might end up in a situation where you do not have shortcuts anymore. Then the information will start to go up and down the ladders of hierarchy, and the opportunity for prevention is lost.

A doctrine is defined as a principle of law established through past decisions, a statement of fundamental government policy especially in international relations or a military principle or set of strategies [12]. LEA frequently create doctrines to guide their operations. A doctrine will give you advice on how to proceed in any given situation. In any given organization there are lot of doctrines, and the problem is to remember how and where to find them. This same type of problem is described in the context of facility management in [13]. The answer is also the same: the administrator must create control rules.

Our answer is to combine tracking systems (shown in Fig. 8) and situational awareness systems with doctrine libraries. To successfully do this we need a lot more information from the target than just the position. We need real-time status and profile information to match the threat to the right doctrine. Unfortunately, many systems are only producing the positioning information; there is no profile or status information in the message. This must be changed. In the private sector, companies know that the more information they have about customers, the easier it is to get more information. Customer information is the key to good customer support systems [14]. In this LEA tracking context it means that the more information you have about the target in the tracking messages, the better are the chances to succeed.

5 Technical Challenge

Tracking applications have usually been developed by organizations or national agencies, although some commercial devices are nowadays more widely in use. Many of the tracking solution providers offer integrated systems, where tracking devices and mapping software are combined. Traditionally these systems are designed to be standalone services with no built-in way to communicate with other mapping systems. If some interface and protocol exists, the possibility to send properties and status information, so-called metadata, is still missing. Differences between devices, protocols and background systems have caused problems for international cooperation, simply due to lack of commonly agreed interfaces.

The majority of tracking devices use GSM or a similar method of transmission [8]. Especially commercially available devices have in some cases been tailored to the certain environment. Because users of the tracking devices cannot be sure about networks in a foreign country (especially in the

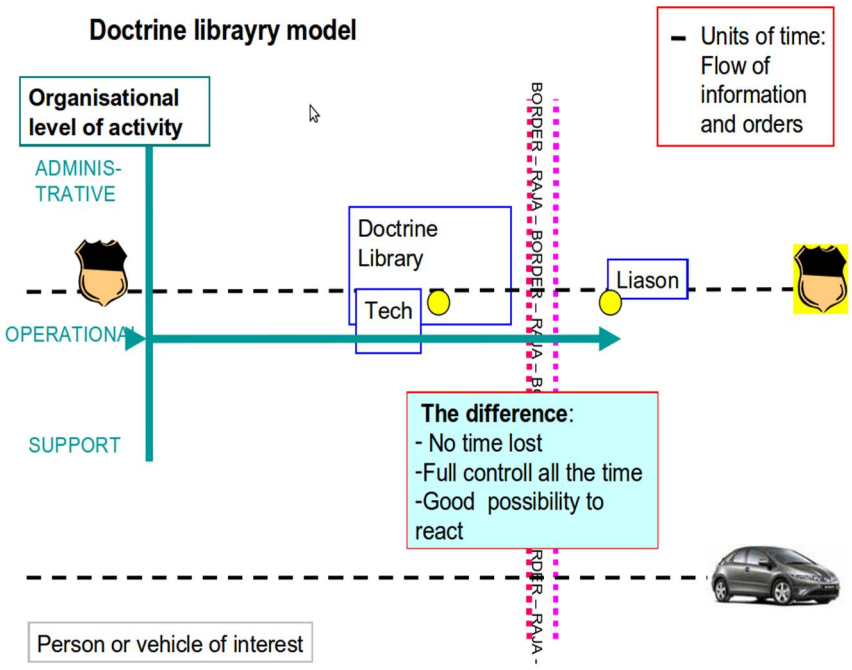

Fig. 8 Faster information flow with doctrine libraries

future), basic SMS capability is needed as a backup transmission method. Although standardization of the mapping software and transmission protocols is not necessary, some common translation to pass information is needed. Exchange of information should be automated between computers. This information flow should be based to organizational doctrine libraries, created beforehand.

Therefore, a conference or workshop for technical specialists is needed. Workshop should be organized by a European joint organization, like EUROPOL or FRONTEX, the EU's agency for external border security [15]. This would give weight for decisions and also reduce financial limitations. When building up a multinational tracking data exchange system, costs are small when compared to benefits of international cooperation of authorities.

Shared data should be considered critical information, and therefore appropriate data protection is required. More and more information and communications have become network-based, and accordingly the number of cyber-security incidents has increased. Although some nations have already established critical information infrastructure protection (CIIP) laws [16], European-level legislation is still missing.

When an information infrastructure is installed and all functions tested, the system should be tested against external and also internal cyber attacks to find possible vulnerabilities. Protection against external attacks and alternative routing with different IP addresses should be tested to provide necessary reliability for the system. Ref. [17] is one useful aid for planning security tests.

The main goal for the technical meeting would be to find a suitable way to share tracking information abroad with no delays. Certain protocols and operational procedures are needed. The possibility to adopt already existing methods, for example from military organizations, should be considered. Currently the National Marine Electronics Association (NMEA) protocol is used in some international situations, but for real-time surveillance it is not sufficient. For example, the NMEA protocol does not provide the possibility to send metadata. [18]

The lack of a transmission protocol is not the only issue in developing a multinational tracking network. A network topology also has to be agreed upon. One possible network topology is presented in Fig. 9. All data transfer is encrypted and protected with a virtual private network (VPN), but should tracking information also be encrypted inside a private network? If so, the easiest way is to use a common public- and private-key solution. All the public keys should be stored in one server connectible via the private network.

When a connection to another LEA authority is needed, the transmitting server acquires needed public keys from a dedicated server, and then encrypts and sends messages to the receiver. When the receiving server gets a new encrypted message, it automatically decrypts the data (if the transmitting

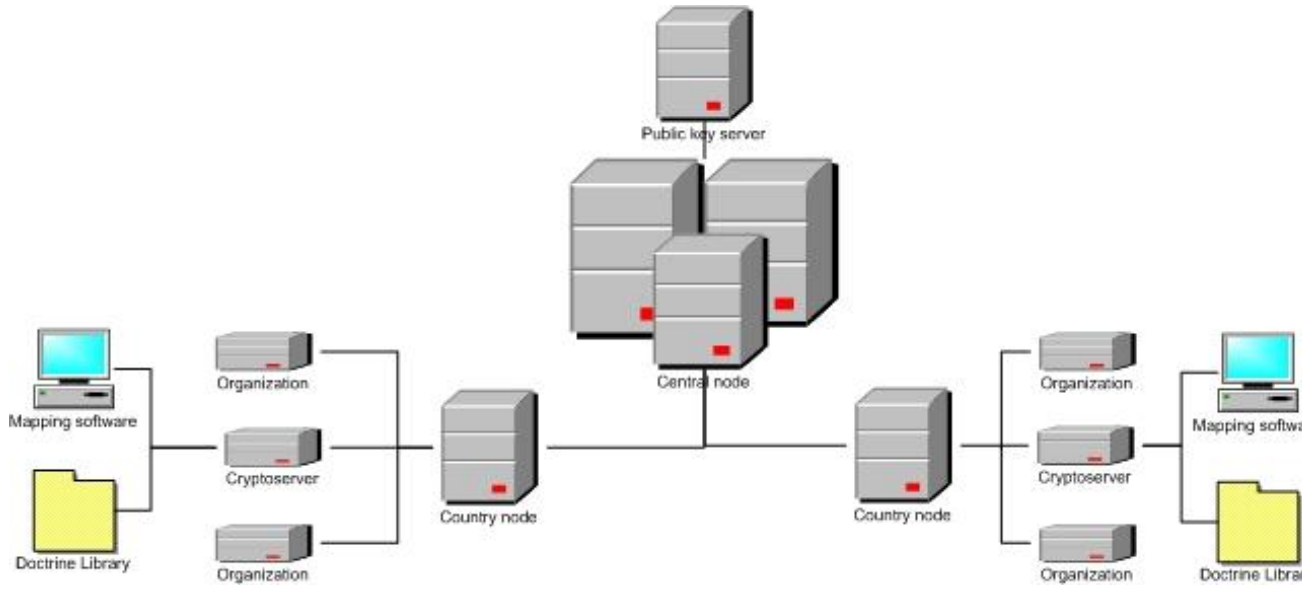

Fig. 9 Network topology

server is in the “allowed” list) and asks permission to create a new target to the map, if it does not already exist. If data transmission is on a nearly daily basis, auto-permission should be used.

The second main topic for this international consortium is to find reliable ways to exchange additional information during tracking. This so-called metadata contains necessary information about the target and therefore should also be transmitted to the foreign authorities. Metadata can include details about the target vehicle, possible risks of the target (e.g. armed) and preferred actions against the target. Like always, all data should be encrypted. All metadata should be sent along with the spatial information.

5 Future Work and Final Words

Many of the suggested solutions are now only on the drawing board, and therefore they need a great deal of testing and international cooperation. Technical and administrative meetings are required to build up an international (or at least EU-wide) network system to handle tracking information flow. Some currently functioning principles can be adopted, for example from military organizations, and usage of this existing know-how should be carefully considered. A common language for the metadata, like military standard MIL-STD 2525 [19], should make it possible to use doctrine libraries. Because of differences in legislation between countries, slightly different doctrine libraries may be needed until united EU legislation can be adopted. In any case, the main principles and the language should be the same.

Building up new multinational tracking information system requires many political, administrative and technical decisions, which will require lots of effort and time. Many bottlenecks and possible problems still need to be solved. Cooperation is the key for better results. The criminals are getting more international every day, and law enforcement should do the same

References:

[1] Viitanen, J., “Planning and requirement analysis of the SATERISK - project”, Master thesis, Laurea University of Applied Sciences, Espoo 2009. (In Finnish)

[2] Happonen, M., Kokkonen, P., Viitanen, J., Ojala, J. & Rajamäki, J., “Jamming Detection in the Future Navigation and Tracking Systems”, in Proceedings of the 16th Saint Petersburg International Conference on Integrated Navigation Systems, 25 - 27 May, 2009 Saint Petersburg, Russia, pp. 314-317. ISBN 978-5-900780-69-6

[3] Risk Management in SMEs, http://www.pk-rh.fi/en-1

[4] COM(2007)781. COMMUNICATION FROM THE COMMISSION on the 2007 Progress Review of the implementation of the EU Action Plan on Drugs (2005-2008), Available: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=196512

[5] Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. “International and Transorganizational Information Flow of Tracking Data”, Proceedings of the 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09), Puerto De La Cruz, Canary Islands, Spain, December 14-16, 2009, pp. 111-115.

[6] SATERISK project, http://www.saterisk.com

[7] 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

[8] Kämppi, P., Rajamäki, J. & Guinness, R., "Information Security in SatelliteTrackign Systems", Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09), Vouliagmeni Beach, Athens Greece, December 29-31, 2009, pp. 153-157.

[9] Viitanen, J. Presentation, Situation Scope I Seminar, Helsinki 20.-21. Nov., 2008.

[10] Muhren, W., Jaarva, M.-M., Rintakoski, K. & Sundqvist, J., “Information sharing and interoperability in national, cross-border and international crisis management”, Crisis Management Initiative, Tilburg University, Crisis Management Centre Finland & Elisa Ltd., June 2008. http://www.cmi.fi/files/Interoperability_report.pdf

[11] EUROPOL, the European Police Office, http://www.europol.europa.eu

[12] Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/doctrine

[13] Vásquez, J., Vásquez, J. & Travieso, C., “Dynamic Management Policies Embedded Digital Control Systems”, in Proceedings of the

8th WSEAS International Conference on E-Activities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 122-129.
[14] Lin, J., Chung, Y.-C., Yu, J. & Hsu, C., "A Construction Method for the Ontology of Customer Information in Customer Support System", in Proceedings of the 8th WSEAS International Conference on E-Activities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 66-71.
[15] FRONTEX, http://www.frontex.europa.eu
[16] Park, S. & Yi, W., "The Evaluation Criteria for Designation of Critical Information Infrastructure", in Proceedings of the 8th WSEAS International Conference on E-Activities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 77-83.
[17] Patriciu, V.-V.& Furtuna, A. C., "Guide for Designing Cyber Security Exercises", in Proceedings of the 8th WSEAS International Conference on E-Activities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 172-177.
[18] National Marine Electronic Association, http://www.nmea.org
[19] DOD MIL-STD-2525 COMMON WARFIGHTING SYMBOLOGY, Defense Information Systems Agency (DEPSO), Nov 17, 2008.