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.

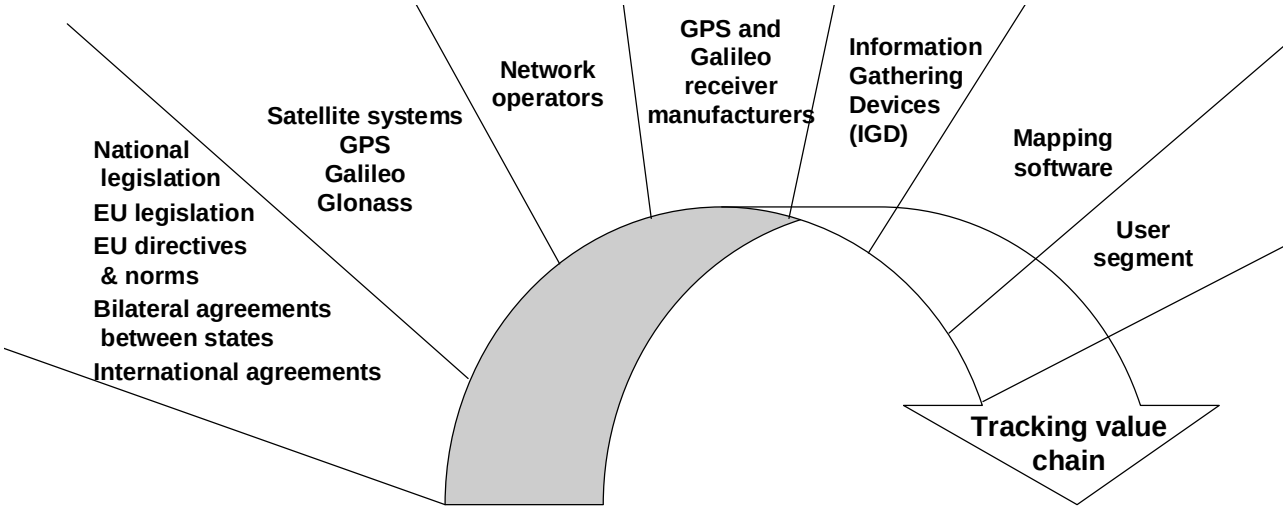

Fig. 1 Sectors of SATERISK project

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,

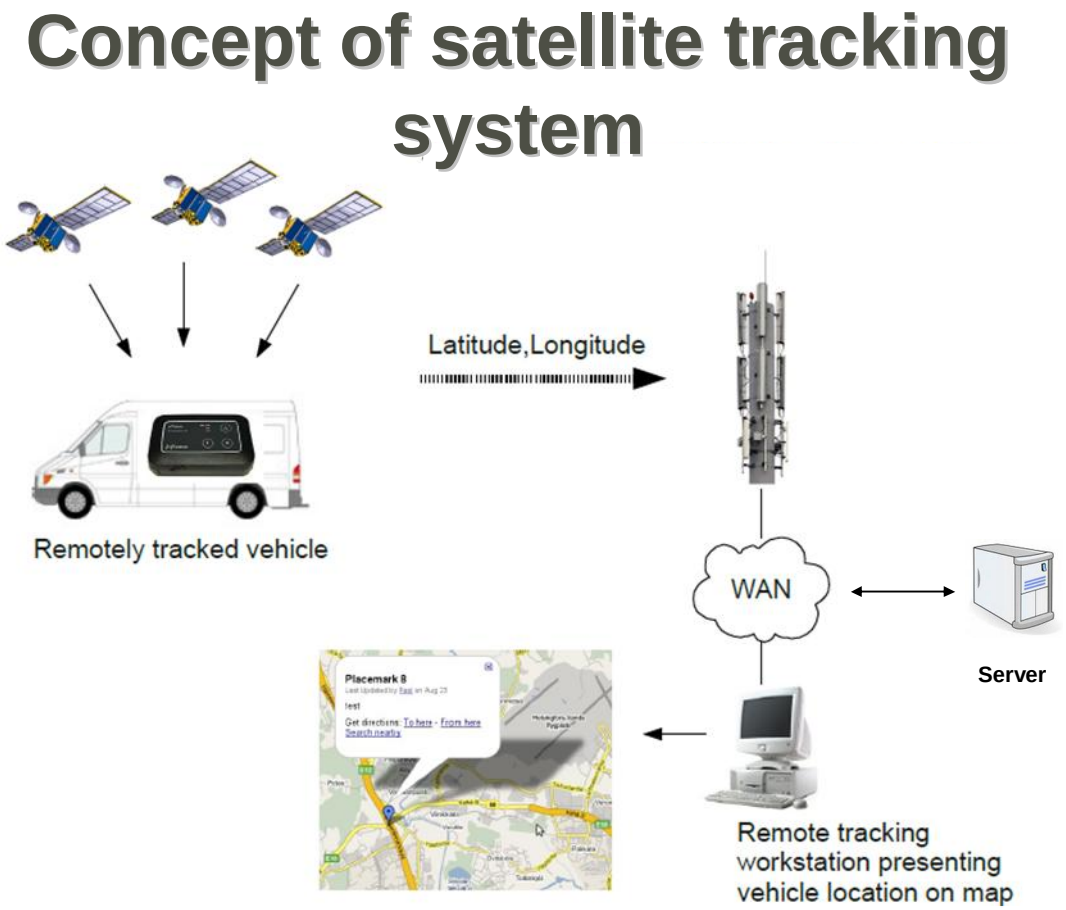

Fig. 2 Concept of satellite tracking system

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

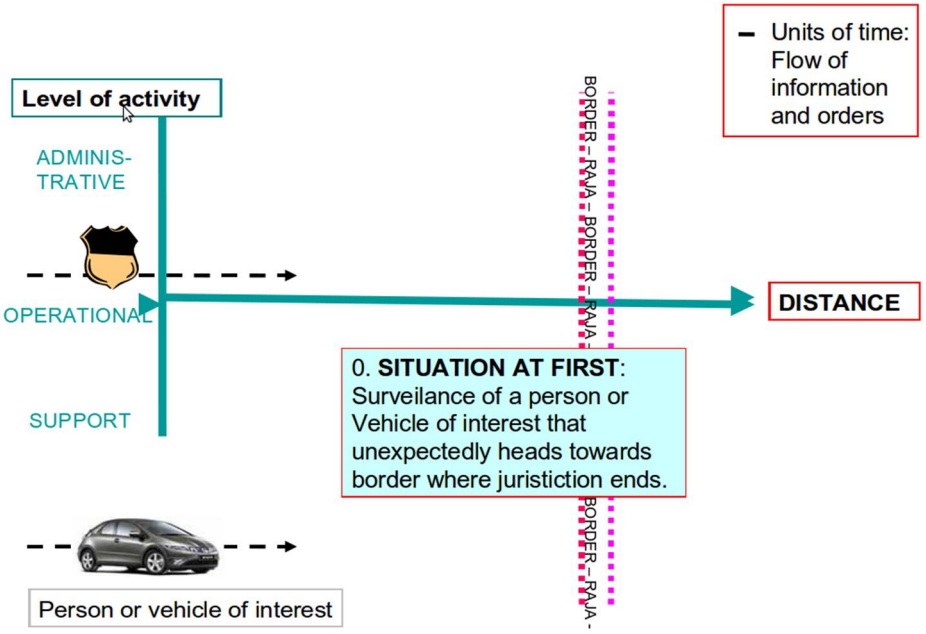

Fig. 3 Flow of information and movement of target – Start situation [9]

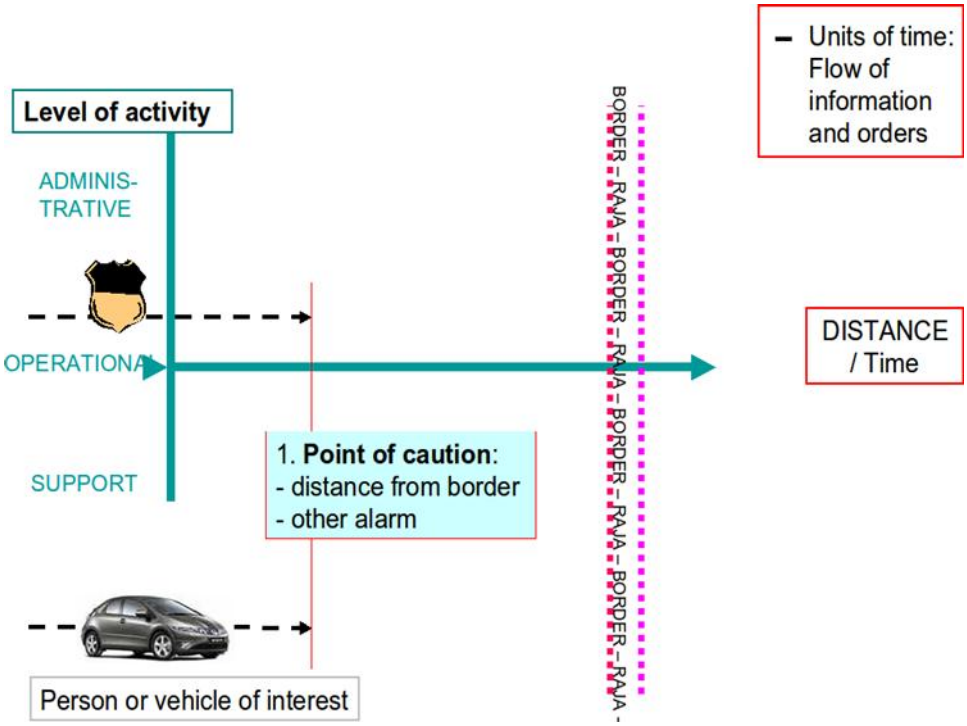

Fig. 4 Flow of information and movement of target – Point of caution [9]

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

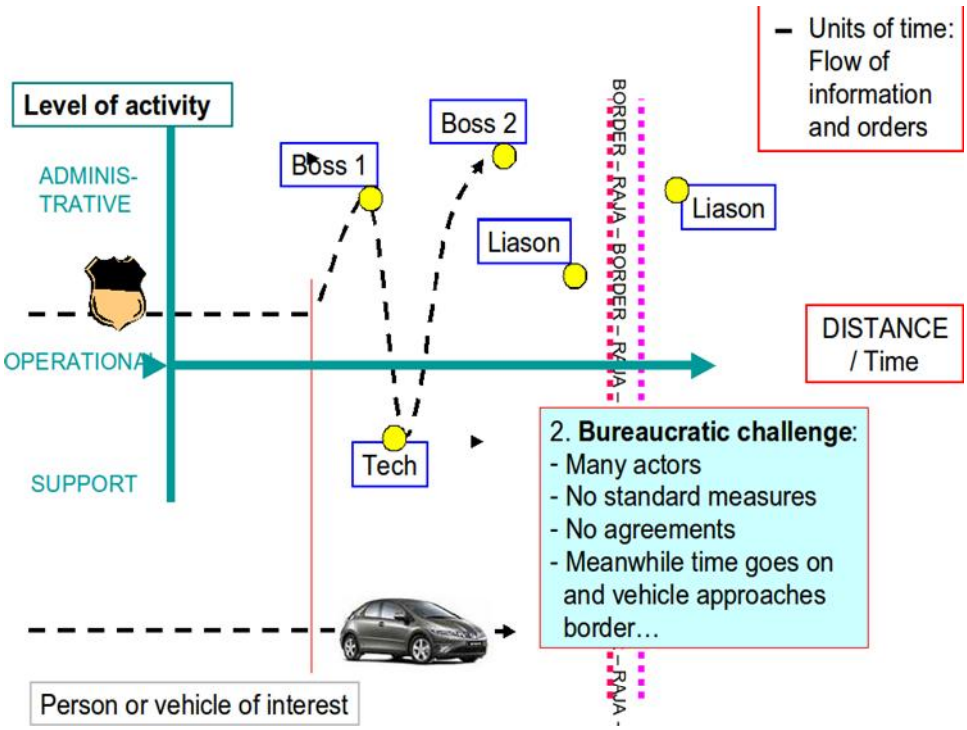

Fig. 5 Flow of information and movement of target – Bureaucratic challenge [9]

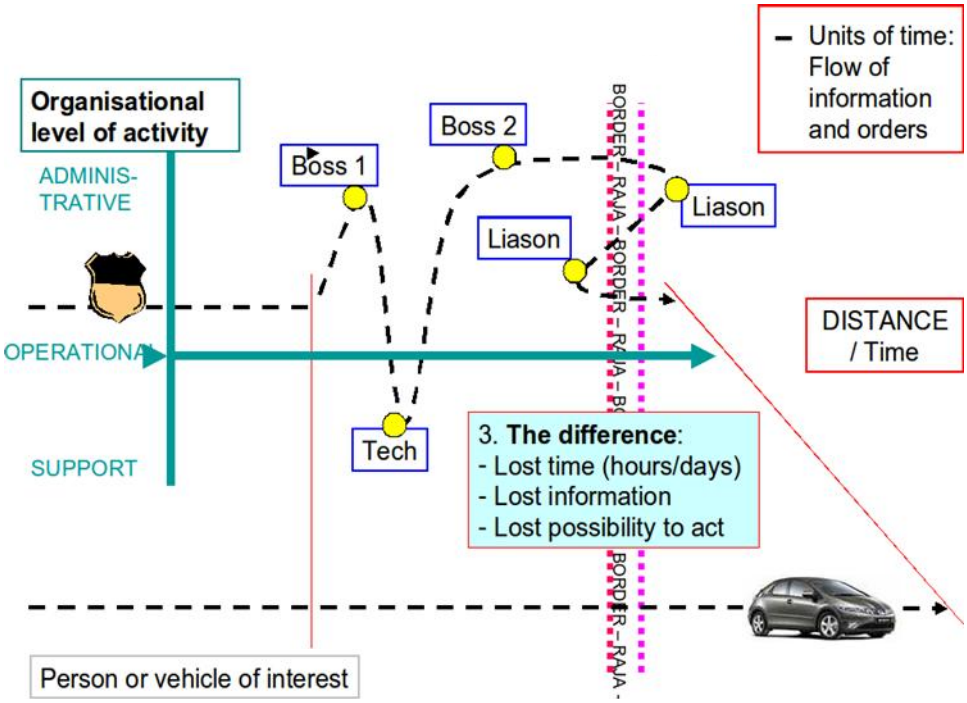

Fig. 6 Flow of information and movement of target – Information is lagging [9]

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,

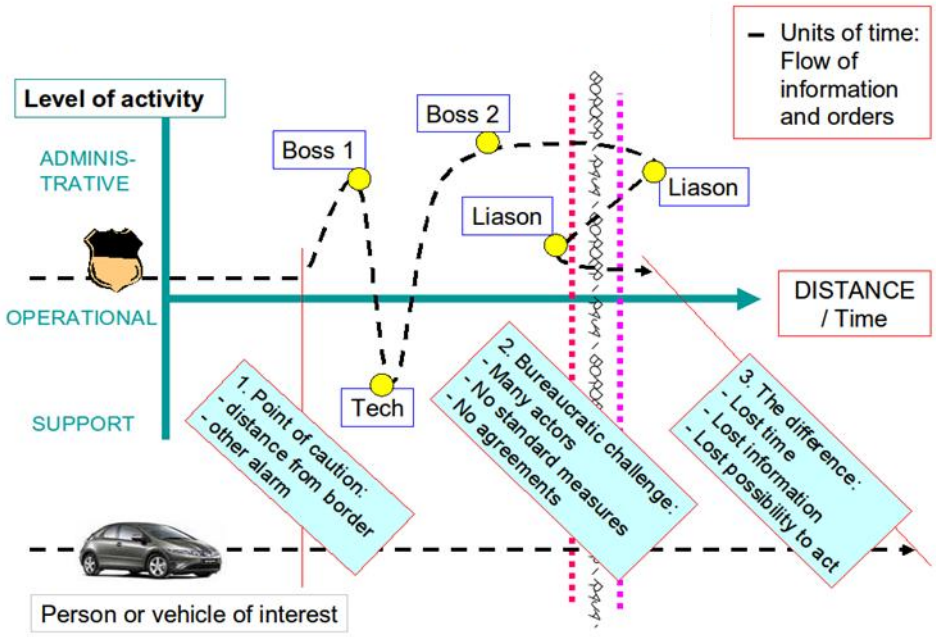

Fig. 7 Flow of information and movement of target – Lost possibility to react [9]

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

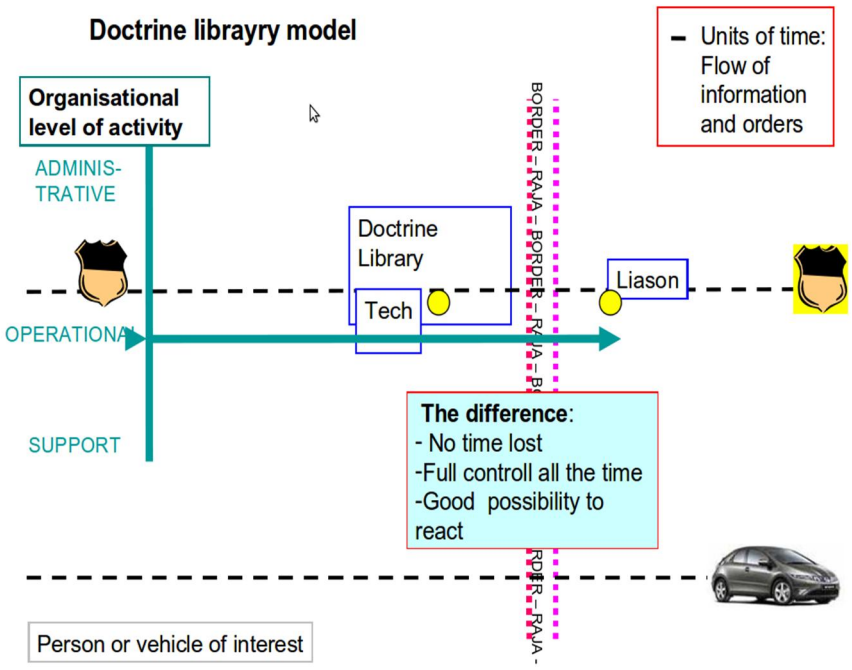

Fig. 8 Faster information flow with doctrine libraries

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

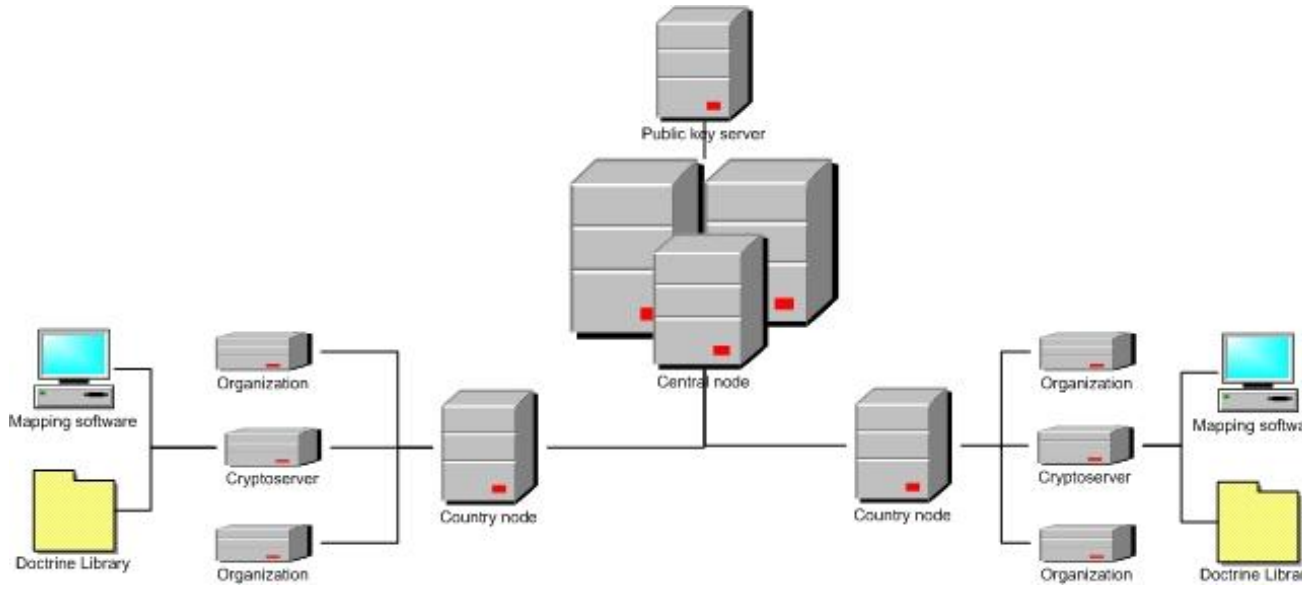

Fig. 9 Network topology

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.