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

---

**Flow of information and movement of target**

- **Units of time:**
  - Flow of information and orders

- **DISTANCE / Time**

1. **Point of caution:**
   - distance from border
   - other alarm

2. **Bureaucratic challenge:**
   - Many actors
   - No standard measures
   - No agreements

3. **The difference:**
   - Lost time
   - Lost information
   - Lost possibility to act

---

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
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, administrative 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