Border surveillance in a transnational environment – aspects of data storage and dissemination

Barbara Essendorfer, Wilmuth Mueller, Heiko Wanning

Fraunhofer Institute for Information and Data Processing
Fraunhoferstraße 1, 76131 Karlsruhe, Germany
{barbara.essendorfer, wilmuth.mueller, heiko.wanning}@iitb.fraunhofer.de

Abstract. This paper deals with aspects of data sharing in a transnational environment. Comprehensive border and coastal surveillance and control are key components of EU's global protection. At present border surveillance is often accomplished through separated stovepiped systems. Data that might be of interest for not only one but many surveillance units from different Member States, especially in regions in which two or more Member States have a border with an third, non-EU country, can't be shared and thus the capabilities to secure the border are limited. To overcome these limitations, interoperable transnational surveillance systems, capable to include all relevant data sources and to share them among border related law enforcement bodies are needed. As the output of sensor and exploitation systems shall be accessible by different users, standardized data formats are needed. Commercial standards were often not defined for the surveillance domain, thus they would need to be adapted. Standards defined within the military domain are of interest because they already take the sharing of products in a heterogeneous security environment into account. Additionally the cooperation of military and civil surveillance and reconnaissance systems will be of greater importance in the future.

1. Introduction

Although transnational and international exchange is a vital economic necessity, a lack of sufficient control can be a deadly threat to domestic security. Criminal and terrorist activities do not stop at national borders.
Therefore, comprehensive border and coastal surveillance and control - balancing economic and safety requirements - are key components of EU's global protection. Effective control and surveillance of external borders is a matter of the utmost importance both to Member States regardless of their geographical position and to the European Union itself.

There is a need to improve the operational cooperation, structural coordination and information exchange between law enforcement authorities of EU Member States. The need for appropriate cooperation mechanisms is most acute in regions in which two or more Member States have a border with an third, non-EU country. Although each region is unique, as regards demography, geography and prosperity, there are similarities in cooperation, coordination and information exchange needs.

Operational cooperation at EU level aims to strengthen security at external borders and the cooperation among border related law enforcement bodies responsible for the internal security of the EU. Operational cooperation includes joint patrols as well as joint intervention and surveillance operations in border regions, especially at green borders.

Structural coordination includes the interoperability of equipment, in particular in communications and surveillance technology.

Operational cooperation, structural coordination and information exchange both at EU level and transnational level will for example

- increase the efficiency in detecting and preventing illegal aliens, terrorists, and contraband from entering the EU between official ports of entry (POEs)
- improve the reaction time from detection to interception.

At present border surveillance is often accomplished through separated stovepiped systems. Data that might be of interest for not only one but many surveillance units can't be shared and thus the capabilities to secure the border are limited. To overcome these limitations, inter-operable transnational surveillance systems, capable to include all relevant data sources and to share them among border related law enforcement bodies are needed.

Security research should emphasize the Union's capabilities regarding surveillance, distribution of information and knowledge of threats and incidents as well as systems for better assessments and situation control through better use of common ICT-systems in the fields of different operations.

2. Integrated surveillance systems

Border surveillance makes use of a number of systems that detect threats and conspicuous behavior. Witin an integrated surveillance systems disparate technologies that complement one another are installed, the interaction of the data output is essential.

2.1 Components

An integrated surveillance system consists of sensors, exploitation systems, that might be deployed as situational awareness boards also and external information systems.

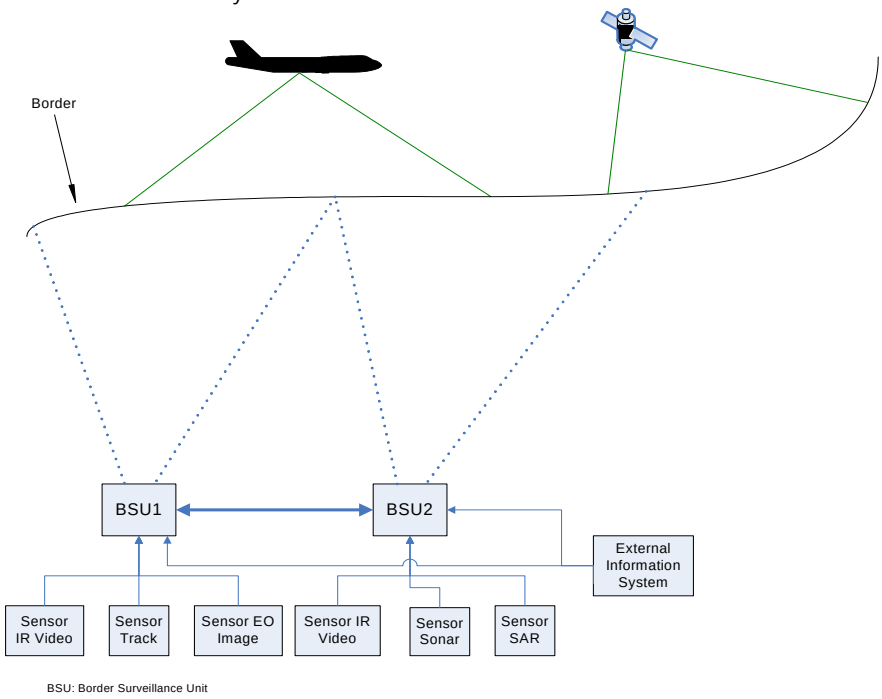

Figure 1: Border Surveillance System

In Figure 1 a border is monitored by different sensor types. Those sensors deliver data to a surveillance unit. However the areas that are surveilled intersect and data that is of interest for one surveillance unit is of interest for the other as well. Thus it is necessary to share data and add

information from an external system to it to be able to get enhanced situation awareness.
In the next paragraphs these components and their connection are described in detail.

2.1.1 Sensor systems

Sensor systems normally consist of the sensor itself and a sensor ground station that does the primary data processing and eventually some exploitation. With modern airborne sensor units for example the data is preprocessed (due to network capabilities) to be sent to the ground via a data link. Combined sensor systems that consist of different sensors might use some sensors as triggers for other sensors and only the secondary information is passed on to an "outside" exploitation system. Depending on the sensor type and the processing a proprietary (raw) data stream is created. An interface with an exploitation station has to be defined.

To observe land and sea borders it is necessary to make use of different sensor types with differing ranges and tasks.

Spaceborne systems

Spaceborne systems provide long-range border surveillance. Depending on the sensor type these platforms support an all-weather and 24 hour view of a wide area, its facilities and the usual traffic at a given point in time (not real time). Identification of buildings and large objects (e.g. large vessels, airplanes at an airport) is (depending on the image-resolution) possible. For the identification of smaller objects other platforms have to be used. The output of spaceborne sensors is primarily some kind of imagery (radar, IR[1], EO[2]) or tracks (GMTI[3]).

[1] Infrared
[2] Electro optical
[3] Ground Moving Target Indicator

Airborne systems

Sensors that are assembled to airplanes, helicopters and UAVs (Unmanned Arial Vehicles) are of interest for the surveillance of boundaries because it is possible to get real time data along a border or another defined area. They are appropriate for long- and medium-range surveillance. It is possible to task these platforms to observe a certain area or even specific targets; they can keep track of moving objects and (depending on the resolution of the image) identify them. With advanced platforms data can be pre-processed already on-board and sent, via a high-speed data link, to a ground station. Airborne system sensors deliver all kinds of imagery like IR, EO, and SAR[4] as well as motion imagery (video), SIGINT[5] or radar data.

Zeppelin/ balloon systems

Medium- and short range border surveillance platforms like zeppelins or balloons are already used to observe intruders in areas of a high security risk, like the southern border of the United States. Balloon- or zeppelin-borne sensors deliver (motion) imagery data, because they operate in a low altitude they are prone to destruction.

Ground-based sensors

Ground-based sensors are specialized on short-range border surveillance and can be installed at fences and checkpoints, at buildings or traffic routes, on vehicles that survey a special area of interest or be integrated in observable objects like containers or vehicles. With ground-based sensors it is possible to get real time information and identify (depending on the sensor type) the object or person that is observed. Because of their location these sensors are at risk to be destroyed by intruders. Sensor types are radar, IR sensors and all kinds of optical sensors, motion detection systems, acoustic sensors, seismic and motion imagery sensors.

Seaborne sensors

Seaborne sensors can be placed underwater or above, on ships or submarines, fixed or mobile. The above water sensors are similar to the

[4] Synthetic Aperture Radar
[5] SIGnals INTelligence

above described ground based sensor types. For underwater surveillance especially sonar, special electro optical cameras, chemical and biological sensors as well as magnetic detectors and other acoustic sensors are of interest. Depending on the tasking these are medium or short- range sensors.

2.1.2 Exploitation systems

Exploitation Systems are used for the exploitation of preproduced data. Exploitation can be done in different contexts:

- Sensor specific exploitation

The primary exploitation of sensor data is normally done by an especially designed ground station that *belongs* to the sensor unit.

- Data type specific exploitation

Some exploitation systems are specialized on certain data types. For example a station could provide the ability to enhance and optimize electro optical images. Analysts that are trained on imagery exploitation operate at these stations and evaluate the products according to predefined aspects.

- Area specific exploitation

To get a situational awareness on a predefined location a variety of preprocessed data can be worked on with situational awareness exploitation stations. Within these systems enhanced information is derived and some kind of areal picture is created.

For exploitation systems that work on products that are produced from various sensors it is important that the data is available in an inter-coordinated data format.

2.1.3 Situation awareness

Situation awareness consists of three states: First the elements have to be perceived; second the meaning of those elements has to be understood and third the implication on future processes has to be drawn [1]. If one transfers this definition to a transnational surveillance scenario this means

that threats and suspicious behavior have to be perceived, the threat has to be understood and an appropriate reaction has to be performed. In order to achieve situational awareness in transnational border surveillance the products of the above mentioned sensor and exploitation systems have to be available. The data has to be accessible with respect to time and location of the product as well as to other decision-relevant information. To enhance the situational awareness this information should be presented time sensitively and user-friendly. Relevant sources of knowledge should be incorporated. Integrated systems achieve enhanced situation awareness by developing a common picture of the tasked area. To support analysts, operators and decision makers it is important to integrate the *right* i.e. temporally relevant information in this common picture.

- Situational awareness and sensor data

The display of sensor data in a common picture only makes sense if the operator/analyst is able to interpret that information correctly. The data has to be presented in an agreed way and it has to be equipped with the adequate metadata. Information on the source, the time and location of the product as well as the type are of interest to integrate it in an overall picture or map.

- Situational awareness and exploitation data

Exploited data normally already contains more enhanced information. Similar to the sensor data it has to be integrated adequately in a common picture. It should be able to trace the exploited product back to the original (primary) sensor product and either combine those two products or display just one (usually the exploited) of them.

- Situational awareness and information systems

Information systems that are not especially developed for the task of border surveillance or are used in different contexts are relevant for the rating/ evaluation of derived data and information. Weather data can give essential advice which product sources are of interest in certain circumstances, systems like the "Schengen Information System" (SIS) provide data on detected persons or goods and the internet can provide background information for all kinds of questions. To enhance the situational awareness it is of interest to be able to integrate these information sources and even enable automatic data fusion and correlation.

2.2 Establishing intrasystem communication

Once the system components are decided upon, it is necessary to establish a way of connecting them. This chapter will detail the "how" of data transfer, what protocol, what network layout to use. It will explain, what happens to the data, once they have left the originating sensor, and in what way they arrive at the desired destination (i.e. the analyst).

2.2.1 Data transmission

The connection properties between the data source and the sink shall be discussed in this section. It shall give guidance on the choice of the transport means and the protocol, although a general best solution is not possible, considering the circumstances the pros and cons must be considered.

The selection over which medium (wired ethernet/ wireless) and transfer protocol (TCP with guaranteed quality/ UDP for higher data rate, but loss possible) to use depends on:

1. the number of connected sensors/sensor ground stations – a larger number of nodes in a network makes cabling an arduous and complicated task. Also, the bandwidth demands are higher in that case.
2. their location in space (i.e. their distance to one another) – If the nodes are present in a confined area the usage of wireless connections might not be necessary.
3. their mobility – If the sensor platforms are mobile, when mounted on a ground vehicle or a satellite for example, it is obvious that wired-only connections are impossible and relays and/or gateways may have to be used as well to provide connection points from the wired to the wireless part of the communication link.
4. and the kind of transmitted data – Video requires a much larger bandwidth than e.g. alarm trigger data which consists solely of short messages.

Generally, if the required overall data rate is very high, wireless communications might have problems before a landline's limit would be reached. Also, security aspects deserve closer attention when using a wireless connection, since it is easier for the man in the middle to listen

in, provide false information or disrupt communication. The usage of cables which can be shielded much easier than the complete area of radar coverage bears a smaller risk in this regard.

If high data throughput is necessary with occasional partial data loss being a minor problem (e.g. in a video stream it is acceptable to lose a frame out of every 25 per second) usage of UDP is a good choice. Here it has to be kept in mind that over wireless networks, frame rate loss does occur more frequently than over landlines [2]. On the other hand, if the requirements for the Quality of Service are high (it has to be guaranteed that not a bit is lost from a transmission) TCP might be a better option with the cost of a bigger overhead.

2.2.2 Data storage and –dissemination

This section will explain how to store and distribute the acquired data within a network, the concept of using regional servers and what else besides receiving and sending information these servers can do.

The sensors and their ground stations in a multi-national environment are positioned over a great areal expanse, often consisting of coastal or land border lines with overlapping regions. Consider for example the EU border with Ukraine depicted partially in fig. 1 below:

Figure 2: Map of border region East Europe – Ukraine [3]

The line colored in red marks the frontier that four EU countries share with the "outside world" in a very close area. Each of the participating EU nations has their own border control system which will have to be combined into a greater structure to form a European border control system.

This suggests using a decentralized setup (see fig. 2). Here the regional servers (in white) collect the data from their directly connected sensors (in black), respectively the sensor ground stations which translate the data stream into a common data format.

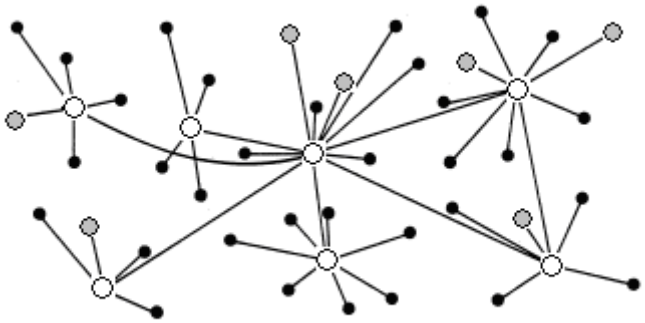

Figure 3: Decentralized network

The regional servers synchronize their respective metadata content among each other in times of otherwise low network usage. When an exploitation station (in grey) wants to collect data from different sensors scattered throughout the whole network it sends a query to its local server which delivers the results by looking only at its own data base. Only when the full data set is requested, a connection to the originating server is initiated where the potentially large files (e.g. videos) are transported across the network.

This setup has the advantage of reducing the amount of data traffic on the overall network, because bigger data packets are only transferred on demand, not every time they are created. Also, the local servers serve as a backup in case of network or server failures. That "complete reliance upon a single point is not always required" [4] was the idea that started the ARPANET in the 1960s, which later evolved into the Internet.

The down side is the potential old age of the data received from a query. If the synchronization interval is set too high, the required information may not be there yet.

This system is fully scalable, i.e. the size of each 'subnet' including its server can be understood to be either belonging to a certain sensor type in a small region or on the other extreme they could also consist of all sensors of a nation participating in an European network.

In addition to accumulation, storage and distribution of data, other tasks of the servers can be the processing and generation of new data out of the received information. Examples are:

- Data fusion (combine the information obtained from a daylight and infrared camera pointing at the same location resulting in new knowledge unobtainable from each single sensor individually)
- Data clarification/extraction (motion imagery processing like image stabilization, mosaicing, object tracking, noise reduction)
- Object recognition (e.g. 3-D object recognition using several 2-D images [5])

3. Dataformats for the surveillance domain

The previously described particularities of surveilling a transnational environment make an adequate handling of the data necessary. As the output of sensor and exploitation systems has to be able to be accessed not only by one but eventually many users (see the previous chapter) it is necessary to agree upon data formats and therefore make full usage of the data.

3.1 Requirements

Border surveillance has to be weather, season and daytime independent. Sensor systems have to consider the various landscapes and elements of the border and it has to be possible to detect all kinds of threats.
Thus different sensor types have to be deployed, depending on the above mentioned boundary conditions. As already stated under 2.1.1 there have to be systems for land and sea and for long, medium and short range surveillance.

To be weather and daytime independent a mix of data types has to be implemented. To survey an area at night time thermal sensors like infrared (passive or active) have to be installed, contrariwise these sensors are not built for hot weather, others like zeppelins or balloons are not efficient in stormy weather. Metal detectors have to be deployed to register weapons and for gas or explosives olfactory sensors are of interest.
Surveillance data is time sensitive. The data format has to consider this.
To get an overall picture and assign surveillance products to an area and put it them in a chronological context as well as to fuse data it is important to provide metadata with the product. The requirements at that point depend on the overall architecture and the display, exploitation and fusion capabilities. Information on chronological and areal allocation of the product, the source and the coverage of the sensor as well as the product type and size should be mandatory. If the data is confidential congruent metadata has to be defined.

3.2 Datatypes

In the surveillance domain a number of sensors and thus a variety of data types are of interest. In the next section those types are summarized in three categories.

Imagery

Still image is of interest if a closer look has to be taken on the surveyed object/ person. Sensors deliver a broad variety of images like different kinds of electro optical, thermal (IR), imaging radar (SAR) or magnetic images to name just a few. If the image is processed it is of interest to store the annotations with the data.

Motion Imagery

Video is a common possibility to watch public places and enhance public security. The most popular application is CCTV [6](Closed–Circuit-Television) that is implemented in areas of special security interest like airports, harbors, banks or areas of high risk. The installation of such systems is supposed to reduce crime by deterrent and to enhance reconnaissance of committed crime. For the surveillance of large areas it

is necessary to furnish such system with automatic detection methods in order to reduce the work load on the operators. To use the video in the in 2.2.2 described setting it has to be digitalized and for (semi-) automatic detection methods it needs to be furnished with collateral data. Additional to that the different kinds of video like electro optical or infrared need to be considered.

Tracks and Alerts

Sensors that detect changes in the environment upon predefined methods deliver alarms or, if they follow those changes, tracks. These magnetic, seismic, thermal, olfactory or radar sensors either just give information on time and place of an occasion dependent on a predefined threshold value or they give more refined information. For example the orientation of a tracked object the size or even the type of an object can be reported.

3.3 Common formats and standards

To enhance interoperability in a transnational environment and provide a quick adaptation of surveillance systems the usage of predefined formats is of interest. Standardization in commercial and military environment is a complicated and time-consuming task. After analyzing modern state-of-the-art technology and work processes, the standard has to be defined and agreed upon by the standardization board and potential stockholders. As modern technology is constantly evolving the adaptation of these standards not always keeps the pace. Nonetheless standards deliver a common "language" that all participants can rely on and therefore enhance interoperability.

Although there are a number of standards relevant for different aspects of border surveillance only the standards for data storage and – dissemination and for surveillance products shall be observed.

3.3.1 Military standards

In the heterogeneous military environment interoperability is crucial for advance in action. Thus a number of common standards for data and information sharing exist. Within the NATO these standardization

agreements (STANAGs) are defined by the NSA (NATO Standardization Agency) or the MAS (Military Agency for Standardization) that analyze commercial standards and agreements as well as national military standards. Many of these standards are based on one another and interlinked.

Data storage and –dissemination

For the storage and dissemination of digital data STANAG 4559 NSILI (NATO Standard ISR Library Interface) is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations. "The interface provides electronic search and retrieval capabilities for distributed users to find products from distributed libraries in support of, but not limited to, rapid mission planning and operation, strategic analysis, and intelligent battlefield preparation. The overall goal is for the users, who may be intelligence analysts, imagery analysts, cartographers, mission planners, simulations and operational users from NATO countries, to have timely access to distributed ISR information..."[7]

Surveillance data standards

A number of standards, depending on usage and data type are defined to enhance interoperability:

- For exploited imagery data STANAG 4545 (NATO Secondary Imagery Standard) [8] is used. It is a container format, where one to many images and associated products can be stored (text files, XML). With the images metadata is associated, that gives information on chronological and areal coordination, structure, quality and exploitation of the primary image.
- For video data STANAG 4609 (NATO Digital Motion Imagery Format) [9] is used. This standard is based on commercial digital motion imagery standards. It provides the means to record and transmit digital imagery using commercial off-the-shelf equipment. The standard also addresses the requirements for metadata which accompanies the motion imagery. At the moment this standard is based on the usage of MPEG-2.
- There are different standards for the numerous types of track data like radar, movement detection through seismic, acoustic and magnetic sensors or GPS based systems.

  - STANAG 5516 [10] provides a number of message types for tactical data links. By that information on sensor and exploitation systems themselves as well as information on targets/ track points can be provided. STANAG 5516 is a successor to STANAG 5511 and provides message types for subsurface and surface maritime surveillance, ground and air surveillance as well as status and emergency message types.
  - Data on ground moving targets derived by radar can be transmitted using STANAG 4607 [11]. It has mechanisms to adapt to different radar systems, exploitation capabilities and communication channels. The format is also designed to be encapsulated in either STANAG 4545 or STANAG 7023 (NATO primary image format) data files.
- For secondary information like the textual analysis of surveillance products report standards are defined. Based on the type of information that is of interest or the mission type, different standards are defined (e.g. STANAG 3377 [12]).

NATO standards are of interest for the transnational security community because of the similar tasking: Nations with heterogonous information and sensor technology need to combine their efforts and achieve a common situational awareness. Most of the information is time sensitive and in both domains there are areas of graded interest[6].

3.3.2 Commercial standards

Other than in the military domain in the commercial world there are a number of standardization organizations but most of them are less binding and the commitment to those standards is dependent on the application domain. In the following section a number of commercial standards are listed that might be of interest for the surveillance domain. The focus is on the special requirements of a transnational surveillance environment.

[6] In the military domain these areas of interest are "named areas of interest" or "target areas of interest" (NAI/TAI) as well as closed or prohibited, restricted and danger areas.

Data storage and –dissemination

The OpenGIS® Catalogue Service [13] defined by the OGC (Open GIS Consortium) concentrates on geospatial data, related services and resources. It was not designed for the surveillance area, but could be enhanced. The functionalities are similar to the ones defined in the STANAG 4559 mentioned under 3.3.1.

Surveillance data standards

There are few commercial standards that are especially designed for surveillance data. Within the next enumeration relevant standards are mentioned that might be of interest, however this list is not complete.

- There are many standards for digital image conservation. In the surveillance area standards are of interest that not only focus on optimized size/ quality relation but are able to contain enhanced metadata as well. Examples of image files containing metadata include Exchangeable Image File Format (EXIF) and Tagged Image File Format (TIFF).
- For digital video data there are a number of commercial standards that deal with compression techniques or container formats.
    - The codices and container formats defined by the MPEG (Moving Pictures Experts Group) consortium are among the most popular ones. Here standards for video compression (MPEG-2/ MPEG-4) and the management of corresponding audio and collateral data (MPEG-4) as well as the handling of metadata (MPEG-7) are defined.
    - Widespread standards for the commercial usage of video are defined by SMPTE (Society of Motion Picture and Television Engineers). For the surveillance domain standards for time-synchronization [14], the structure [15] and encryption [16] of metadata in videos and the transfer [17] are of interest.

  The combined usage of the above named standards is also accredited by the ISO (International Standardization Organization) [18].
- Tracks and Alarms:
    - Eurocontrol developed a standard for radar data. The "ASTERIX (All Purpose STructured Eurocontrol Radar Information EXchange) is a messaging format which allows a meaningful transfer of information between two

application entities using a mutually agreed representation of the data to be exchanged.
The ASTERIX Standard, as a Presentation protocol, defines the structure of the data to be exchanged over the communication medium, from the encoding of every bit of information up to the organization of the data within a block of data." [19]. As Eurocontrol is an organization that focuses on the safety of air navigation this standard was mainly developed for this area but it is of interest for radar surveillance in general.

- In the maritime sector the NMEA (National Marine Electronics Association) defined a standard that handles navigation data (NMEA-0183 [20]). GPS data and special marine data like depth, water temperature, orientation, speed etc. can be transferred by this protocol. The standard is essential for maritime communication.

4. Implications for an integrated surveillance system architecture

The above mentioned aspects have to be included in an overall architecture. Fraunhofer IITB has developed such an architecture based on military standards[7]. Figure 4 gives a top level impression of the elements. The *sensor systems* that produce proprietary data streams convert that formats in standardized formats (see 3.3.1). The data is transported through a predefined network (the choice here has to be made based upon the considerations listed under 2.2.1) and stored within the *shared data server*. To be coherent with the military architecture the server is based on STANAG 4559. Based on metadata enabled query or subscription the *exploitation systems* that include a *shared data client* (see 2.2) have access to the data they need depending on their tasking.
Exploiation system A uses track data (e.g. radar) as a trigger and verifies alarms by exploiting imagery. *Exploitation system B* might be tasked to an area of interest (AOI) and uses all data gained in this area to answer requests from an upper surveillance unit. *System C* is a mobile device that is able to exploit one kind of data only. The evaluated data is also stored within the *shared data server* so that other systems can use it.

[7] The full architecture is described elsewhere.

The *situational awareness system* is operated by an upper surveillance body that is responible for different border units. By subscribing to data from the *shared data server* (exploited and raw data) and including outside information this system will get an overall ground and littoral picture.

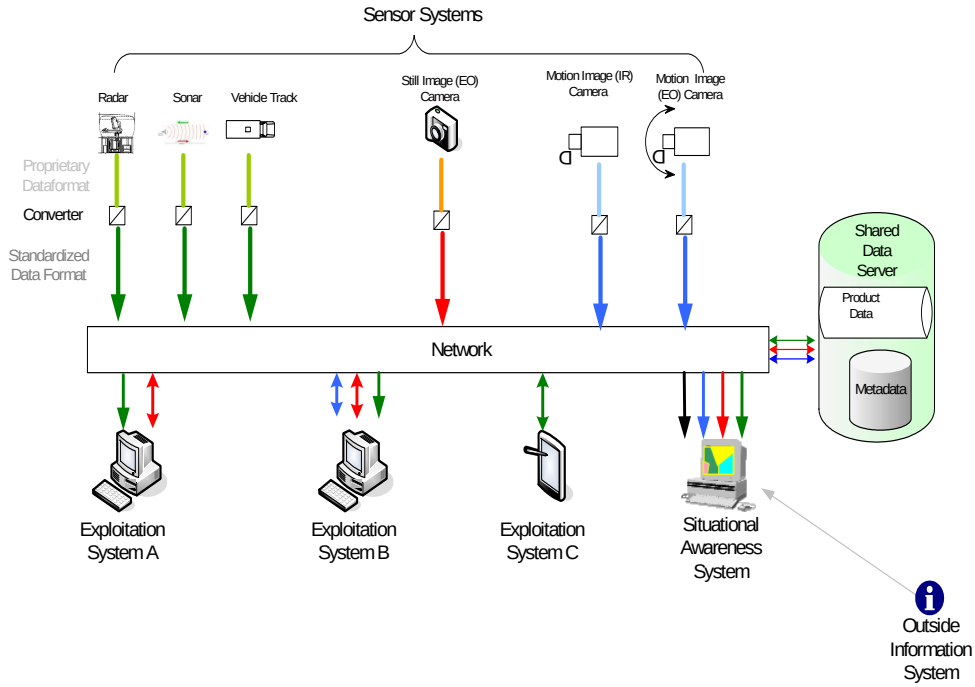

Figure 4: Integrated Surveillance System

5. Conclusions

At present border surveillance is often accomplished through separated stovepiped systems. Data that might be of interest for not only one but many surveillance units can't be shared and thus the capabilities to secure the border are limited. To accomplish an interoperable transnational surveillance system and include all relevant data sources a distributed architecture has to be chosen that is flexible and reduces the data load as much as possible. The architecture that is described in this paper is based on the usage of common data formats.
For a flexible data transfer it is necessary to convert the proprietary data formats that are used by the single system. As in a transnational

environment many systems are supposed to share data, the format should be predefined and reusable. The commercial standards that are described in 3.3.2 were often not defined for the surveillance domain and do especially not focus on security but on safety[8] aspects. The few standards that were developed for the surveillance domain focus on a single aspect (like the ASTERIX standard on radar and airborne systems). However it should be reviewed if these specialized standards could be adapted to a broader usage.
Standards defined within the military domain are of interest because they were created based on comparable requirements (see 3.3.1). As securing borders and infrastructure of terrorist attacks is a military task as well the cooperation of military and civil surveillance and reconnaissance systems will be of greater importance in the future. For that the usage of military standards has to be considered.

The producers and users of systems for border surveillance should take these considerations into account when defining internal data standards or adapting systems. As the definition of new standards or the commitment to predefined standards is a key enabler for enhanced security systems transnational projects have to focus on these efforts.

[8] Security is the protection of target oriented and malicious attacks. Safety is the protection against technical and human failure.

References

[1] Endsley, M. R. (1988): Situation awareness global assessment technique (SAGAT). Proceedings of the National Aerospace and Electronics Conference (NAECON). (New York: IEEE), 789-795.
[2] Waclawski, J., Gunn, J.: "Solving the WLAN VoIP Challenge", http://www.commsdesign.com/showArticle.jhtml?articleID=23900695
[3] Map taken out of the CIA World Factbook. https://www.cia.gov/cia/publications/factbook/
[4] Baran, P. "On Distributed Communications Network", IEEE Transactions on Communications [legacy, pre - 1988], Vol.12, Iss.1, Mar 1964
[5] Dutta Roy, S., Chaudhury, S. and Banerjee, S.: "Active Recognition through Next View Planning: A Survey.'' Pattern Recognition, vol. 37, no. 3, pp. 429 - 446, March 2004.
[6] Gill, M., Springgs, A.: Assessing the impact of CCTV. Home Office Research Study 292. Home Office Research, Development and Statistics Directorate February 2005. http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf
[7] STANAG 4559: NATO Standard ISR Library Interface. Edition 2. http://www.nato.int/structur/AC/224/standard/4575/ag4_4575_E_ed2_nu.pdf
[8] STANAG 4545: NATO Secondary Imagery Format (NSIF). http://www.nato.int/structur/AC/224/standard/4545/4545_documents/4545_ed1_amd1.pdf
[9] STANAG 4609: NATO Digital Motion Imagery Format. http://www.nato.int/structur/AC/224/standard/4609/4609_documents/4609Eed01.pdf
[10] STANAG 5516: Tactical Data Exchange- Link 16.
[11] STANAG 4607: Ground Moving Target Indicator Format (GMTIF). http://www.nato.int/structur/AC/224/standard/4607/ag4_4607_Ed1_eng_nu.pdf
[12] STANAG 3377: Air Reconnaissance Report Forms.
[13] OGC catalogue service specification: 2005. Open GIS Consortium. http://portal.opengeospatial.org/files/?artifact_id=5929&version=2
[14] SMPTE 12M-1999 Television, Audio and Film – Time and Control Code
[15] SMPTE 335M-2001 Television – Metadata Dictionary Structure
[16] SMPTE 336M-2001 Television – Data Encoding Protocol using Key-Length-Value
[17] SMPTE 305M-2005 Television – Serial Data Transport Interface (SDTI)
[18] ISO/IEC 13818-1-2000 Generic coding of moving pictures and associated audio information: Systems
[19] Eurocontrol standard document for surveillance data exchange. Part 1. All Purpose Structured Eurocontrol Surveillance Information Exchange (ASTERIX). 02. 2002. http://www.eurocontrol.int/asterix/gallery/content/public/documents/pt1ed129.pdf
[20] NMEA 0183 Interface Standard. NMEA 0183 Interface Standard