Integrating Persistent Surveillance Systems into ISR Architecture

Çağatay Soyer[1], Florian Segor[2], Barbara Essendorfer[2], Wilmuth Müller[2]

[1]NATO Consultation, Command and Control Agency NC3A, The Hague, Netherlands
Cagatay.Soyer@nc3a.nato.int
[2]Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe, Germany
{Florian.Segor, Barbara.Essendorfer, Wilmuth.Mueller}@iosb.fraunhofer.de

Abstract. Persistent Surveillance is an increasingly important concept in today's conflicts due to the asymmetric and complex nature of threats. With the proliferation of Persistent Surveillance Systems, NATO and its nations face a new challenge to integrate these systems into their overall Intelligence, Surveillance, and Reconnaissance (ISR) architecture. The same can be observed for the civil security domain. Persistent Surveillance Systems are widely used, but without integrating them into an overall Surveillance and Reconnaissance Architecture. This paper addresses the issue of integrating a Persistent Surveillance System into a standards-based architecture enabling efficient dissemination, search and retrieval. In particular, specific features of Persistent Surveillance Systems and current ISR architectures, potentially causing poor and inefficient integration, are identified. Functional and technical requirements and operating procedures are discussed as potential solutions to prevent these adverse effects. An example system compliant with the NATO ISR Interoperability Architecture (NIIA) is considered to demonstrate applicability and effectiveness of proposed solutions in a perimeter surveillance scenario. The proposed solutions, including the (I)SR Architecture are applicable also in the civil security domain.

Keywords: Persistent Surveillance, ISR Architecture, Interoperability

1 Introduction

Persistent Surveillance is a casual term without an agreed technical definition. When the term is used in a military context, it is generally understood that the system can be available or 'on station' on a continuous basis. In the civil security context, the term Persitent Surveillance is not used yet, but there exists the mutual understanding that a surveillance system is permanently available. Permanent availability requires not only 24/7 operation, but also an 'all weather' capability for the sensor payload and supporting elements. In this respect, it can be argued that ideal persistent surveillance (i.e. 100% availability) is a theoretical concept, which cannot be realized. In practice, however, several systems and systems of systems come close enough to meeting this

requirement. Current systems which are generally considered to be persistent include fixed surveillance cameras, aerostats, long endurance UAVs or teams of UAVs, unattended ground sensors for vibration, pressure, sound, chemical/biological/radiological agents and several types of intrusion detection systems.

In this paper, we primarily focus on video surveillance systems and imagery intelligence. However, other sensors are considered as complementary elements potentially co-existing with a video surveillance system, especially in a perimeter surveillance scenario. The key difference between imaging systems and other sensors is the significantly lower information content of the latter. For example, signals transmitted by vibration or acoustic sensors are usually processed and classified automatically in order to trigger an alert whereas a video stream requires human analysis.

In the next section we summarize the key features of ISR architectures using NATO ISR Interoperability Architecture (NIIA) as an example. In section 3, we identify the differences between a traditional ISR asset (such as a UAV system) and a Persistent Surveillance System, which make such systems a challenge for integration into ISR architectures. We propose potential solutions to the integration problem in Section 4. The proposed solutions are intended to be used both in military and civilian applications. In section 5, we discuss potential application in a perimeter surveillance scenario. The paper concludes with a summary and future directions.

2 ISR Architecture

For the military domain, NATO has defined an ISR Interoperability Architecture (NIIA) [1]. This architecture defines how reconnaissance and surveillance assets will achieve interoperability within coalition and NATO environments. A series of Standardization Agreements (STANAG) standardize the exchange of ISR data.

The STANAGs include amongst others:

- STANAG 3377, "Air Reconnaissance Intelligence Report Forms", which defines the standard reporting formats for intelligence reports (e.g. results of image exploitation processes) to operational users.
- STANAG 4545, "NATO Secondary Imagery Format (NSIF)", which establishes the format for exchange of electronic secondary imagery. Secondary imagery is sensor data that has been previously processed into a human interpretable picture.
- STANAG 4609, "NATO Digital Motion Imagery Standard", which intends to provide common methods for exchange of motion imagery (video) across systems within and among NATO nations. It includes guidance on uncompressed, compressed, and related motion imagery sampling structures; motion imagery time standards, motion imagery metadata standards, interconnections, and common language descriptions of motion imagery system parameters [2].
- STANAG 7085, "Interoperable Data Links for Imaging Systems", which establishes interoperability standards for imagery data links.
- STANAG 4586, "Standard Interfaces of UAV Control System for NATO UAV Interoperability", with the objective to facilitate communication between UCS and different Unmanned Aerial Vehicles (UAV) and their payloads as well as multiple

Command, Control, Communications, Computers, and Intelligence (C4I) users. Although not part of NATO ISR Interoperability Architecture, STANAG 4586 mandates the use of NIIA STANAGS for the Command and Control Interface (CCI) to enable interoperability of a UCS with other systems.

- STANAG 4559, "NATO Standard ISR Library Interface (NSILI)", which provides interoperability between NATO nations' reconnaissance databases and ISR product libraries by defining an interoperable interface to the ISR library systems (for more details see 4.3 and [4]).

The NIIA orients itself on the reconnaissance cycle (Figure 1). The reconnaissance cycle is a process, subdivided into five phases.

- Based on a Request for Information (RFI) by an operational user, a reconnaissance mission is tasked. The mission tasking identifies the area to be reconnoitered and further requirements set by the tasking agency.
- The aircrews prepare the flight plan to accomplish the mission.
- Subsequent to the flight preparations, the reconnaissance flight is performed.
- The reconnaissance flight mission is followed by the actual interpretation of the data collected during the flight.
- Upon completion of a mission, an exploitation report containing the results and answers to the RFI is prepared and forwarded to the tasking agency.

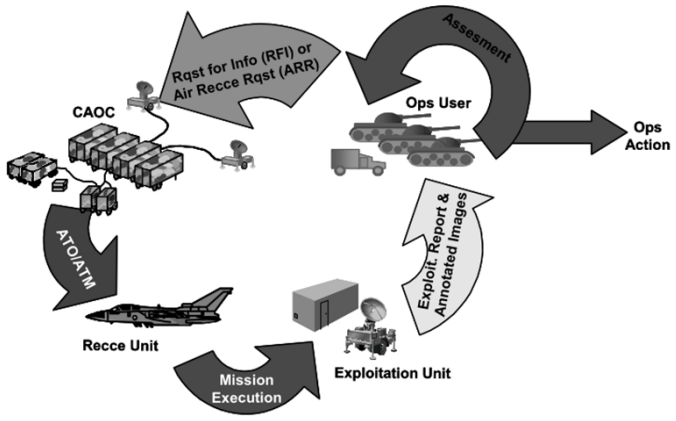

Fig. 1. The NATO Reconnaissance Cycle (from [1])

The reconnaissance cycle was designed with classical ISR assets in mind, and is not well suited for newer persistent capabilities like long endurance flight platforms, aerostats, mast-mounted long range sensors and unattended ground sensors, as well as small tactical UAVs with nowadays video and other sensing capabilities.

For the civil security domain a Surveillance Interoperability Architecture similar to NIIA does not exist.

3 Persistent Surveillance Challenge

In this section we identify key properties of Persistent Surveillance Systems that make them a challenge for integration into the overall ISR architecture. As mentioned above, video surveillance is our primary focus with other sensors considered as supporting elements providing either cueing or contextual information.

Using video as the primary sensor, coupled with other sensors, a persistent surveillance system is characterized through:

- Continuous streaming of large amounts of low relevance data
- High percentage of idle time
- Possibilities for automatic operation via cross-cuing and rule-based video analytics
- Multiple sensors in one system dynamically allocated by operator
- No pre-defined mission or collection plan
- Collection triggered by events either through human response or automatically
- Closed and highly dynamic tasking-collection loop

In a typical persistent surveillance scenario, video sensors deliver a continuous stream of data which shall be monitored and exploited almost instantly. Relevant information, captured in appropriate video clips and extracted images as well as other sensor data shall be stored and disseminated to a higher headquarter. For an eventual forensic analysis at a later point in time, the data streams shall also be stored for a longer term. Furthermore, a persistent surveillance system does not comprise only one single video sensor, but multiple sensors, ideally mounted on platforms with various characteristics such as fixed platforms on masts or roofs of high buildings, aerostats, and mobile platforms, like UAVs in different sizes – from small multi-copters to large surveillance assets. The data from these sensors shall be merged and displayed in one single monitoring and control station, which also allows control of different sensors both manually and automatically, based on detected relevant events.

The system generates multiple video streams and other data, which is generally stored only for a short time period unless it is directly relevant or linked to an event. This data is not presented or available to the people with overall responsibility of a particular area or operation. When high-relevance video is captured, this is generally assessed locally by the operators and recorded for future reference or reporting purposes. In a developing situation, this information is also used by decision makers to guide the operators, who actively control the sensors, creating a local tasking-collection loop. A significant amount of contextual information about the event is used during these activities. Current standards for recorded imagery or clips do not contain this context and therefore the resulting sensor products become very difficult or impossible to interpret at a later time.

In addition to the event context, there are several possibilities for automatic operation in conjunction with other sensors used as triggers. These include alerting the operator, e.g. in case of a critical event, performing automatic video analysis or recording tasks and cross-cueing of different sensors used within one system. These automation parameters, cross-cueing rules and overall system architecture are not

evident in recorded clips and imagery, contributing to the lack of contextual information and situational awareness.

In case of automatic video analysis (or video analytics), several algorithms are being developed, which enable detection and identification of humans, human actions and activities, vehicles, unattended objects, separation/merging events, intrusion/violation events, movement and trajectories [8]. Although some of these technologies are still at lower readiness levels, there is significant progress in specific applications. Developments in the field of video analytics are critical to dealing with high volumes of sensor data in Persistent Surveillance Systems. Current ISR architectures and standards do not readily capture results of video analytics and associate them with stored clips. As discussed in the next section, integration of Persistent Surveillance into current architectures will require solutions to associate automatic exploitation results with imagery, either directly or through further processing and mapping into existing metadata fields where possible.

The traditional reconnaissance cycle also fails to capture the highly dynamic nature of a persistent surveillance system, the need to react immediately on a critical event, and to cross-cue (automatically) other sensors or sensor platforms in near real-time. In a persistent surveillance environment, a sensor platform is triggered by events – a reaction of the human operator to some suspicious appearance or by other sensors. The tasking-collection-exploitation loop is therefore highly dynamic and it is a closed loop within the persistent surveillance cell. The only pre-defined mission or collection requirement within a collection plan is to task the persistent surveillance system to perform its mission.

4 Proposed Solution

Based on the requirements described in the previous section, solutions can be identified to facilitate the permanent use of surveillance systems, make them more reliable and improve the usefulness of the results. The proposed solution consists of both a new tasking-collection process and technical innovations.

In order to tackle the highly dynamic nature of a persistent surveillance system, a new tasking-collection process was defined (see Figure 2). The persistent surveillance system integrates all the sensors, sensor assets, and a local command & control station into one node, the Persistent Surveillance Cell (PSC). The Persistent Surveillance Cell is tasked by a Collection Planning System or a Command & Control Station of a higher headquarter only once, with the task to survey permanently a given area, an infrastructure, etc. The Persistent Surveillance Cell plans the sensor deployment autonomously, selecting dynamically the most appropriate sensors. Based on collected relevant data or critical events detected during its mission, a sensor re-deployment or tasking (deployment) of additional sensors under direct control of the PSC is performed. The higher headquarter and decision-makers are informed about critical events and may access relevant data, but sensor control authority remains within the PSC.

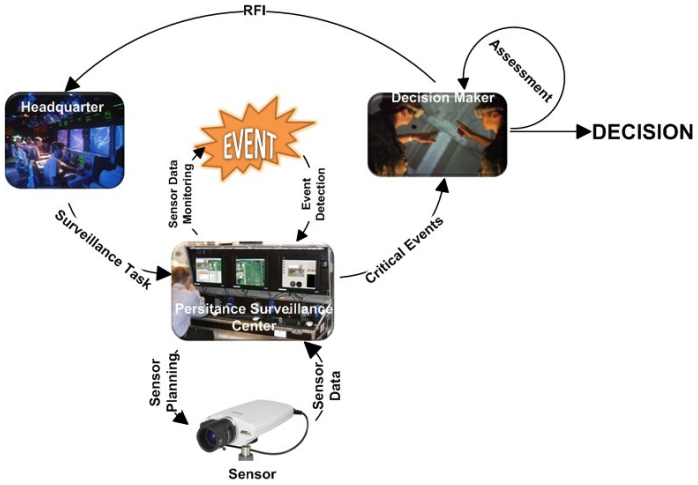

Fig. 2. Tasking-Collection Loop for Persistent Surveillance

The sensors and sensor assets are controlled and tasked by a control station, which provides the operator with

- Display of data stream from selected sensors and flipping through different streams
- Display of a map of the monitored area, showing also the sensor positions and their footprints, thus contributing to the operator's situational awareness
- Tools for tasking additional sensors, re-tasking sensors, and sensor-assets
- Tools for communicating with the higher headquarter
- Tools and algorithms for automatic video exploitation
- A storage and dissemination mechanism, allowing for interoperable exchange of relevant data with other PSCs or with higher headquarters.

4.1 Enhancing the discovery of useful information

A persistent surveillance system, such as an aerostat, can produce large amounts of video data containing only small fragments of useful information. This information has to be identified during the evaluation of the real-time data stream, and tagged (marked) appropriately for dissemination to the higher headquarter as well as for later search and retrieval. Such tags, also called metadata, help to find the interesting data by other users or other systems which has to process the data.

Evaluating continuous streams of video data in real time manually is only possible with enormous effort on personnel. Using a combination of automated video exploitation algorithms and supporting sensors as triggers, the workload on the operator can be reduced drastically. The operator may still screen the video data, but he will be alerted about events that were not recognized by him.

Possible critical events are those, in which a change in the environment is detected. The change detection method is based on comparing current images with an original base image and calculating the differences between the two images. For example, a

solid pan tilt camera can be trained on the surrounding terrain as part of its installation. This means it will record its environment and create an internal image of a “normal” situation. In operational use, this camera constantly matches the current environment to what was trained as "normal". If the camera (the algorithm) detects a deviation, extended algorithms can be used to process this further and alert the operator if the deviation is critical, or the operator is alerted immediately.

Additional sensors (vibration detection, magnetic sensors, passive infrared sensors) can be used to trigger the video sensors by cuing them to the corresponding location and by providing information for tagging the video stream. If the data is merged from several sensors and types of sensors it is possible to identify the cause of the disorder.

The operator is provided with an effective user interface, which allows him to quickly mark and tag the relevant video segments. In addition, the operator is supported by automatic clipping and tagging mechanisms, including metadata generation. STANAG 4609 (NATO Digital Motion Imagery Standard) [2] of the NIIA provides the possibility to add metadata to a video stream, but the offered metadata types are not tailored to persistent surveillance systems. Within a PSC additional metadata can be generated. Some examples of this metadata are as follows:

- Local features: Pre-defined areas of interest, cultural and geographic features inside a fixed sensor’s footprint can be used as metadata to provide additional information about the content of video clips.
- Periodic or planned activities: Video segments can be clipped and tagged automatically based on periodic or planned events such as patrols, force movements, shift changes and routine activities of the local population.
- Change detection: Video segments can be marked and tagged based on the results of change detection as described in Section 4.1.
- Video analytics and cues: Cues from other sensors and built-in video analytics rules can be used to automatically clip and tag video segments. These include motion detection, intrusion detection, automatic target recognition and tracking.

4.2 Adding operational context

In addition to external events and sensor data processing, operational context plays an important role in understanding video content. One possibility to capture this information is for the operators to manually enter/select operating modes for their system such as “idle”, “search”, “track vehicle”, “track human”, etc. which can later be used as additional metadata attached to clips.

In an attempt to automate this process (at least partially), an additional inward directed analyzing component can detect the situation based on the behavior of the operator and draw conclusions about possibly important meta information.

For example during "search" the common operator behavior is "pan/tilt, zoom in, zoom out, pan/tilt, zoom in, zoom out, etc." Similarly during "track vehicle", the behavior is a smooth path aligned with roads with a relatively fixed field of view. Combined with data from a Geographic Information System (GIS), the current task can be detected automatically and confirmed by the operator.

Another interesting aspect is the possibility of strengthening the information by the use of semantic analysis. This way, linkages between data sets can be detected automatically. Because of the tags and metadata associated, the semantic analysis can draw conclusions on possible cross-connections and the unity of different information is recognized. For example, such connections can be made to previous mission reports or even chat logs.

The combination and data fusion of different sensors as mentioned earlier can also be done on a semantic basis. If the system can assign a spatial and temporal component to a detected event, identification of other affected sensors becomes possible and events in the past which might be related to the current event can be linked.

4.3 Storage and Dissemination

To be able to share information that was collected in one PSC with other PSCs and, more importantly, a higher headquarter, an adequate storage and dissemination architecture has to be defined and put in place [3]. A higher headquarter should be able to access relevant data from multiple PSCs, different organizations and different sources to enable situation awareness. As mentioned above it is of importance that surveillance information is tagged with specific metadata and can be discovered.

Standardized interfaces and data formats help to integrate information flexibly. The NIIA (see section 2) foresees STANAGs as a solution. For information sharing the Coalition Shared Data (CSD) concept based on STANAG 4559 [4] is of interest.

Here sensor systems store relevant surveillance data like images, videos, radar plots or surveillance reports on a local server (see Figure 3). Connected to the same network, exploitation systems are taking in a filtered set of the provided information (depending on the tasking) by querying or subscribing to metadata. By fusion and analysis they generate new additional information (e.g. reports) that is also stored on the data server(s). Situational awareness systems are able to display selected intelligence and can ask for additional information from sensors, exploitation or information systems to support decision makers. The concept foresees that each processing system can use internally proprietary formats. In this way each system can provide advanced mechanisms of data processing and exploitation with the full spectrum of information a sensor type provides. For dissemination purposes, the proprietary data formats are converted into standardized ones. In this way, other communities of interest (COIs) do not have to concentrate on specifics of the surveillance domain.

On a CSD server the data (sensor data, exploitation results) is stored together with the attached metadata. Within the metadata all relevant aspects of the product (depending on the domain) are defined and searchable. Those parameters could be for example: location, time, speed, size, friend/foe, weather condition, certainty of the info, and product type. An important aspect of the CSD concept is the ability to synchronize data over wide area networks. Here a server A connects to another server B and performs a subscription on all metadata or specific aspects (e.g. only video data). By this the information about all data is available in the full network. The original product data (e.g., images, video clips of possibly high data volume) is kept on the originating server. Only when a client connected to server A has analyzed the metada-

ta and is actually interested in a product that resides on server B the specific data is transferred. Transferring only relevant high-volume data over the network saves bandwidth.

Fig. 3. Information sharing within a local architecture

The CSD concept is based on NATO STANAGs (see section 2). It has already been tested and fielded by different nations and system owners in exercises and military operations (e.g. [5], [6], [7]). However, this architecture was developed with a focus on classical ISR assets, such as surveillance aircraft. In order to adapt the CSD concept to other environments like the Persistent Surveillance scenario, the metadata model of the CSD can be extended as described in the previous sections. Specific attributes or new entities can be added and, if desired, access options can be defined by filtering through those attributes. In the process, the core of the data model is maintained and the server continues to be compatible with other CSDs.

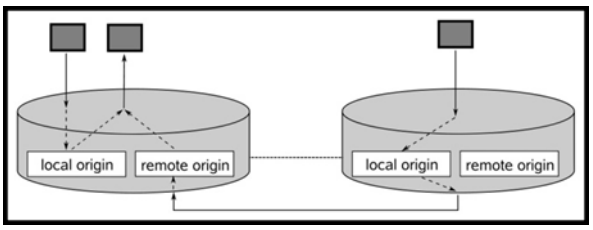

Fig. 4. Synchronization, single point of contact

Another aspect of adapting the CSD concept to the usage of “off the shelf” sensors or exploitation systems is to add an additional interface to the CSD. The STANAG 4559 demands CORBA based client-server interaction [4]. This is specific to the standard and therefore interoperability with civil systems is somewhat complicated.

Currently work is performed to add an interface to the CSD that takes open standards like the Web Feature Service (WFS) by the Open Geospatial Consortium (OGC) into account. First tests are showing good results.

By the usage of open standard interfaces the CSD could be used by a wider community and in a civil security environment a lot easier than before. Through this and by extending the metadata to the requirements of the PSC domain the CSD concept recommends itself to be used as a means of data storage and dissemination among PSCs and higher headquarters.

5 Perimeter Surveillance Scenario

This section discusses the use of a system that allows persistent surveillance and threat analysis for an infrastructure with a permanently high threat potential and its integration into an existing (I)SR Architecture.

On this assumption it is basically irrelevant whether it is a civilian or military scenario because the main distinguishing features can be seen in the response to a perceived threat and not so much in their reconnaissance.

Let us consider the following scenario: we are in a property with a size of 200 x 200 meters. The perimeter is secured primarily by a two meter high fence to the outside. Within the site there are several buildings. The main command and control center is located inside one of the buildings. In addition there is a second control center (PSC) which oversees the use and control of the applied sensor network.

On the perimeter a permanent network of motion detectors, vibration sensors and various video cameras (IR, EO) is installed. Imaging sensors mounted on fixed platforms, like masts or roofs of high buildings provide a complete, persistent monitoring of the area. An aerostat serves as a long endurance supervision platform above the area, which provides an overview of the situation. In addition, there are several multicopter drones on standby and can be used as needed for single spot reconnaissance.

Of great importance, however, are not only the sensor systems that are responsible for the provision of environmental data, but also the back-end systems which allow fusion of data and analysis at a high level. A permanent threat does not necessarily mean a permanent real danger. Due to the high idle times, the system must have certain intelligence to detect acute hazards independently and alert the operator.

Most of the data created in this scenario is video data. In the PSC, data is collected continuously and must be evaluated, managed and stored. The associated metadata to the video recordings e.g. footprint, time, or used sensor carriers have to be given special consideration because this information contribute significantly to situational awareness. As a very efficient way to keep video and metadata together, the PSC can provide its data on an external interface in the STANAG 4609 standard. The two data types (video and metadata) are packed into one combined data stream, which is then stored on a local CSD server. The local CSD server is connected with CSD servers in the main command and control center. Using STANAG 4609 for providing video data and a CSD server for storing and disseminating the data, the PSC is effectively inte-

grated into an already existing ISR Architecture. Using the provided standards such as STANAG 4609, as it has been done in this experiment, the exchange of information between the PSC and other nodes within the ISR Architecture is seamlessly possible.

Within a PSC the amount of generated data is very large and not all of this data ends in the CSD for further dissemination to headquarters. However, events that are recorded by the sensor network could remain entirely undetected and a subsequent review of the data will become necessary. Due to this, the collected data as well as sensor status data, including the dependencies between the employed sensors is stored persistently and tamper-proofed in the PSC. This provides the ability to replay a situation as it was recorded by all sensors in real time after the event took place. Undetected events or activities can thus be explained and analyzed retrospectively. In addition, the operator has the possibility to even retrospectively create CSD products.

In support of the operator, video analysis algorithms are used. These algorithms provide functionalities like video stabilization, super resolution, and are detecting and tracking moving objects such as people or vehicles in order to mark suspicious movements or identify potential threats. Artificial intelligence methods like a rule processing engine are used to detect and respond to certain events. Detected anomalies can then be reported and placed as a product into the CSD automatically.

If a sensor placed around the perimeter is triggered, some automated functions will be called. This allows recognizing that the sensor is located in an area that cannot be seen by a stationary camera. Therefore, an automatic command to the aerostat's camera platform is sent to align its payload to this position. The operator will be alerted by just the automatic response of the system. The IR sensor on the aerostat detects a nonspecific heat signature, but neither the software nor the operator is capable of identifying the target. After a brief observation, however, a movement is registered and the software recognizes that the anomaly is a human trespasser in the security zone. As a result an alarm is generated and the operator of the sensor network is provided with a feedback about the perceived threat. In addition, the reconnaissance results are automatically or semi-automatically stored in the CSD. The threat information is synchronized to the CSD in the main command and control center, where this data is accessed and further analysis is performed. In the absence of information about the intentions of the unidentified person a miniature unmanned air vehicle (multicopter UAV) is sent autonomously to the position with an optical sensor as payload. The UAV is manually maneuvered to get the best view on the localized threat. The result of this single spot reconnaissance is also streamed to the main command and control center. The PSC will switch back into the routine mode until the orders are changed or a new alarm occurs.

6 Conclusion and Future Work

Persistent Surveillance Systems present a challenge to ISR managers in military and civilian domains due to their differences from traditional sensor platforms. Current ISR processes and interoperability architectures designed around a tasking-collection-exploitation cycle do not necessarily apply to such systems, which continu-

ously provide real-time video and other sensor data in border surveillance or perimeter protection applications. Furthermore, due to continuous and unstructured collection, a large percentage of collected data is not directly relevant to an event, making it difficult to exploit for intelligence purposes. As a result, sensor products from these systems are rarely available or useful to a wider group of users through a dissemination and exploitation network.

In this paper, we compared Persistent Surveillance Systems to traditional ISR assets and identified key differences that make them difficult to integrate into a classical ISR architecture such as NATO ISR Architecture or NIIA. We proposed manual and automated methods to associate relevant metadata and contextual information with imagery products from Persistent Surveillance Systems. Based on our experience with operational and research systems, we envisaged a scenario where these methods could significantly improve our ability to exploit sensor products at a later time. A key requirement in our approach was the ability to integrate with an existing ISR Architecture such as NIIA in a relatively short time, rather than to propose bespoke solutions. Therefore, the use of metadata fields in video and imagery STANAGs is proposed as the technical solution by which context information is captured, archived and discovered. However, new procedures and algorithms are required to generate additional metadata that is either not present or not exploited in current standards.

The next step in our research is to implement and demonstrate the proposed solutions in a real world system, which is already based on NIIA. For this purpose, an existing perimeter surveillance system will be used and modified as discussed in Sections 4 and 5 in order to assess its potential to achieve better utilization of continuous sensor feeds. Initial results from development of proposed methods as well as the implementation of NIIA in a perimeter surveillance application have been promising. If successful, these solutions can also be utilized to reduce analyst effort required for exploiting increasing volumes of imagery from traditional ISR assets.

References

1. NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA). Allied Engineering Documentation Publication (AEDP)-2. Edition 1. (2005)
2. STANAG 4609 (Edition 3) – NATO Digital Motion Imagery Standard. Edition 3. (2009)
3. F. del Pozo, A. Dymock, L. Feldt, P. Hebrard, and F. Sanfelice di Monteforte, "Maritime Surveillance in Support of CSDP," The Wise Pen Team final report to EDA steering board, European Defence Agency, 2010.
4. STANAG 4559 (Edition 3) – NATO Standard ISR Library Interface. Edition 3. (2010)
5. SOBCAH. Surveillance of Borders, Coastlines and Harbors. 2005. DOI= ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/sobcah_en.pdf
6. Stockfisch, D. 2008. Common Shield 08. TechDemo 08/Harbor Protection Trials. Strategie & Technik, October 2008.
7. Trial Quest. 2007: Key NATO Reconnaissance Technology Passes Major Test. DOI= www.nato.int/docu/update/2007/12-december/e1210d.html
8. Ma, Y. and Qian. G. editors: Intelligent Video Surveillance: Systems and Technology. CRC Press, 2010.