Faculty of Maritime Studies
University of Rijeka, Croatia

Royal Institute of Navigation
Science Technology Practice

The University of Nottingham

6th GNSS
Vulnerabilities and Solutions Conference

LAW ENFORCEMENT AUTHORITIES' SPECIAL REQUIREMENTS FOR GNSS

Jyri Rajamäki, Jouni Viitanen

Laurea University of Applied Sciences
Ratatie 22, 01300 Vantaa, Finland
E-mail: Jyri.Rajamaki@laurea.fi

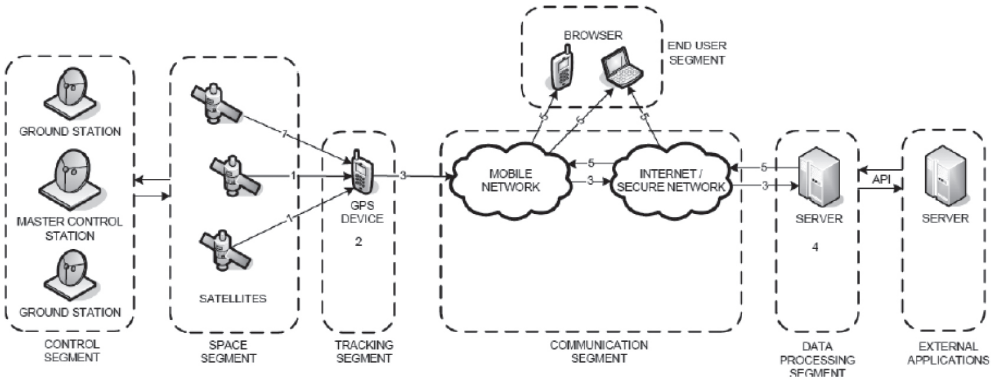
ABSTRACT. *Organised crime is a real threat in Europe with the emergence of international warehouses of crime. For improving their evidence-gathering abilities, law enforcement authorities (LEAs) are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organisations. The criminals' counter measure activities, such as electronic counter-surveillance, jamming and constant changes in behaviour for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new intelligent technologies, which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive, is emerging and is a high-priority task. With regard to the global navigation satellite systems (GNSS), LEAs have five operational and technological challenges: (1) commercial GNSS sensors do not fulfil the needs of LEAs; (2) cross-border operations are difficult because criminal nature has internationalised but LEAs are national organisations; (3) secure mobile communications is more and more important in all operations; (4) the surveillance data that LEAs collect should be valid in the court; and (5) LEAs' operations should be transparent ensuring sufficient privacy safeguards for the public.*

KEY WORDS: *GNSS, law enforcement, law enforcement authority, legality control, technical surveillance, tracking*

1 INTRODUCTION

Satellite-based navigation and tracking have become routine features of modern society and everyday life. Their use is still growing—a recent market research report predicts that the Global Navigation Satellite System (GNSS) market will likely double by 2016. The European Commission launched its first two operational satellites for the Galileo positioning system in October 2011. A modern satellite-based tracking system combines navigation and telecommunications technologies. The system is complicated and it consists of many technical segments, including the control segment, space segment, tracking segment, communication segment, data processing segment, application interface for external applications and end-user segment. The basic principle is that a tracked device is positioned by GNSS and positioning data is delivered for post-processing via mobile networks, the Internet or a secure network as shown in Figure 1 (Kämppi and Guinness, 2010). The system is complex and vulnerable of several kinds of cyber-attacks (Kämppi et al., 2009).

Figure 1
Principle of a satellite-based tracking system



GNSS-based tracking devices are able to calculate and deliver position information for post processing. Today many mobile phones include Global Positioning System (GPS) receivers, and phones are easy to turn into tracking devices by client software. For professional services and public authorities, TETRA clients and tracking-only clients (without communications functionality) are available. New positioning devices will support several systems, such as GPS, GLObalnaja NAvigatsionnaja Sputnikovaja Sistema (GLONASS) and Galileo, so that several techniques can be used simultaneously to guarantee better positioning accuracy and availability. GNSS-based tracking is used in

many applications, e.g. in logistics, fleet management, road tolls, traffic signal management. Also, Law Enforcement Authorities (LEAs) are using them e.g. for tracking suspects.

Professional criminals are aware that LEAs are gathering information about them, their actions and whereabouts. They have learned to find a tailing car among other traffic. GNSS-based tracking is a good tool for LEAs, because a small device under the car is harder to find than a tailing car. But criminals are learning, they have learned to check their vehicles and use other countermeasures. Therefore, LEAs needs new tracking sensors which are resilient to these countermeasures.

European LEAs' GNSS-based tracking sensors are based on GPS. U.S. Department of Defense operates the GPS systems, but they cannot guarantee to maintain global uninterrupted service. If GPS signals were switched off in Europe tomorrow LEAs efficiency would suffer heavily jeopardizing the public safety.

This article has five sections. The second section briefly introduces the empirical case, the SATERISK research project, in which the results and findings of this paper are based on. The third section shows the operational environment where LEAs apply BNSS-based tracking. The fourth section presents the findings with regard to the tracking challenges that LEAs have. The last section discusses the future role of GNSS-based tracking in LEAs' operations and presents future research topics.

2 ANALYTICAL FRAMEWORK AND METHODS

2.1 The SATERISK Research Project

Often new technologies will present opportunities for increased safety and security—and this is certainly true with satellite-based navigation and tracking—but they can also create new risks. It is important for the technology developers, end-users, and authorities to clearly understand these risks and take steps to mitigate them. Amongst all of the developments within navigation and tracking issues, Laurea University of Applied Sciences led a research project to investigate the risks associated with satellite-based tracking. The SATERISK (SATEllite positioning RISKs) project started in September 2008 and ended in December 2011. It aimed to answer the following questions:

- Does satellite-based navigation and tracking involve risks?
- Do we know what the risks are now and what they will be in the future?

The SATERISK project also aimed to bring new know-how to the European field of security. The project created new methods and development paths for positioning and tracking systems that address the risks and limitations that had already been discovered. These include methods related to information security, signal interference, and legal restrictions on tracking. A special emphasis had been placed on the use of satellite-based tracking amongst security professionals—both in the public and private sectors—where the risks could be high if they were not properly addressed. (Rajamäki et al., 2012.)

The SATERISK project had partners and other participants from the whole value-chain of satellite-based tracking; starting from the network operators like Cassidian Finland to companies that offer information-gathering devices and tracking software, and finally to the users of these tracking systems, such as Finnish Customs. The legal aspects of satellite-based tracking were studied at the University of Lapland in its own SATERISK co-project (Viikari, 2011).

2.2 Research Methodology

Neither computer science alone with its technical solutions nor psychology or other behavioural disciplines is able to address the challenges of today's security problems in a sufficiently integrated way. If we put innovative artefacts into action and analyse how they are used and how they perform, we will see things that cannot be seen in the lab. (Nunamaker, 2010.) Management information systems (MIS) involve three primary resources: people, technology, and information. The SATERISK project follows the basic development research in the MIS wheel diagram, first published by Nunamaker, Chan and Purdin (1991). In the concept of Development Research (DR), the continuum of scientific method using each aspect to inform system design as Design Science Research (DSR) choices and using systems technology to inform the science (March and Smith, 1995; Van Aken, 2004; Hevner et al., 2004). DR and DSR are research approaches that can be combined with other social science methods, such as the grounded theory or action research as well as case study research.

According to Nunamaker's (2010) "going the last mile" approach, the starting point of research should be a real problem for real people. In the SATERISK project, this real problem came from Law Enforcement Authorities who had exploited GNSS-based tracking but who had fretted about how it had been used. Nunamaker continues that the creation of innovative artefacts includes three phases: proof of concept (POC), proof of value (POV) and proof of use (POU). This means that a designed artefact is not really understood and cannot really be evaluated before it is actually implemented. In addition to POC and POV, they should also strive for POU. The SATERISK project integrates science both in

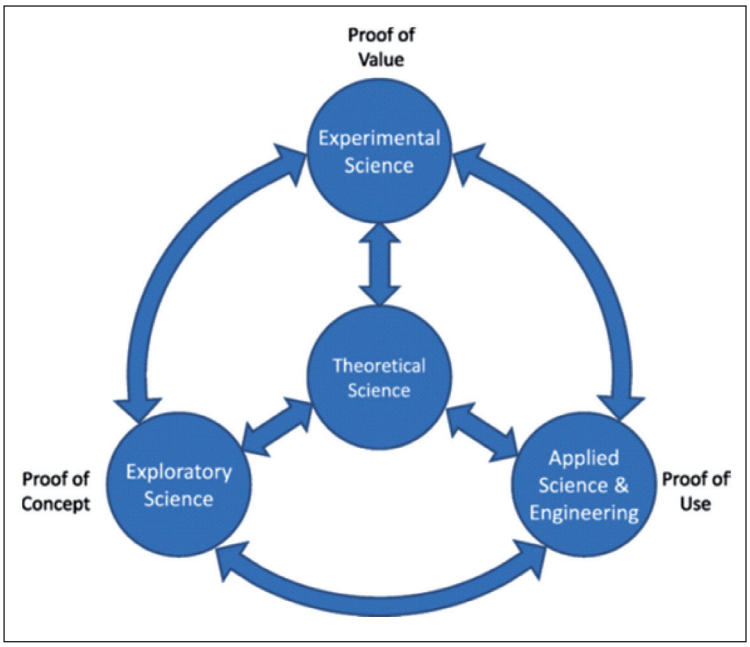


Figure 2
Integrated, multidisciplinary, multi methodological development research

the lab and in the field (see Figure 2), including the theory, prototype and validation by experiments or field study.

The SATERISK project has widely studied technical, operational and legislative risks from different points of view. All end-users of tracking devices and systems face some risks when they use tracking; also being tracked by someone else is a problematic issue. This paper presents the SATERISK project's main results with regard to the risks that law enforcement authorities face when they exploit tracking.

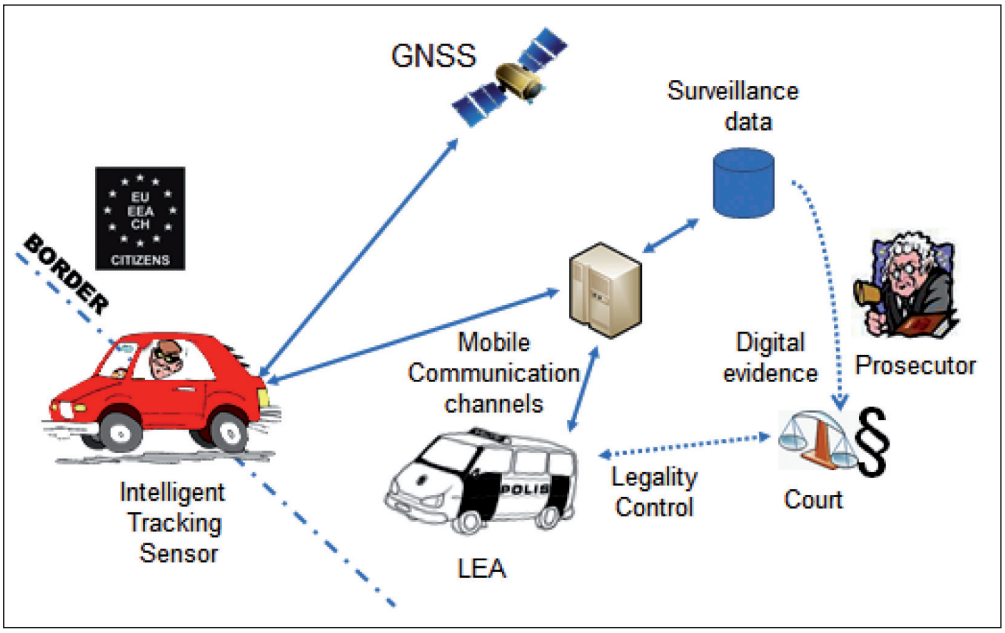
3 OPERATIONAL ENVIRONMENT

Organized crime is a real threat in Europe with the emergence of international warehouses of crime. For improving their evidence-gathering abilities, the law enforcement authorities are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. The criminals' counter measure activities like electronic counter-surveillance, jamming and constant changes in behaviour for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new, harder to detect, more strongly encrypted, longer-lasting and quicker to install and more adaptive intelligent technologies, is emerging and a high priority task. Respecting the accountability and integrity requirements and

smooth utilization of data in different phases of chains-of-custody is of utmost importance. In the current situation the chain of custody is difficult to maintain due to different techniques that operate on their own and are connected to different monitoring systems. This makes LEA work very labour-intensive so the use of new state-of-the-art technologies should enable the optimization of the use of human resources.

Figure 3 shows the operational environment where LEAs use tracking.

Figure 3
Operational environment



For pinpointing the major deficiencies in existing surveillance technologies, in the discussions between researchers and industrial and LEA experts, the following major needs or gaps related to everyday investigation and monitoring technologies and the context they are deployed were highlighted:

- Current tracking and monitoring systems are lacking in performance, old equipment is too big in size, hard to disguise and energy consuming.
- Most devices produced for LEAs take account their needs, but commercial interests are sometimes stronger incentive. This situation means that the best solutions are not always for sale and the manufacturers sell out the first generation products before bringing the next generation. This means that LEAs end up with having several inefficient systems lacking integration. This

requires a lot of support and logistics. The open IT solutions launched on the markets should be adaptable with new (experimental) sensors.

- Counter measures by criminals are posing new challenges as criminals use advanced detection and signal jamming technologies. Because of this the technologies used by LEAs have to be concealed in better ways, e.g. by size and appearance and have the jamming detection capabilities.
- Operational models of LEAs' information gathering do not comply with the legal and societal requirements and expectations in the needed level, neither with the possibilities the modern technology would allow. Harmonizing by implementing legal requirements into a new system that is useful for all LEAs in Europe is a first step.
- Safety, encryption and access control are very important. For investigation data has to be protected so that no unpermitted access will be possible and the content will not be revealed. Encryption safeguards privacy; tampering will be recognized and encrypted files will guarantee a strong chain of custody.
- New alternative positioning system is required; Galileo becoming operative will give new interdependence possibilities and advantages for tracking.

4 TRACKING CHALLENGES FOR LEAS

LEA officers need to have an easier access to all investigation data, independently from place and time and attention has to be paid to public awareness and concern on the use of surveillance equipment. However, legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way raise two problems: (a) how to ensure the accountability of law enforcement officers making use of such intrusive techniques and (b) how to ensure that sufficient privacy safeguards are implemented to ensure that these measures are used exclusively when overriding interests prevail and in a proportionate way.

Based on the identified deficiencies in the existing solutions, operational scenarios defined by the consortium LEAs and considerations of future challenges and issues that would be the most influential in European and international context, SATERISK has found to follow five main operational and technological challenges.

1. GNSS sensors; commercial sensor do not fulfil the needs of LEAs.
2. Cross-border operations; criminal nature has internationalised but LEAs are national organisations.
3. Secure mobile communications is more and more important in all operations.

4. Digital evidence; surveillance data LEAs collect should be valid in the court.
5. Legality control; LEAs' operations should be transparent.

4.1 GNSS Sensors

With regard to tracking operations, the LEAs have the following problems: The size of available equipment is too big which restricts concealment possibilities. Power consumption is too high (maintaining of devices during the operation brings risks of being exposed etc.), there is scalability but low power options mean lower data quality so alternatives should be found. The systems are GPS and GSM dependent for positioning and communications; there are no cross-over possibilities, e.g. positioning could be based on using different satellite systems, known WLAN networks, mobile phone cell location, RF/DF etc. Also, intelligence is lacking from the systems; they can be commanded but they do not have the capability of self-reacting and alerting. Furthermore, available commercial products are vulnerable to jamming without jamming detection possibilities.

A new tracking sensor system, which has multi GNSS capability (Galileo, GPS, CLONASS) should be developed. Because the battery is the biggest part of these sensors, miniaturizing will mainly be achieved by optimizing sensor's power consumption, and utilizing energy harvesting and new high energy rechargeable battery technologies, For easy concealment, recharging will be wireless. For improving legal, policy and social acceptance issues, tracking sensors should need authenticated permission token to operate. Encryption should be done in the first possible phase, so that there will be no plain information stored in the system. Self-protection and counter measure protection as well as jamming detection should be included.

European LEAs can only be independent if their tracking is based on Galileo, the only European global navigation satellite system Galileo will allow positions to be determined accurately even in high-rise cities, where buildings obscure signals from today's satellites. Galileo will also offer several signal enhancements making the signal more easy to track and acquire and more resistant against interference and reflections. European GNSS will deliver much more precise and much more reliable services than the American and Russian systems. By placing satellites in orbits at a greater inclination to the equatorial plane, Galileo will also achieve better coverage at high latitudes, making it particularly suitable for operation over northern Europe, an area not well covered by GPS[1].

[1] http://www.gsa.europa.eu/go/galileo/why-galileo

Many companies are developing tracking sensors and miniaturizing them; some are even considering the power consumption. However, most are concentrating only to hardware size. Military equipment are very sophisticated but use too much energy, because their main interest is Blue Force Tracking (tracking for own vehicles and people) and not for the enemy tracking. This means that energy consumption is not a big problem, because tracking sensors are in your possession; it is easy to change batteries or use other power sources from the car etc. Big part of the power consumption is how you use the equipment. Today already, the actual hardware is usually smaller than the battery back, smaller hardware size with no reduction in battery consumption helps only marginally. Figure 4 shows all relevant miniaturizing levels. Also, energy harvesting methods could be used; energy from ambient vibrations, wind, heat or light could enable smart sensors to be functional indefinitely.

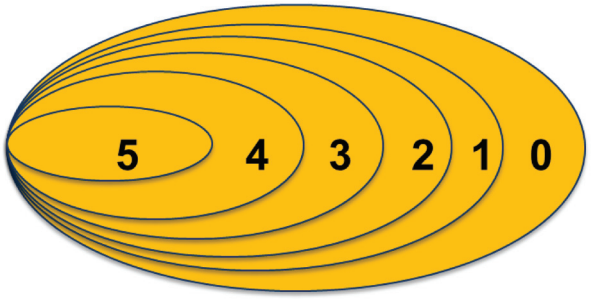


Figure 4
Miniaturizing levels in tracking sensor development

0 – Starting point: sensors and battery now;
1 – Add: Optimizing the use with AI;
2 – Add: Better sensor software;
3 – Add: New battery or other power source technology;
4 – ADD: Lower hardware power consumption;
5 – ADD: Smaller hardware size

On batteries new technology is based on the elements of lithium and sulphur. These two combine to yield a battery system with the highest theoretical gravimetric and volumetric energy densities of any known useful battery couple. This will enable many new LEA applications. The difference with Lithium-Ion is that the cell voltage is not anymore 3.6 V but varies nonlinearly in the range 2.5-1.7 V during discharge.

4.2 Cross-border LEA Operations

Organized criminality does not respect national borderlines and international warehouses of crime involved in smuggling, drug and human trafficking and terrorism are becoming a stronger threat to the European security. Following this, there is an increased need for European collaboration and information sharing related to the investigation technologies; cross-border usability and interoperability of investigation tools have to be guaranteed. However, joint

cross-border investigations are challenging as the LEA practices and technologies used in technical operations and legal procedures have big differences and incompatibilities. This leads to e.g. to slow or even hindered information exchange, endangering the success of entire investigations.

Viitanen et al.[7](2010) focus on cross-border surveillance operations dealing with time critical data communication between multinational organizations. This problem is common between the LEAs. Criminals are working more often abroad due the European integration, but LEAs do not have common protocols and procedures, how to pass information between each other. Especially machine to machine (M2M) communication is not researched yet.

4.3 Secure Mobile Communications

Secure, uninterruptable communication is a pre-requisite in critical environments, for example in public safety applications and critical infrastructure telemetry. General purpose IP based communication links may not be adequate and sufficient. For example, capacity of communication links and cyber warfare may present problems. Methods for ensuring constant connectivity and maintaining unbroken communication in all circumstances are needed. Traffic engineering and multichannel communication may mitigate the aforementioned problems. The DSiP solution (Distributed Systems intercommunication Protocol ®) enables parallel use of different network technologies in a consistent and transparent way enabling communications services platforms to be created. For example in cross-border operations, this is a huge advantage (Rajamäki at al., 2010).

Information security has at least five dimensions: Availability, authenticity, confidentiality, integrity and non-repudiation. Violating any of these may cause considerable harm or even damage. Identifying issues related to information security in satellite-based tracking systems is a huge topic. Kämppi et al. (2009) open this playground in the SATERISK project introducing the technical architecture and data flow in General Packet Radio Service (GPRS) and points out vulnerabilities and unknown issues in information security. They conclude that applicable security solutions or satellite-based tracking systems are, however, available. The also study describe major technical vulnerabilities of such systems. The field is divided into four segments: the satellite and tracking segment, the communication segment, the data-processing segment and the end-user segment. Each of these segments has its own set of risks and threats, which can be reduced to an acceptable level. Preserving the confidentiality of data is seen as the most important issue.

4.4 Digital evidence

Remote operation is the control and operation of a system or equipment from a remote location. In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. LEA monitoring station is a workstation or a place in which sensor information accumulates for end-users how needs it. There must be a central control station, which collects and stores all the information according to the rules and provides also legality control. The real time information will be sent on demand to the end-user where ever he or she is. In many cases, the users of information are not in the office but in the field using portable devices. This is called front deployed knowledge. Monitoring systems should be able to combine multiple forms of information, temporal, spatial, audio and visual, etc. However, combining information from many sources is technically, operationally and legally difficult task and analysing is suffering from it.

At present many LEAs are still using point to point investigation tools and tracking systems, where the information is transmitted from the sensor to e.g. a laptop of the surveillance team for monitoring. These old-fashioned stand-alone systems create neither watermarks nor log file marks; the system only retrieves the information and stores it locally. For that reason neither chain-of-custody nor social acceptance by transparency comes true. (Viitanen et al., 2011.)

The gathering, conservation, communication and presentation of the computer - derived evidence must fulfil legal requirements with regard to the admissibility of the evidence; they should be admissible, authentic, complete, reliable and believable. Electronic evidence not gathered in accordance with the law will be inadmissible and be ruled out of court. Today's main evidence authentication system is the hash value calculated from the retrieved information. With hash value you can prove that the data is the original and no one has tampered with it. The problem is that systems like hashing are incapable to fully expose when, where and by whom data is produced.

4.5 Legality control

For example in Finland, the oversight of police's coercive measures is based on a file system SALPA run by National Bureau of Investigation. The SALPA system guides how to make applications and notifications in the correct manner. The question then is, can this system alone be a sufficient legality control system, if the information that police officers write down are not based on actual log files. These non-transparent systems might be handicaps to LEAs (Tuohimaa et al. 2011). LEAs may also act according to the law but they are not able to prove it because methods cannot be audited by an outsider. The current state of affairs

is neither efficient nor transparent. More advanced monitoring system is needed to provide faultless control of the surveillance equipment and procedure all the time. At present no process or instance is able to present publicly accepted proof of correct use of these equipment as long as there are no a publicly proven technical control methods involved in the chain.

5 DISCUSSION AND CONCLUSIONS

In order to bringing about the LEAs' special requirements for GNSS, technological and socio-technical research and development work is needed. Development of novel monitoring systems and miniaturized sensors improves LEAs' evidence-gathering abilities while respecting legal and ethical expectations of society. The over-all development target will be accomplished through the following specific objectives:

1) to enable new operational models for investigation for LEAs
   - by improving existing technology and developing new integrated digital systems for tracking and audio and video retrieving and monitoring
   - to achieve next level in digital miniaturization and state of the art development including: a) easy usability; equipment can be handled under difficult situations; b) long life-time; extended to several months or even over an year; c) (self-) protection; applying artificial intelligence, the sensor is capable of monitoring its surroundings and can change its operation model autonomously for its own safety, d) data securement by deep encrypting
2) to develop methods of working that are legally binding and social acceptable
   - information gathered is legally binding and court proof developed technology will enable audit trail, accountability and further societal acceptance
3) to support wider European goals
   - to recognize needs for regulation and harmonisation
   - to promote use of other European technologies like Galileo and create needed interfaces.

REFERENCE

[1] Hevner, A., March, S., Park, J. & Ram, S. (2004). Design science in information systems research. *MIS Quarterly* 28, No 1.

[2] Kämppi, P. and Guinness, R (2010) Technical Risk Analysis for Satellite Based Tracking Systems. *Proceedings of the Integrated Communications Navigation and Surveillance Conference*, Herndon, VA, USA, May, M3-1 - M3-16.

[3] Kämppi, P. Rajamäki, J. and Guinness, R. (2009) Information security risks for satellite tracking systems. *International Journal of Computers and Communications*, Issue 1, Volume 3.

[4] March, S. & Smith, G. (1995). Design and natural science research on information technology, *Decision Support Systems* 15.

[5] Nunamaker (2010). Interview with Jay F. Nunamaker, Jr. on "Toward a Broader Vision of IS Research". *Business & Information Systems Engineering,* Issue 5.

[6] Nunamaker, J., Chan, M. & Purdin, T. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems*. Vol. 7, No. 3.

[7] Rajamäki, J., Pirinen, R. & Knuuttila, J. (eds.) (2012). *SATERISK Risks of Satellite Based Tracking*. *Sample of Evidence Series: Volume (2)*. Edita Prima Oy, Helsinki.

[8] Rajamäki, J., Holmström. J. & Knuuttila, J. (2010). Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities. *Proceedings of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, Twente, The Netherlands Nov. 24–25 and IEEE Xplore.

[9] Tuohimaa, T., Tikanmaki, I., Rajamäki, J., Viitanen, J., Patama, P., Knuuttila, J. & Ruoslahti, H. (2011). Is Big Brother Watching You? *International Journal of Systems Engineering, Applications and Development*, Issue 5, Volume 5, 602–609.

[10] Van Aken, J. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. *Journal of Management Studies* 41, No 2.

[11] Viikari, L. (ed.) (2011). *SATERISK: Tutkimusraportti 2008-2011*. University of Lappland. Lapin yliopistopaino (in Finnish).

[12] Viitanen, J., Happonen, M. Patama, P. & Rajamäki, J. (2010). Near Border Procedures for Tracking Information. *WSEAS TRANSACTIONS on SYSTEMS*. Issue 3. Volume 9. pp. 223–232.

[13] Viitannen, J., Patama, P., Rajamäki, J., Knuuttila, J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. (2011). How to Create Oversight in Intelligence Surveillance. *Proceedings of 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications*, March 24-26, Meloneras, Gran Canaria, 52–56.