JRC Scientific and Technical Reports

SeBoCom Pre-Study

A preliminary study on
Secure Border Communications

Dimokritos Tziritis
EU Frontex Agency

Aleksander Pur
Ministry of the Interior, Slovenia

Franco Oliveri
EC Joint Research Ispra

Advanced Radar and Telecommunications Techniques for Security

Sensors, radar technologies and cybersecurity unit

Institute for the protection and security of the citizen

EUR 23536 EN - 2008

JRC
EUROPEAN COMMISSION

FRONTEX
LIBERTAS SECURITAS JUSTITIA

The Institute for the Protection and Security of the Citizen provides research based, systems-oriented support to EU policies so as to protect the citizen against economic and technological risk. The Institute maintains and develops its expertise and networks in information, communication, space and engineering technologies in support of its mission. The strong crossfertilisation between its nuclear and non-nuclear activities strengthens the expertise it can bring to the benefit of customers in both domains.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Centro Comune di Ricerca
Via Enrico Fermi 1, Ispra (VA) 21020 ITALY

E-mail: Franco.Oliveri@jrc.it
Tel.: +39 0332 789320
Fax: +39 0332 785469

http://www.jrc.ec.europa.eu

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC 48004
EUR 23536 EN
ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

Table of Contents

1. Executive Summary

The main objective of the SeBoCom project was to define the way to proceed to a further and complete study. This task was to be achieved through this pre-study and through a Workshop involving end-users to stimulate the discussion and gain the input regarding their needs.

The issues related to the collaboration of different forces, within the same Member State and from different Member States, aimed at securing the EU border against the present threats have already been analyzed in several previous studies.

However, there is a need for a study that will aim at bringing together operational and technical knowledge to help providing the European Border Forces with effective, reliable, easy to use communications infrastructure capable of secure, end-to-end delivery of voice and data.

This study has already collected some initial data on the present Communications infrastructures outlining the co-existence of many different systems, some already based on digital technology, others outdated or quite obsolete.

One of the key finding of the present study is the need to define joint procedure to manage communications among different bodies belonging to different Member States: the most reliable and secure telecommunication infrastructure will be useless if there is no agreement on the type and structure of communications that are transmitted over the infrastructure.

The full fledged study will have to:

- Create and populate a database of the existing telecommunications infrastructures;
- Identify operational scenarios for different contexts which gain consensus from all interested organizations;
- Identify operational requirements focusing on the specific needs of Border Security in the perspective of the present technological state of the art and the legacy systems still in use;
- Establish a permanent forum, managed by Frontex that officers from the relevant organizations can use to share views and reach consensus on operational procedures.

2. Introduction

2.1 Communications: the key enabler for Field Operations

Communications allow operators to coordinate their actions to be more effective in performing their tasks; therefore communications are a key factor for the successful execution of any organized operation.
When we refer to a communication system we consider it as a whole, therefore we include both the wired and the wireless part of it, the wireless part often being the more needed and critical one.

In routine operations of any organization, the communication system is tuned to the average needs by daily usage: the staff in charge of the communication system has a continuous feedback on the system and users learn the workaround to overcome the most annoying defects of the system.

The situation changes dramatically if an emergency situation stresses the performance of the system or if it is required to integrate the stand alone communication system of an organization with the ones of other organizations.

The worst case is when the two situations mentioned in the previous paragraph happen at the same time.

A further bit of complexity may be added if the emergency situation occurs in a foreign country where infrastructure may or may not be available and the spectrum occupancy may be fairly unknown.

The lack of interoperability among the different communication systems is usually pointed out as the most hampering factor in joint emergency operations: this is obviously true, but to reach a real solution to this problem it is necessary to be aware that procedures for exchanging information, and a peer to peer relationship, must be established at the appropriate level before the operation is initiated.

It is clear that to allow different Bodies from different Member States to work together there are difficulties at different levels:

- Political;
- Law and regulations;
- Procedures;
- Language;
- Technical.

Each level requires to be managed and a proper solution needs to be found.

To tackle, at least the procedural and technical levels, it is necessary to:

- Define procedures accepted by all the players involved in the joint operations (such procedures should also consider the exchange of possibly classified information over a network that may be used also by NGOs without any formal clearance);

- Find technical solutions, such as gateways, to allow different organizations to communicate maintaining the use of their equipment (avoiding training issues for in field operators);
- Train the operators to perform their duties in joint operations in such a way that they become familiar with this, otherwise, unusual environment.

2.1.1 Operational aspects

It is necessary to differentiate various scenarios that may occur in an emergency operation using different categories.

Scenarios can be differentiated by:

- Environment:
  - ◊ Existing (non existing) infrastructure
  - ◊ Available spectrum
  - ◊ Threats
  - ◊ Orography
- Number and type of involved organizations
  - ◊ Military/non military
  - ◊ Public safety
  - ◊ NGOs
- Same Country/different Countries
  - ◊ Language problems

2.1.1.1 Environment

It is important to know in advance the situation of the area where the operation will be carried out, both to use it or to avoid interferences.

It would be advisable to prepare and maintain a database of the existing communications infrastructures in the Countries where an intervention may be foreseen.

The possibility of using an existing infrastructure can greatly reduce the set up time of a communication network, but small issues like the kind of electrical power available or the available interface in the existing network (as an example the availability of T1 interfaces rather than E1) can jeopardize the use of the existing infrastructure.

The unavailability of the frequency band used by the communication systems used by the deployed organization, may completely disrupt the operation, while in case of a very disastrous event the lack of any communication whatsoever may be exploited in the short time by using the so called “GSM in a box” networks that can provide immediate GSM coverage as well as hooking up to a satellite and giving instantaneous communication with the rest of the world.

Dense urban environments or very hilly territories make, obviously, a lot of difference in the establishment of a radio network compared to a flat suburban area.

Similarly, being in a hostile environment with a significant possibility of attacks on transmitting equipment may suggest the use of very specific radio equipment (frequency hopping and spread spectrum).

Beyond the purely communications related aspects, all the logistic and safety aspects have to be considered when operating in a disaster scenario.

2.1.1.2 Organizations

The interaction between different types of organization may require a very careful handling of the access to the communication media as well as information.

Military organizations do not, generally, agree to share their networks even with security forces, let alone with civilian NGOs. In such a case it will be mandatory to have different infrastructures connected by secure gateways.

If the number of organizations and Countries involved increase, the scale of problems to be solved at organizational level greatly increases and the technicalities of interoperability become irrelevant.

2.1.1.3 Countries

If more Countries are involved, once all the major relationship problems have been solved and the chain of command has been established, we still have the language barrier.

2.1.2 Technical aspects

When people think of the problem faced by operators in the field, in terms of interoperability, the most mentioned issue is: over the air interoperability [air interface].

It is necessary to understand that although it may appear “nice” to have over the air interoperability, it is, actually, not that important because there are other cheaper ways to allow different entities to communicate: for example through gateways.

Gateways allow different entities to use their own networks and their own equipment within the organization while they also allow the communication to be bridged to other networks.

Most systems, commonly used, such as TETRA already have provisions for such need: it is obviously necessary to prepare the operation in advance in order to allow the communication experts to activate and connect such gateways.

Software radios are often depicted as the solution to interoperability problems; it is important to be aware that a Software Radio able to download a different waveform, common among the different forces operating in the field is still far from being commercially available at a reasonable price and, anyway, the organizations working in the field will have to schedule the purchase of these equipment and this will happen only when the present ones will be phased out, at the end of their lifecycle.

At technical level there are many other issues to be addressed, such as:

1. Security:
   - Encryption
   - Right of access (authentication)
   - Interconnection of different entities (Military, Police, Emergency services, NGOs, etc.)
2. Reliability:
   - Reversionary modes
   - Back-up systems
   - Networks interconnections
   - Satellite/GSM/UMTS/WiMax/WiFi, etc.
3. Services:
   - Voice
     - Traditional calls
     - Direct mode
     - Group calls
     - VOIP
   - Data (Real time/ non real time)
     - Electronic messaging (SMS, MMS, Email).
     - Access, switching, and rebroadcast of real-time video sources to field resources.
     - Transmission of complex data structures
     - Transmission of user and patient monitoring telemetry.
     - Transmission of geographical location data (Galileo)
     - Transmission of streaming data (full-motion video, still photographs, images, sounds).
4. System of systems:
   - System integration and interoperability
   - Transparent network and system access.
   - Over the air interoperability
   - Spectrum management
   - Network interoperability (Gateways, connections, etc.)
   - Network of sensors
   - C^{4}I
   - Database integration
   - Interferences
5. Technologies:
   - Software Radio
   - Gateways
   - TETRA/TetraPol
   - GSM/UMTS/WiMax/WiFi
   - Ad Hoc Networks
   - Satellite communications
6. Safety (radiated transmission power):
   - Work safety of personnel
   - EMC

2.1.2.1 Security

Security is a relevant aspect of a communication network for Border Surveillance operations. There are many different techniques to guarantee the security of a Network, both for the wireless and for the wired part of it; therefore it is feasible to provide end-to-end security for any kind of connection.

Unfortunately when different organizations are involved, even if they have the same “level” of security and even the same type of equipment, the interactions at political level between the different Security Agencies are difficult and they often require an advanced planning. Encryption is one of the key factors required to ensure the security of a communication network and encryption keys need to be exchanged among the different organizations in accordance with pre-defined procedures and each organization has to trust the others on the procedural aspects.

The complexity of the problem, also at technical level increases when organizations with different internal levels of security (Military, Police, Emergency services, NGOs, etc.) need to co-operate, because the interconnection among the different networks must be able to cater for different levels of security and that should be provided through Right of access (authentication) at different levels.

2.1.2.2 Reliability

Any system taken to the limit of its capacity and operated by personnel under stress may happen to fail; communications being crucial to the effective execution of Border Control operations, it is pivotal that the communication systems for Border Security are intrinsically designed to be reliable; this includes the provision for Reversionary modes.

Reversionary modes are operating modes used by a system when failures make the system unable to be fully operational; a good system, even under some sort of failure, should be able to automatically switch to a (reversionary) mode that will provide the best possible service, in the specific situation, to the user.

Good practice to increase the system reliability is also to provide a back-up system, but such systems should also be designed to provide interoperability.

In communications, an excellent approach to reliability is the creation of a meshed network of networks in order to provide many possible paths to each end to end connection; obviously, also in this case, each network should be able to provide the minimum required characteristics for security, etc.

In order to further improve the resilience of the communication system it is advisable to utilize networks using different technologies and different frequencies, such as satellite/GSM/UMTS/WiMax/WiFi, etc.

2.1.2.3 Services

Communications for security forces, such as Border Security, require a number of different services; they can be grouped in the following three categories:

1. Voice
2. Data (Real time / non real time)
3. Streaming

2.1.2.3.1 Voice

Voice calls can be further categorized as follows:

- Traditional calls
- Direct mode
- Group calls
- VOIP

Traditional voice calls are generally provided by any phone system, while direct mode calls are established directly between two terminals without using any Base Station, they are required in case of operation outside the coverage area of the system or in case of failure of the network.

Group Calls are typical of single channel Private Mobile Radio, but they are very useful in operations and they are part of the mandatory characteristic of systems such as TETRA: they allow operators to be grouped in such way that it is possible to establish a call that connects the whole group so that everybody can listen when anybody else talks.

VOIP may be one of the key technologies for an all IP Network that, leveraging on the intrinsic interoperability provided by the Internet Protocol (IP), could foster the integration of networks and the creation of more resilient and interoperable communication systems.

2.1.2.3.2 Data

Data calls can be further categorized as follows:

- Electronic messaging (SMS, MMS, Email)
- Transmission of complex data structures
- Transmission of user and patient monitoring telemetry
- Transmission of geographical location data (Galileo)

These functions that are usually available on most public communication networks such as GSM or UMTS and can provide very valuable support to Border Secure Operations. It is anyway necessary to carefully evaluate their use in order to correctly size the capacity of the network and to define their use in the operational procedure.

As an example, SMS delivery within a specified time frame, in GSM Networks, is not guaranteed, as anybody had surely experienced; therefore a correct procedure should forbid their use in circumstances that require timely guarantee delivery.

2.1.2.3.3 Streaming

Also the streaming functions, such as the ones listed below, are easily available on commercial systems and they can be very useful in field operations:

- Transmission of streaming data (full-motion video, still photographs, images, sounds).
- Access, switching, and rebroadcast of real-time video sources to field resources.

But their utilization should be well defined in the procedures since they cause a significant load to the communication network and procedures should take into account that many legacy networks are completely unable to support them.

2.1.2.4 System of systems

Nowadays, the integration of a large number of functions through communication systems, while providing the users a significant number of vital services, also makes them dependent on the correct operation of these systems of systems; moreover sometimes these systems are interconnected without paying enough attention to the need of operators in the field to have the services they need without being burdened by the hurdles of getting the systems to work together.

Thus it is crucial that the integration of systems is implemented focusing on the users' need to have interoperability and seamless access to networks and systems.
Over the air interoperability, spectrum management, interferences are issues that must be carefully studied and solved to allow different systems to work together as well as in cross border operation.

Networks of sensors could be greatly helpful in Border Surveillance as well as in other operations, but their deployment and their integration in the communication networks must be well planned and elaboration nodes should be introduced since the distribution of raw data from sensors to operators may not only overload the communication networks, but may also flood the users with raw data rather than provide them with information.

2.1.2.5 Technologies

The following is a non exhaustive list of communication technologies that are, presently, considered suitable to be used in an interoperable communication system for Security Forces or to be used to facilitate interoperability:

- Software Defined Radio (SDR): is a technology aiming at implementing all the characteristics of a radio “waveform” in software having a “standard” platform, waveform denoting not just the time-dependency of the radio wave but all the characteristics of the radio communications protocol. The expected advantage of SDR is the possibility of implementing different radio standards on the same hardware to allow the Software Radio to be compatible with legacy system as well as with new generation systems; SDR is also expected to host different waveforms at the same time, thus being able to act like a bridge between to different radio system providing over the air interoperability;
- Gateways: are equipment capable of bridging two or more networks, they are usually satisfactory in bridging voice calls, but they are often not capable of providing the full set of features across the networks;
- TETRA/TetraPol;
- GSM/UMTS/WiMax/WiFi;
- Ad Hoc Networks;
- Satellite communications.

2.1.2.6 Safety (radiated transmission power)

Safety issues are twofold, they are relevant for the personnel using the equipment and to the people living or temporarily staying in the proximity of transmitters such as Base Stations.

Usually there are strict safety rules regarding the limits to the radiated power of every transmitter in relation to the distance of human beings as well as their exposure time.

It is necessary to pay attention also to different rules set in different countries, especially for the ones that are not EU Members: during joint operations, it can happen that partners use transmitters well above the safety threshold; while conducting operations abroad it is necessary to avoid interfering with local wireless services (communications, radars, etc.). Thus a good knowledge of the radiation pattern of one's own equipment is needed to be sure of abiding by the EMC regulation of the hosting country.

2.1.3 Consideration

As a rule, most of the issues can be technically addressed if agreement is reached on the related political questions.

If such issues are not solved and it is required that the technical solution is open enough to accommodate any possible political choice, then too many options remain opened and the problem, from the technical point of view, becomes quickly too complex.

The issue of secure communications between different organizations working together in an emergency situation is crucial.

There is no single solution for every situation; it is very important to identify the different operational scenarios in order to select the most effective solution.

Advance knowledge of the environment to be faced in the field would be very helpful in the definition of the specific solution and in its implementation.

Training of the communications experts and of the personnel is mandatory to allow them to successfully operate in crisis situation.

No technical solution will be effective if the mission had not been prepared at political level (procedure, chain of command, permission of access to services and data, etc.).

2.2 Border Security Forces in Europe[1]

Border Guard and Coast Guard Services, Police Forces, Border Police, Customs, Airport Police are some of the different authorities in the Member States that monitor the activities on and through the external borders of EU.

The description of the existing situation gives more than 50 authorities under more than 30 Ministries only for the "blue borders" (maritime). The Member States (MS) have undertaken actions to ensure the cooperation between the national authorities as well as the coordinative approach concerning external borders security.

Under these circumstances, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) was

[1] All the information contained in this paragraph are extracted from the FRONTEX website: http://www.frontex.europa.eu/

established by Council Regulation (EC) 2007/2004. It is a specialized and independent body tasked with coordinating the operational cooperation between Member States in the field of border security.

Frontex focuses on six principal areas: Carrying out risk analysis; Coordination of operational cooperation between Member States; Assistance to Member States in circumstances requiring increased technical and operational assistance; Providing Member States with the necessary support in organizing joint return operations; Assistance to Member States in the training of national border guards; Following up the development of research relevant for the control and surveillance of external borders.

In order to enhance this cross-border and cross-sectoral cooperation and coordination, Frontex took the following initiatives.

First, it established the "European Patrol Network" (EPN), which is a permanent regional border security concept that enables the synchronization of national measures of the Member States and their integration in joint European activities. It introduced the National Coordination Centers (NCCs). As explained before, most MSs have, (regarding the borders), two, three and more authorities responsible for the surveillance and security. So, it is needed to have one point per MS in order to have better coordination. This is the National Coordination Center (NCC). Except of that EPN increased the systematic patrolling in Patrolling Areas. It extended the Joint Operational Areas and Frontex Joint Operations. Hera 2007, Nautilus 2007, Poseidon 2007, Pandora/ Minerva, Heracles, KRAS, Agelaus and Zeus are some of the Joint Operations Frontex coordinated previous years, jointly with the MS.

The second initiative was the establishment of CRATE and RABITs.

CRATE is a centralized record where the member states have enrolled their assets, which could be deployed under certain conditions.

RABITs is a pool of experts from the Member States, trained by Frontex, that could be deployed in joint operations in urgent and exceptional situations.

The above mentioned is the present situation and the challenges faced regarding Border Security Forces in Europe.

2.2.1 The communication landscape of Border Security Forces in Europe

2.2.1.1 Existing Situation

2.2.1.1.1 General

Border Guard Authorities are currently using a number of diverse and competing technologies. The diversities in the technological solutions create an interoperability problem at different levels that reduces the efficiency of the operating competent authorities within a Member State and much more in joint operations at a European level.

Generally speaking, the market of "Border Security Communication" equipment is relatively small and mainly based on governmental funding. Consequently it increases the market fragmentation and equipment costs.

It is important in the early research stages to consider the development of interoperable and harmonized technologies.

There is also, lack of research toward the use and optimization of existing technologies that will take into account public security users' requirements and will be focused on heterogeneous multi-standard system approach.

The common European user requirements and scenarios must be considered in R&D process and has not been developed yet.

In many countries the level of penetration of data communications in border security communication is very low. Border Guard user groups are still using, more or less, mainly voice communication. The promotion and further introduction of digital technologies for data communication can dramatically increase the efficiency of Border Guard Officers.

2.2.1.1.2 Challenges

There are many barriers to allowing more 'open' access to information and communication systems. Often they are not technical but rely on the adoption of common language, processes and operating procedures.

Conflicting terminology and lack of trust are key disablers to information sharing. But what are the other obstacles? Barriers to the access of information are still present. How could they be overcome?

Is data ownership still a significant issue, and who is legally responsible for subsequent action once disparate sources of information are collated, analyzed and new conclusions drawn? There are also questions such as: Who is in control? Is the controlling entity reliable, safe and dedicated?

These questions are not meant to be all encompassing; they merely reflect a small number of the issues associated with authorization, authentication, security and access, which for the most part are being dealt with on an ad-hoc basis rather than through the adoption of cohesive or standard approaches.

2.2.1.1.3 The communications landscape

Several Member States use TETRA and much less use TETRAPOL. These systems are mainly used for voice communication and much less for data communication. In addition several Member States use interfaces and gateways in order to interconnect with the old analogue systems. The majority of MSs have no encryption in the analogue systems. They have the standard encryption in digital systems like TETRA / TETRAPOL with additional services like "group calls", "Direct Mode" or "sensors connection". Group calls are simply calls which more than one person can listen to. A direct mode call is sent directly from phone to phone, without going via base station, possibly needed in case of network failure. Sensors connection: a sensor can be connected to the digital port fitted to TETRA phones to send low-bandwidth information from a sensor, for example, an alarm to indicate the presence of an intruder detected by an IR camera with intelligence.

The coverage of the "external borders" (land and sea) in most of them are very good (90-100%).

Furthermore, in most of the MSs different authorities involved in border security can communicate with each other through the above mentioned digital systems. Communication between MSs regarding Border Security is rarer and it is done through hierarchical / official channels. Local border authorities sometimes do communicate with each other but unofficially, through conventional ways (e.g. telephone etc.). More important and critical needs arise in “Joint Operations” where there is an explicit requirement that the units in the field are able to communicate each other and, moreover, with the Coordination Centers (MSs / Frontex).

2.2.1.2 Technical aspects

Digital radio is governed by the same laws of physics and rules of propagation as is analogue, however, when reception is poor analogue fades gracefully but digital is either very good, or simply not there.

Analogue users tolerated very poor broken signals and this may influence their perception of coverage. For digital users there is essentially no choice what to tolerate: once a 4% bit error rate is exceeded reception stops. Consequently digital voice quality, when available at all, is excellent.

As with analogue the airwave digital signal will penetrate buildings and vehicles if there is sufficient external signal strength to make that happen. The use of different site locations leads to different propagation patterns. Finally the ‘good signal or no signal’ nature of digital radio needs to be understood by users.

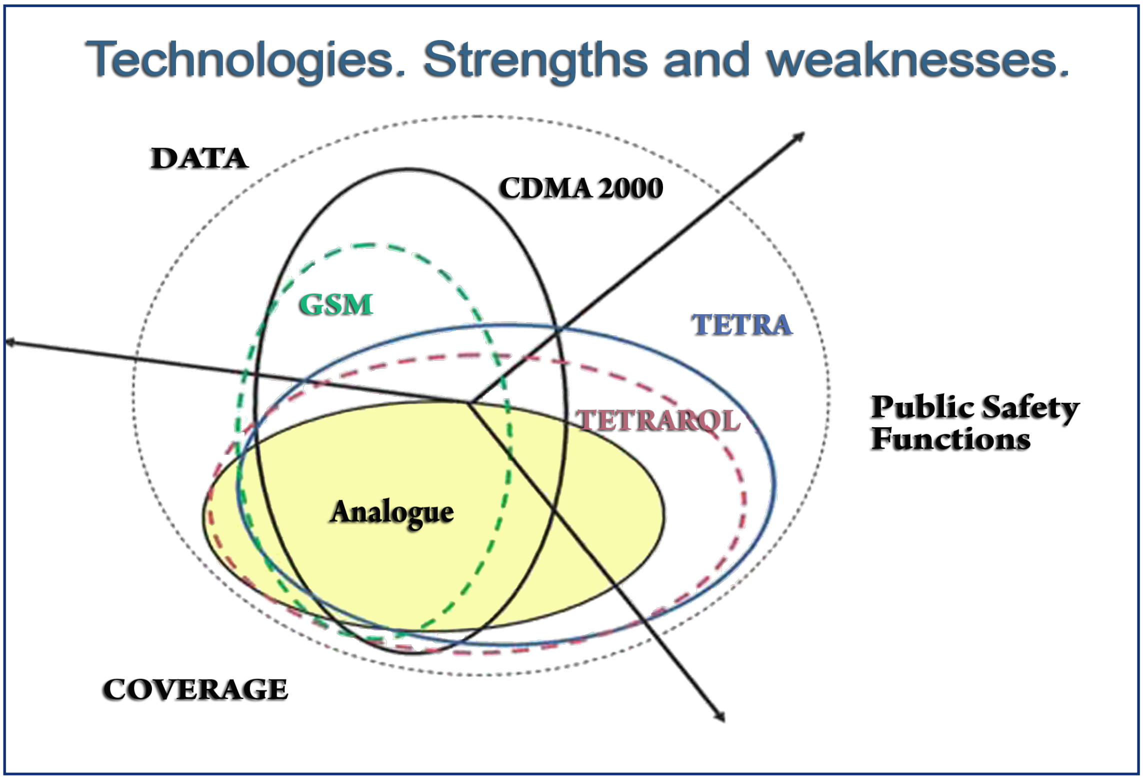
From a technical point of view there are the following issues:

- Limited air interface encryption.
- Authentication and encryption can only be done by exchanging very important keys.
- End-to-end encryption is a “question-mark”.
- Possible use of modems and leased lines are necessary “costs”.
- Multiple conversations from digital to analogue and back to digital reduce the audio quality.

In addition, attention should be given to configuration issues like radio configuration or network configuration and to the logistical challenge of the large scale application of the proposed solution.

The expectation is that the full Inter-System-Interface (ISI) answers to these questions and it will provide a structural maintainable and manageable European solution.

The following schema indicates advantages-disadvantages of each system in three parameters: coverage; functions; data.



2.2.1.3 “What’s up” on Research and Development

There are some ongoing pilot projects (The “three-country pilot project” for the ‘Cross Border Communication for Public Safety’, is a typical example regarding this topic, see also: www.3countrypilot.com) in existence in cross-border cooperation among several organizations in public security communications. In these projects it was proved that a communication flow model for cross-border communication was quite important.

Also, there was a review to what extent (with this technology) cross-border communication will be sufficiently supported in operational practice and whether improvements are still possible.

2.2.1.4 Communication Market

Though the technologies are often similar, the “Border Security Communication” market is quite different from the public telecommunications market; for a start, it is much smaller in number of users and economical investment.

Improvements are restricted by the level of annual public budget set aside for scheduled purchasing and maintenance in this field.

This also implies that the new system has to be compatible with the old (both in terms of technical interoperability and be able to be operated following the existing organizational procedures). Furthermore, the operational costs must not be more expensive than today.

An initial set of topics for discussion includes:

- → Identification of the key aspects that define the structures and technologies through which Border Security services are currently provided
- → Find or build an analytical (but not too complex) model based on these components, which can be used to calculate the costs for such systems
- → Discuss if the model needs to be updated to be usable for a Europe system
- → Comparison and discussion of the differences.

2.2.1.5 Maritime Scenario

A typical Maritime Joint Operation (JO) starts with its "Operation Plan". It describes its Objectives, Execution and Co-ordination.

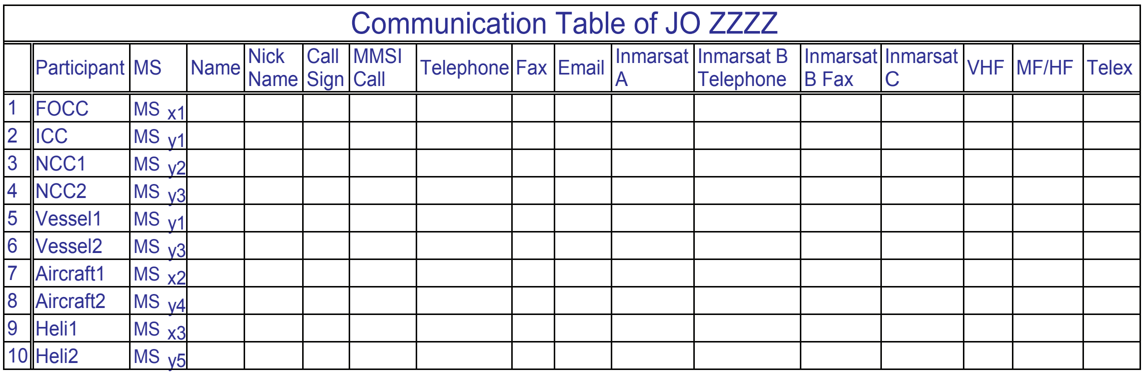
The Objectives are the "general objectives" of Frontex and the "main objectives" of the JO itself.

The Execution chapter of the plan defines issues such as: International Coordination Centers (ICC), tasks; Assets Employed; Area; Time; Course; Conduct of Operation.

Regarding ICC, some of the topics that are being defined in the plan are such as: the manning, the Director, the co-ordination board, the employed national officials, the command and control and finally the communications.

The Communications must be according to international and national regulations in force of the competent agencies of participating EU MS. These communications include exchange of e-mails, fax and telephone.

They are often defined in attached annexes having the shape of a matrix table, as following:



Communication Table of JO ZZZZ

	Participant	MS	Name	Nick Name	Call Sign	MMSI Call	Telephone	Fax	Email	Inmarsat A	Inmarsat B Telephone	Inmarsat B Fax	Inmarsat C	VHF	MF/HF	Telex
1	FOCC	MS x1														
2	ICC	MS y1														
3	NCC1	MS y2														
4	NCC2	MS y3														
5	Vessel1	MS y1														
6	Vessel2	MS y3														
7	Aircraft1	MS x2														
8	Aircraft2	MS y4														
9	Heli1	MS x3														
10	Heli2	MS y5														

Obviously, the communication means that the Units use in the field are of various technologies and capabilities. Having in mind that communications in an "Operation Plan" are essential for the success of a JO and more over the interoperability and security of those communications in the reality of a JO reflects in the effectiveness of assets and personnel.

2.2.1.6 Future Development / Future Situation

It is estimated that in the near future there will be a deployment of advanced broadband applications, related radio technologies and modern IP-based system architecture. Further more the interoperable IP capable networks will be developed nation-wide and European wide. Progress will be in the following areas:

→ Enablement of Trusted End-to-End IP based Network Security.

→ Enablement of IP based Network Management.

→ Common open standards construction protocol to support multiple wireless networks configuration and integration (e.g. Sensor, Link, and Internet).

→ Complex system would be less complex by modularity.

A future shared system for communication across geographic and organizational limits shall offer the following features:

→ Group and one-to-one communication.

→ Fast call set up.

→ Safety alarm call.

→ Recording + logging of calls.

→ Robust system that operates independent of other networks.

→ Autonomous area working

→ Direct communication terminal-terminal.

→ Encrypted system — not possible to listen in.

Also, one common "user terminal" will substitute many different terminals that are in use today (radio pager, mobile radio, GSM).

2.3 Broad view of the requirements

The user requirements for wireless interoperability in the border control domain can be divided into two main categories:

- requirements in normal daily operation;
- requirements in crisis situations.

These two main categories differ in several aspects. The requirements under normal daily operation are much less stringent than under a crisis situation, when the system that enables wireless interoperability will come under significantly more stress. This higher level of stress is due to the increased number of users, who will most likely be part of even more diverse teams than usual. This may be because teams are transferred from other regions to assist in the emergency operations. Thus a wider range of wireless standards will need to be accommodated.

Apart from these two very basic parameters (number of users, number of different wireless standards), the rest of the requirements are similar in both daily operation and crisis situations.

The number, capabilities and locations of dispatch/coordination centers need to be studied, planned and drill-tested in advance. The number of dispatch centers may depend on the number of different languages spoken by the end-users, by the different levels of security clearance in play, and/or by the scale of the operation. The capabilities depend more or less on the same factors as above. Their locations may depend on the map of existing telecommunications and other infrastructures, on the morphology of the terrain as well as other factors.

Another important requirement often overlooked is call setup time, both in point-to-point (unicast), point-to-multipoint (multicast) and broadcast scenarios. While call setup times of several seconds are tolerated by commercial users, sub-second call setup times are required, even critical for public safety users, including border control agents.

Scalability of the infrastructure that achieves interoperability is important, mainly in crisis situations, but also in normal daily operation, as borders expand or more agencies come into play in the border control domain.

The system needs to be flexible and easily adaptable. This will come in handy when one of the agencies in play decides to upgrade its communication systems, or when new user requirements come up and the infrastructure is asked to support them. The speed, ease and reliability with which parameters can be changed or new features introduced will make a difference in maintenance costs.

Reliability is of course a very important aspect that is easy to be defined, even measured, however it is not always as easy to be achieved, especially as systems become more and more complicated and we are moving steadily into a system-of-systems world. Hidden parameters come into play in such situations, and system behavior is not always deterministic, in the sense that small changes in input can make a major difference in results. The infrastructure needs to be designed to be fault-tolerant and accommodate components being replaced in real time, or nodes failing due to unpredicted reasons (by accident or sabotage). It is important that the system is designed to have no single point of failure, and redundancy needs to be kept in mind.

Intentional sabotage needs to be anticipated, both in the physical domain (e.g. material damage), in the support layer (e.g. power failures) or wireless layer (e.g. frequency jamming). These situations need to be reliably identified / isolated and different measures need to be taken in each of these cases.

System robustness is obviously crucial, since the system needs to be able to operate in extreme temperature/humidity/vibration conditions or with unreliable power and communications infrastructures.

The cost effectiveness of the system is not to be overlooked, since often these agencies have limited budget, both for purchasing and maintenance. Any solution should strive to limit the costs of production, operation and repair. Standardization and modularity is certain to aid in this goal.

Ease of use is another common user requirement, as the equipment often needs to be operated under difficult, unpredictable and often stressful conditions. Equipment/system usability is often in competition with system flexibility/complexity. The system should integrate some level of intelligence, freeing the operator from the maximum possible number of obvious decisions/actions.

The Communication System for Secure Border Communications should reflect the following broad requirement:

- Transparent and seamless wide-area network applications.
- Multiple levels of security and data encryption schemes.
- Robust operational management and control systems capabilities.

- Priority operational services and priority system restoration.
- Provision of an extremely reliable service model and ubiquitous coverage within a user's defined service area.
- Support for the transport and distribution of rate-intensive data, digital video, infrared video and digital voice for both service-specific and general applications.

2.3.1 General technology-requirements

Some of the primary required capabilities of the communication system may include, but are not limited to, the following:

- Full Duplex communication.
- Compatibility with legacy systems.
- Digital Data Communications.
- Broadband.
- Multiple levels of security.
- Multiple levels of availability of service.
- End-to-end network integrity.
- Security requirements.
- User Safety.
- System and network access.
- Economical and ergonomically friendly design.
- Incorporation of frequency neutrality and/or agility.
- Consistency with existing standards.
- Compatibility with multiple international standards.
- Spectrum efficiencies awareness.
- Compliance with the need of the participating Member States.

3. METHODOLOGY

The present pre-study has been based on a twofold approach; on one side we have examined the existing studies on communications for Public Safety organizations, focusing on the lessons learned in emergency situations; on the other side we have circulated a questionnaire aiming at finding out the present technological level of the communication equipment used by Border Police in the Member States.

The analysis of the literature is outlined in chapter 4; such an analysis was not meant to be exhaustive, but to present the pivotal importance of communications in Border Police operations based on the analogy with other type of operations in critical situation.

Similarly the survey of existing studies was intended to show that there is a great deal of background knowledge on the topic of secure communications, but further work is necessary to harmonize the outcome of existing studies and to focus on the specific needs of Border Police operations.

The response to the questionnaire has been quite satisfactory showing a significant interest in the Member States.

The results of the analysis of the data collected from the answers to the questionnaires are described in the chapter “Learning from Questionnaires”.

4. Data; Survey of Literature; Collected data

4.1 Learning from previous events

4.1.1 Introduction

In disaster or crisis situations, it is beneficial for law enforcement, rescue agencies and border security operators to have the ability to communicate and exchange information quickly and reliably. Since wired networks are not always available to security operators and maybe impractical, wireless networks are the ideal instruments.

The examples below point out to the fact that emergency wireless communications are of paramount importance in order to provide relief and save lives in national/international emergency and crisis situations.

However, it is also evident that problems arise whenever different operators from different contexts are called to cooperate in such emergencies.

The situation becomes even more complex when international partners from different countries are involved, since the lack of coordination and standardization among wireless communication system is more severe than at the national levels where in many cases there are plans and contingency measures to improve communications in such scenarios. The examples below describe clearly how the lack of secure and reliable communications can affect negatively the emergency relief operations, in national and international contexts, in Europe, US and in the rest of the world where European forces might be involved.

4.1.2 London bombings, July 7, 2005[2]

London bombings, July 7, 2005

- Rescue teams were unable to communicate properly between the sites of the explosions underground, colleagues at ground level and control rooms.
- The lack of a digital radio network meant that many senior managers among the main emergency services, and the London Ambulance Service in particular, were forced to rely on already-overloaded mobile phone networks to communicate in the aftermath of the explosions.
- Communications failures had a direct impact on rescue efforts, with requests for further ambulances, supplies and equipment by London Ambulance Service personnel at the scenes of incidents failing to get through to the main control room. They were also unable to receive instructions as to which hospitals were still receiving patients.

A report on the July 7, 2005, London bombings has said the lack of a digital radio network hampered the efforts of emergency service rescue teams.

[2] The information used in this paragraph has been obtained from: "Communication failures hampered London bombing rescues, article" appeared on CNET www.news.com By Andy McCue: http://www.news.com/Communication-failures-hampered-London-bombing-rescues/2100-7348_3-6079889.html as of 14-5-08

Noting that rescue teams were unable to communicate properly between the sites of the explosions underground, colleagues at ground level and control rooms, the London Assembly's July 7 Review Committee report[3] said it is "unacceptable" that the emergency services are still not able to communicate by radio when they are underground, 18 years after the official inquiry into a fire at King's Cross station recommended action to address the problem.

"It is essential that London's emergency services are equipped with digital radio equipment so that they no longer have to rely on mobile telephones to communicate between the scenes of major incidents and the control rooms," the London Assembly report concluded.

The scale of the mobile network overload is revealed in the report. Vodafone, for example, experienced a 250 percent increase in the volume of calls and a doubling of the volume of text messages. Across all networks on July 7, 11 million calls were connected--60 percent more than usual. This figure doesn't include unsuccessful calls.

Despite this network overload, the emergency services did not invoke the Access Overload Control (ACCOLC) system—apart from a 1 kilometer-square area around the Aldgate incident—which allows mobile network access only to the police, fire and ambulance personnel.

One of the reasons ACCOLC was not activated was that key emergency services personnel who were not carrying specially enabled telephones would not have been able to make or receive any calls.

"This is clearly a major flaw in the system: There is no point in having the technology to enable key people to communicate with each other if the relevant authorities do not make sure that the right people are in possession of that technology," the London Assembly report said.

The report also criticized London Underground's "antiquated" radio systems after they failed to work on any of the three affected tube trains on July 7, preventing direct communication from the trains to either the emergency services or Transport for London's control center.

4.1.3 World Trade Center Attack[4,5,6]

World Trade Center Attack, New YorkS City, September 11, 2001

- As live images of the unfolding events of September 11, 2001 were broadcast on television, many police officers, firefighters, and emergency medical personnel who were called to duty in New York City could not use their wireless systems to communicate with one another.
- After the south tower collapsed, police helicopters relayed a message for public safety officials to evacuate the north tower

[3] "Report of the 7 July Review Committee, Greater London Authority, June 2006"

[4] The information used in this paragraph have been obtained from: "The lessons of non-interoperability in public safety communications systems", Donald A. Lund April 2002, the ATLAS project, Advanced technology in law and society, University of New Hampshire USA

[5] Steve Worrall (2005). An International Study of Radio Interoperability, steve.worrall@shropshirefire.gov.uk

[6] Protecting Public Safety With Better Communications Systems" Jon M. Peha Carnegie Mellon University IEEE Communications, March 2005

- Firefighters never received the police warning because their radio system did not interoperate with the police communication system.

The worst failure occurred in the World Trade Center's North Tower. At 9:59AM on September 11, 2001, the first of several announcements was transmitted to emergency responders ordering them to evacuate the North Tower. Police inside the building heard the order on their radios, and most left safely. However, firefighters were using incompatible communications equipment that could not receive the order. People watching television at home knew that the unimaginable had already occurred - that the World Trade Center's South Tower had collapsed - but many firefighters inside the North Tower would never learn of this. When the North tower fell 29 minutes after that first evacuation order, 121 firefighters were still inside. None survived. At the same time, two hundred miles away, more communications failures were making it harder to contain fires at the Pentagon, where another plane had crashed. These failures put more lives at risk.

In his New Jersey volunteer fire station, Glenn Corbett watched his colleagues desperately try to send emergency messages to the medical and fire personnel mounting rescue operations inside the Twin Towers.

"It was such a tragedy to see the battalion chief of the first battalion and the first fire chief on the scene of the Trade Center trying to communicate with other officers up in the building and we saw on national television, where there was no answer. He kept calling and calling and there was no answer," he said.

Corbett, like many others, lost friends that day, Chief Raymond Downey and firefighter Andrew Fredericks. In all, the New York Fire Department suffered tremendous losses on September 11, with 343 firefighters killed.

The Incident Command Post was located across from the South Tower, so when it collapsed the post was destroyed. This made it even harder to communicate and coordinate with rescue teams inside the towers. Mobile radios did not work properly even after rescue workers tried to use repeaters to boost signals.

Congested and fragmented spectral resources, inadequate funding for technology upgrades, and a wide variety of institutional obstacles compromised the ability of public safety officials to protect life and property. The press attributed much loss of life among NYC firefighters to the malfunction of handheld radios in the Twin Towers.

4.1.4 South Asian Tsunami 2004[7]

South Asian Tsunami 2004

- Controversy about Alert System
- Difficulty to reach remote regions in order to find out about the situation there
- Lack of coordination and communication among national/international aid/relief teams, in particular European teams.

The Indian Ocean tsunami of 26 December 2004 caused devastation on an almost unprecedented

[7] The information used in this paragraph have been obtained from: "Mobile Information and Communication Systems in Crisis Situations" Presentation by EPFL (MICS) Jacques Panchard: jacques.panchard@epfl.ch http://www.terminodes.org and IISc HS Jamadagni: hsjam@cedt.iisc.ernet.in http://www.iisc.ernet.in

scale, killing an estimated 200,000 people and leaving hundreds of thousands more homeless and in urgent need of water, shelter and medical treatment throughout south-east Asia and as far away as east Africa.

Following the experience of the tsunami, civil society gave a clear signal that it wished to see a stronger and more effective European response to disasters. A number of initiatives have been taken to address limitations in the system. In April 2005, the Commission issued a Proposal for a Council Regulation establishing a Rapid Response and Preparedness Instrument for major emergencies, to fund actions contributing to preparedness and response in case of disaster, as well as a Communication on Improving the Community Civil Protection Mechanism. This was followed in January 2006 by a Proposal for the Council Decision establishing a Community civil protection mechanism (recast); subsequently enacted through the Council Decision of 8 November 2007 [2007/779/EC,Euratom] establishing a Community Civil Protection Mechanism.

Quoting an excerpt for the proposal for council regulations:

“To that effect, the proposals build sup on the existing instruments while widening and setting out in more detail the actions eligible for funding. The range of actions that could potentially be financed under the proposal, in terms of preparedness and rapid response, is wide since the Instrument to be established could finance actions ranging from capacity building assistance, demonstration projects, awareness and dissemination actions to training and exercises, dispatching and sending out of experts and mobilization on short notice of adequate means and equipment. **Particular attention has also been given to identify logistical support actions, such as secure communication systems and tools, which are necessary for the proper achievement of rapid response interventions.”**

4.1.5 Germany Flood (2002)[8]

Germany Flood (2002)

- More than 100,000 phone links were out of order.
- Mobile network was overwhelmed.
- Numerous problems with emergency services.

Heavy rains on 07-08 August 2002 caused severe flooding along the Moldau and Elbe Rivers, affecting the Czech Republic and Southeastern Germany.

Heavy rains in the Alps earlier that summer also contributed to the flooding.

Water levels peaked at 7.5 meters (m) and 9.4 m above average for the Moldau and Elbe Rivers, respectively.

The resulting floods devastated villages, towns, large areas of arable land, streets, roads, and industrial areas. Thousands of people were forced to leave their homes, and several hospitals were evacuated. The flooding strained the entire community, both during the emergency and in the long-term.

However, panic and chaos did not constitute a major problem.

[8] The information used in this paragraph have been obtained from: KAMEDO Report No. 88:“Floods in the Czech Republic and Southeastern Germany, 2002” Ulla Näsman; Birgit Zetterberg-Randén; Helge Brändström (ed), KAMEDO = Swedish Disaster Medicine Study Organization

A total of 48,000 inhabitants of the Czech capital of Prague were evacuated;

About 25,000 of them were elderly. Two urban districts in Prague were evacuated completely, mostly by bus. Evacuation centers were established in schools, student hostels, and military camps. Ten percent of those forced to leave their homes (about 5,000 people) took advantage of this opportunity.

The evacuation was so extensive that it was impossible to check if every house actually had been evacuated. It was up to individuals to decide whether or not to leave their homes.

16.08.2002: The Interior Ministry of the German Federal State of Saxony is calling upon people to reduce their mobile phone calls “to a minimum” in those areas affected by the flooding so as to keep the mobile network open for the emergency services. More than 100,000 terrestrial-based phone links in the state of Saxony are still out of order, a fact that is adding to the strain upon the mobile network.

4.1.6 Conclusion

In the quoted complex emergency/crisis scenarios a number of different first responders from different organizations are usually involved.

Each organization, in turn is autonomous and independent from the others and in this respect usually adopts a wireless emergency communication technology based on its own internal requirements.

The communications needs become more complicated and multifaceted in the scenarios considered, due to the requirements for coordination among diverse parties.

Coordination in turn is also a very multifaceted issue that involves many technical and non technical aspects. However there are some pre conditions or enablers that must be satisfied in order for this process to take place.

The examples presented clearly point out a fundamental pre-requisite that is absolutely necessary for effectively exchanging information among diverse partners on the field.

Interoperability of field-based radios together with connectivity with public networks (PSTN, cellular, IP/internet) is the most critical enabling factor that was not in place in the scenarios described by the example. It is important to notice that interoperability alone would not be sufficient for efficient coordination but it is a fundamental enabling factor in this case.

These examples point out that the effort to standardize a common wireless emergency communication system can be considered as a first essential step for inter-force coordination in crisis situations.

The difficulties involved in identifying a common standard can be overcome by the recent development of highly reconfigurable field radios. These radios have already found successful applications in the military field and the adoption of similar technology in the field of border security could represent an important step forward for bringing commercial success and hence reduction of costs to this promising technology.

4.2 Learning from previous studies

4.2.1 SAFECOM[9]

SAFECOM is a communications program of the Department of Homeland Security. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies.

As an emergency responder-driven program, SAFECOM is working with existing Federal communications initiatives and key emergency response stakeholders to address the need to develop better technologies and processes for the multi-jurisdictional and cross-disciplinary coordination of existing systems and future networks.

SAFECOM harnesses diverse Federal resources in service of the emergency response community.

SAFECOM, through its website provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs.

SAFECOM activity has clearly identified and progressed to meet the following needs:

- A nationwide coordination for:
  - funding,
  - technical assistance,
  - standards development, and
  - regulations affecting communications and interoperability;
- a commonly agreed requirements for interoperability issues, SAFECOM published the “Statement of Requirements which, for the first time, defines what it will take to achieve full interoperability and provides industry requirements against which to map their product capabilities;
- the development of a national interoperability baseline;
- the development of critical standards for interoperability;
- the management of spectrum and regulatory issues;
- the creation of a model methodology for developing statewide communications plans.

SAFECOM has greatly helped in clarifying the needs of the Public Safety Community in terms of communication interoperability.[10]

The Interoperability Continuum is a framework that graphically depicts the five critical elements of interoperability success - governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications.

These critical elements must be addressed to develop robust interoperability solutions.

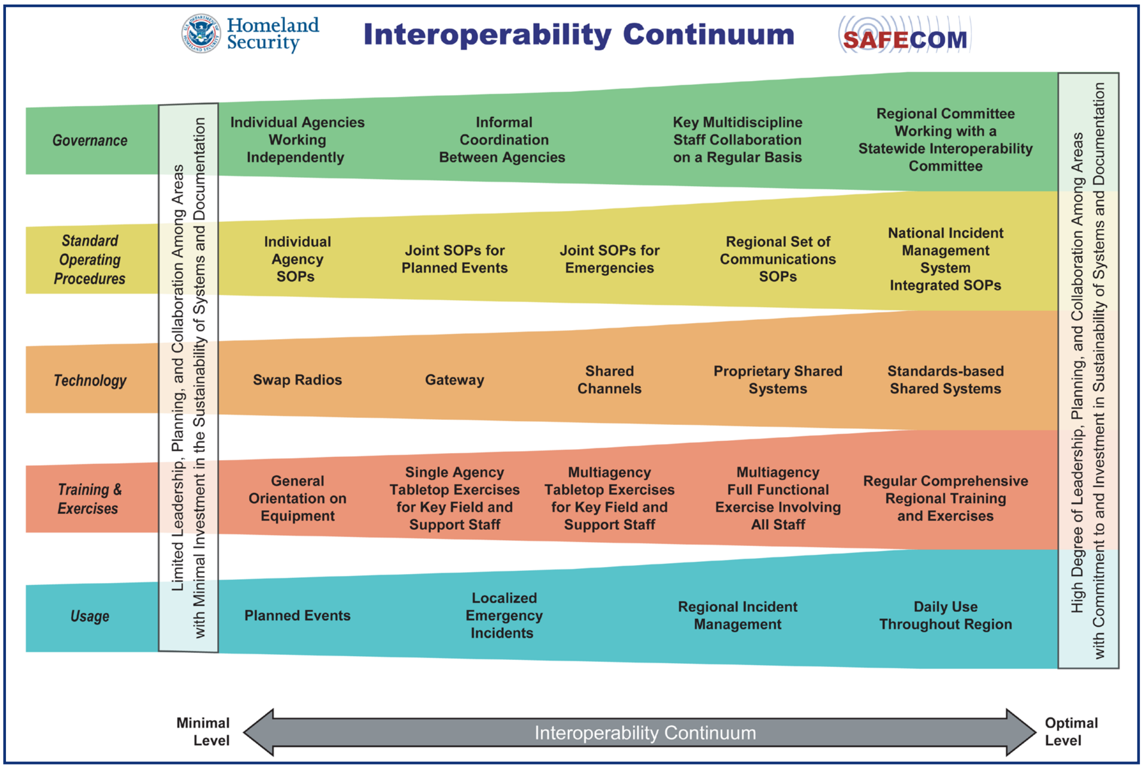
[9] All the information contained in this paragraph are extracted from the SAFECOMM website: http://www.safecomprogram.gov/SAFECOM

[10] Wireless Technologies and the SAFECOM SoR for Public Safety Communications; Leonard E. Miller - 2005

This framework is to encourage a shift from a technology-centric focus to a comprehensive operational focus on the key interoperability success factors.

The Interoperability Continuum is a tool that can be used to assess the current level of interoperability and to determine what elements need further development.

Making progress in all aspects of interoperability is essential, since the elements are interdependent. Therefore, to gain a true picture of a region's interoperability, progress along all five elements of the continuum must be considered together. For example, when a region procures new equipment, that region should plan training and conduct exercises to learn how to make the best use of that equipment.


Homeland Security
Interoperability Continuum
SAFECOM
Governance
Individual Agencies Working Independently
Informal Coordination Between Agencies
Key Multidiscipline Staff Collaboration on a Regular Basis
Regional Committee Working with a Statewide Interoperability Committee
Standard Operating Procedures
Individual Agency SOPs
Joint SOPs for Planned Events
Joint SOPs for Emergencies
Regional Set of Communications SOPs
National Incident Management System Integrated SOPs
Technology
Swap Radios
Gateway
Shared Channels
Proprietary Shared Systems
Standards-based Shared Systems
Training & Exercises
General Orientation on Equipment
Single Agency Tabletop Exercises for Key Field and Support Staff
Multiagency Tabletop Exercises for Key Field and Support Staff
Multiagency Full Functional Exercise Involving All Staff
Regular Comprehensive Regional Training and Exercises
Usage
Planned Events
Localized Emergency Incidents
Regional Incident Management
Daily Use Throughout Region
Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation
High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation
Minimal Level
Interoperability Continuum
Optimal Level

4.2.2 Project MESA[11]

The Public Safety Partnership Project (PSPP), known as Project MESA (Mobility for Emergency and Safety Applications) was established between the Telecommunications Industry Association (TIA) of the United States and the European Telecommunications Standards Institute (ETSI).
The mission of the Project is to meet the emerging communications needs of Professionals in the area of Public Safety; such needs can be summarized as follow:

> **The next-generation public safety communications shall provide for broadband data access, interoperability, increased security, technical interoperability, user transparency and communications over myriad technological platforms and applications.**

[11] All the information contained in this paragraph are extracted from the MESA Project website: http://www.projectmesa.org

TIA and ETSI agreed to collaborate and combine work efforts to provide a cooperative forum in which key stakeholders (e.g., agencies, users and industry) can contribute to the elaboration of next-generation digital broadband data capabilities, initially focusing on public safety and emergency response agencies, organizations and professional users.

MESA was the first international communications standardization partnership project whose aim is to identify, coordinate and develop common mobile broadband data communications capabilities and specifications, based on continued input from the public safety and emergency response community, industry and research entities.

The development of future technologies will be driven by common scenarios, technical specifications, existing standards and spectrum allocations.

4.2.2.1 Statement of Requirements (SoR)

The initial Project MESA Statement of Requirements (SoR) was developed within the Service Specification Group of MESA and approved by the Project MESA Steering Committee in 2002.

> ***It represents the first consolidated transatlantic vision to be expressed by critical public service users of advanced wireless data communications equipment and systems.***

Capabilities, involving either an ad hoc or day-to-day operational environment, include:

- Wireless mission-critical broadband data
- Secure and interoperable capabilities
- Multiple users with multiple applications
- Self-establishing and -healing network nodes
- IP-based mobile networking
- Robust management and control systems
- Flexible existing infrastructure dependence
- Dynamic and flexible radio configuration
- Real-time digital voice, video and sensing
- Still photos, complex graphics and drawings files
- Enhanced bio-telemetry information
- Maintain integrity/security of national networks

4.2.2.2 MESA Technical Specifications

Based on the SoR, the MESA Technical Specification Group is now mapping existing capabilities and gaps, progressing toward the development of corresponding technical specifications.

A "System of Systems" approach is being utilized, leveraging current and evolving communications technology and user requirements. MESA output will be transposed by supporting standards development organizations (i.e., TIA, ETSI, etc.) for regional development and publication.

4.2.2.3 A Growing Market

The global demand for advanced communications tools and applications is growing significantly.

This broadband capability standardization process, involving current and next-generation technology, will lead to a defined multi-vendor global marketplace for MESA-capable products and services, benefiting from production volumes and reduced procurement costs for users and their organizations.

Project MESA is well on the way to developing coordinated technical specifications supporting the deployment of next-generation mobile broadband digital communications capabilities for public safety and emergency response applications.

Project MESA capabilities and resulting regional standards will be utilized in government-owned systems, government/ private sector partnerships or other appropriate uses, helping to grow the market, thus giving first responders the capabilities they need to serve and protect citizens from a local to an international level.

4.2.2.4 Communications on the Move

Recent wide-scale emergencies have made it clear that public safety and disaster response agencies need effective, high quality and reliable broadband communications services. Currently, voice communication is transmitted over narrow-band radios without benefit of advanced capabilities.

MESA-capable technology would allow first responders and command units not only digital voice communications but also utilization of streaming video feeds (e.g., visible/infrared) and real-time data, including vital statistics, remote sensors, incident records and other information.

For example, consider large-scale emergencies where fire trucks, ambulances, police vehicles and surveillance helicopters are en route to the scene.

Electrical power is shut off in the area and worried citizens overload cell and wired phone systems.

With standardized wireless voice interoperability and MESA-capable equipment on board, all responding agencies/units will automatically establish full voice interoperability and a high-speed wireless network as they approach each other. Incident planning can start before arrival at the scene.

Command units also are equipped with MESA-capable master nodes, including a satellite communications link for high-speed data back-haul on the way to and at the scene. The result is enhanced communications and response.

> ***MESA will bring national, local and cross-border interoperability for coordinating responses to disasters and crises.***

4.2.2.5 The Moving Hot-Spot

Densely populated urban areas and critical infrastructure areas will clearly be an avenue for the deployment of next generation capabilities.

However, disaster can strike anywhere, so an important aspect of MESA-capable technology is its trans-jurisdictional mobility and rapid deployment as a totally independent yet interoperable service network.

The term "moving hot-spot" illustrates the unique network topology potential of MESA capabilities and its ability to support an effective ad hoc emergency response characterized by disrupted or non-existent public infrastructure and electrical supply.

4.2.3 Public Safety Communication Europe[12]

"Forum for Public Safety Communication Europe" has been established in order to facilitate consensus building in the area of public safety communication and information management systems.

The Forum invites users and policy makers, industrials (technology and service providers), research organizations and standard making authorities to reach consensus on:

- Consolidated user requirements,
- Solutions for inter-operability of communication systems among users;
- A R&D road map for future activities.

Guidelines for policy makers and regulators, indicating ways for the improvement of Global, European or National inter-operability through implementation of harmonized technologies and/or approximation of legal environments.

The Forum's conclusions and recommendations will be put together in Memoranda of Understanding to be submitted to relevant authorities and representative bodies.

The Forum was launched on 1st June 2006 for an initial duration of 3 years.

4.2.3.1 The Problem

Recent events in Europe and other parts of the world have again demonstrated that effective response to emergencies, crises and disasters depends on timely available, reliable and intelligible information.

Advanced information and communications technologies (ICT's) offer an increasing number of valuable, however divergent, tools for emergency response, crisis management, and disaster preparedness and response.

The speed with which ICT's emerge, leads to different levels of implementation.

Successful application of ICT's by the increasing number of national and international stakeholders confronted with cross-border incidents depends on better integration of frameworks for action.

[12] All the information contained in this paragraph are extracted from the Public Safety Communication Europe website: http://www.psc-europe.eu/

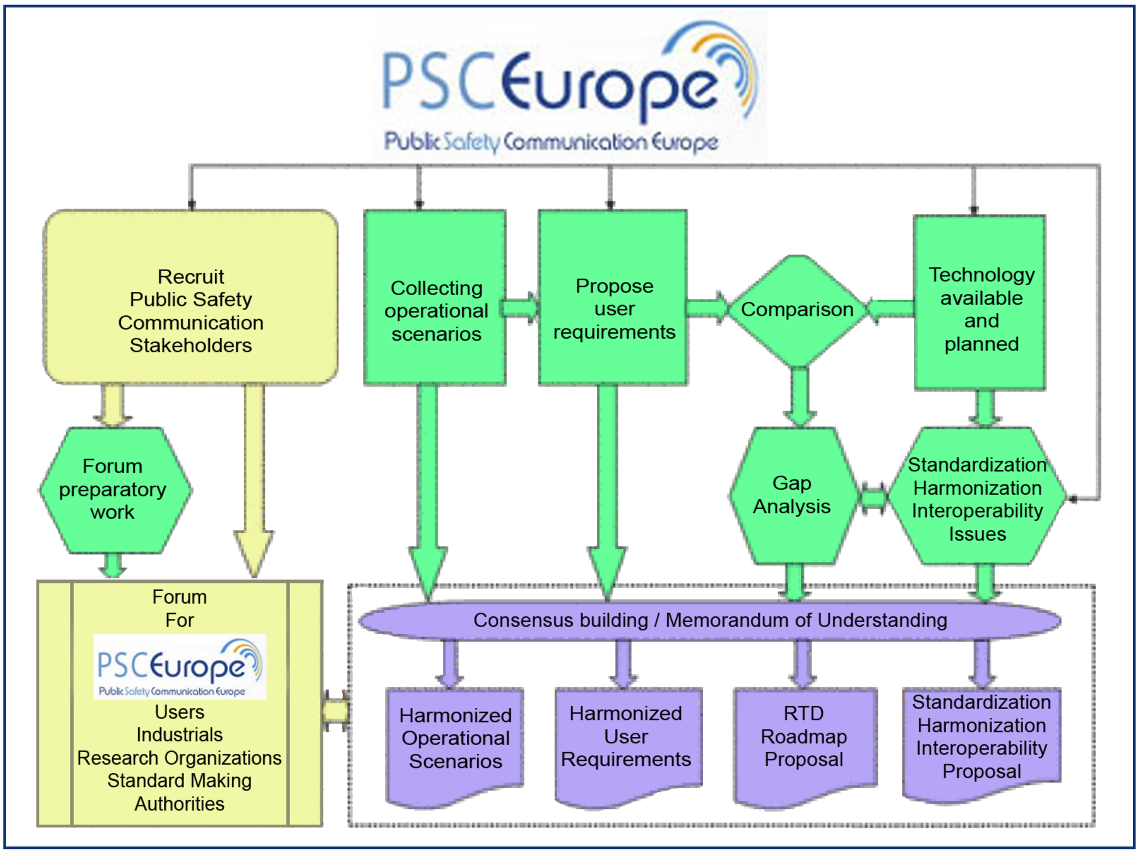
4.2.3.2 Purpose of the project PSC Europe

Stakeholders involved in these problems, namely:

- users providing emergency and disaster response,
- industry providing equipment and services,
- researchers developing new ideas and concepts,
- organizations defining standards for cooperation frameworks, will be brought together.

Convergence, at international level, of requirements formulated by each of them, is an essential goal of the project in order to lay the ground for possible solutions.

The project PSC Europe focuses on establishing and maintaining a Forum for regular exchange of ideas, information, experiences and best practices, and on seeking agreement among participating stakeholders.


PSC Europe
Public Safety Communication Europe
Recruit Public Safety Communication Stakeholders
Collecting operational scenarios
Propose user requirements
Comparison
Technology available and planned
Forum preparatory work
Gap Analysis
Standardization Harmonization Interoperability Issues
Forum For PSC Europe Users Industrials Research Organizations Standard Making Authorities
Consensus building / Memorandum of Understanding
Harmonized Operational Scenarios
Harmonized User Requirements
RTD Roadmap Proposal
Standardization Harmonization Interoperability Proposal

4.2.3.3 Expected results

The conclusions and recommendations emerging from the Forum are expected to:

- lead to convergence on user requirements,
- propose solutions for inter-operability of communication systems among users,
- supply an overview of available technologies and assess how they match user requirements,
- establish a R&D road map for future activities, hence ensuring European leadership in ICT,

- present guidelines for policy makers and regulators, indicating ways for the improvement of global, European or national inter-operability through implementation of harmonized technologies and/or approximation of legal environments.

These conclusions and recommendations will be put together in Memoranda of Understanding to be submitted to relevant authorities and representative bodies.

4.2.4 Conclusions

The previous chapters highlighted the fact that Public Safety Agencies need to have flexible, secure, reliable, broadband Communications.

It is also clear that a great deal of effort has been made to produce a common set of requirements that will help the industry to design and produce communication systems capable of meeting the needs of the Public Safety community.

On the other hand, the effort of generating a common set of requirements has been, partly, hampered by competing interests and greatly dissimilar "environmental" conditions, i.e. the "landscape" of communications in the U.S. is significantly different from the E.U. one.

Moreover a number of different concurrent Projects started with the same purpose and, although they generated quite similar outputs, there are still a quite large number of different documents on requirements.

Furthermore, the drive for generality has produced requirements that could easily lead to the design of expensive systems that may not be affordable by many organizations.

It is therefore necessary to produce specific requirements that match the need of the Border Police, leveraging on the results of existing studies.

4.3 Technology Survey

As mentioned earlier, Border Guard Authorities are currently using a number of diverse and competing technologies. It is necessary to study the current and emerging technologies that have the potential to facilitate interoperability among border control agencies.

Four different (but complimentary) approaches are put forward as possible solutions to the interoperability problem:

1. Reconfigurable (possibly SDR) Bridge Base stations
2. Reconfigurable (possibly SDR) Terminals
3. A Core Network Layer
4. A common Wireless Standard (e.g. TETRA, TETRAPOL or APCO-25)

4.3.1 Reconfigurable Bridge Base stations

The first approach calls for base stations that act as bridges between wireless standards. These base stations might be fixed (dispersed along the border) or portable (deployed in crisis situations as needed). They would need to be reconfigurable, in order to accommodate the different standards and requirements in different scenarios. This re-configurability might be achieved through the Software Defined Radio architecture, but other solutions might come up in the future, so it would be prudent to keep open the possibility of incorporating such features.

This solution requires significant effort before deployment, as all possible wireless standards need to be implemented, tested and certified as waveforms in the reconfigurable base stations. These waveforms would need to be tested for interoperability with legacy radios of the same standard. In addition to that, a way to interconnect two or more waveforms would need to be devised. This interconnection mechanism would then need to be tested for enough combinations of waveforms. Moreover, concurrent operation of several waveforms in real-time would need to be tested, as well as the system's ability to load/unload a waveform without disturbing the operation of other running waveforms. Finally, staff would need to be hired, trained in the use of these base stations and be placed on round-the-clock availability.

On the other hand, this approach has significant advantages compared to the other three. The cost of developing and deploying this solution is expected to be lower than, for example, replacing all terminals with new ones, especially if training is included. Furthermore, this solution is more centralized, and thus easier to manage, maintain and upgrade. This solution is also highly flexible, in the sense that it is easy to upgrade the base stations (increase performance) and add more waveforms or features. This would lower long-term maintenance costs and would make it easier to satisfy extra requirements that might come up in the future.

4.3.2 Reconfigurable Terminals

The second approach calls for reconfigurable terminals. These terminals would be assigned to key agents deployed in the field, who would be trained to use them and act as gateway nodes between different teams. The terminals would again be reconfigured according to the conditions at hand and the choice of teams that need to intercommunicate and be coordinated. As with the first approach, this terminal re-configurability could be achieved through the Software Defined Radio architecture, but other technologies for reconfigurable radios might emerge in the future, so again it would be wise not to predefine the technologies used to achieve re-configurability.

This approach is more decentralized than the first one (reconfigurable bridge base stations). This fact reduces the complexity (both technological and procedural) and -as a result- procurement and maintenance costs. The re-configurability makes this approach also very flexible, however less than the reconfigurable base stations approach, mainly due to limitations in size, weight and power. New waveforms can easily be added as needed and upgrades are easier than in other cases.

An important disadvantage of this approach is the need to train the selected agents in the use and procedures related to the terminals. This increases the deployment cost and adds reliance on specialized personnel who can operate this equipment. Furthermore, it includes the same effort before deployment

4.3.3 Core Network Layer

In the third approach, a core network layer connects the base stations of the different border

control agencies and thus achieves interoperability in a centralized way. Several current technologies follow the core network layer paradigm:
Spain uses a network called SIRDEE (Sistema Integral de Radiodifusión Encriptada del Estado), which based on TETRAPOL technology
In the USA, ISSI (Inter RF Subsystem Interface) is part of the Project 25 (P25) or APCO-25 suite of standards
SCIP (Secure Communications Interoperability Protocol) was designed by the US DoD (Department of Defense) in cooperation with the NSA (National Security Agency)

- CISCO has developed IPICS (IP Interoperability and Communications System) for emergency first responders
- Ericsson has developed the CoordCom Public Safety Communication Center
- Artevea has developed for NATO a system called T-MATRIX P, which stands for Transportable TETRA over IP
- The 3GPP standards body has designed IMS (IP Multimedia System), which uses SIP for call establishment and IPv6.

Some advantages of the Core Network Layer approach are: a) it does not call for the replacement of current infrastructures, neither for terminals nor base stations, b) it does not require field agents to be trained on new technologies, and c) it is a centralized technology, which makes it easier to manage and upgrade. It is also probably the cheapest of all four approaches in terms of deployment and maintenance.

On the other hand, it bears a significant disadvantage: it does not enable interoperability among different radio standards in the same area, if the infrastructure (base stations) does not already exist. Instead it only enables interoperability between the existing, currently isolated infrastructures.

4.3.4 Common Wireless Standard

The fourth approach calls for a common wireless standard to solve the interoperability problem. In this scenario, user requirements from all the end-users are accumulated. An existing wireless standard satisfying all of them is chosen; otherwise a new wireless standard is developed. This new standard then replaces all the existing radios in the fragmented border security landscape. Of course, this approach would induce the highest cost of all other approaches. Furthermore, it would require agreement of all agencies on a common standard, something rather difficult, if not impossible.

Another drawback in this approach is user training. Replacement of all user terminals means that all users need to be trained on the usage of the new terminals. This could be problematic for different reasons: a) people generally dislike change, so one might face resistance from the end users to adopting the new standard, b) border control agents need to be able to use their terminals instantly and intuitively, without stopping to read a manual or ask for guidance, and c) a common standard satisfying user requirements from different agencies would mean that the average user does not need many of the features in the new handset.

On the other hand, new wireless standards are usually more technologically advanced, so by replacing an old standard with a new one, end users would profit from the advantages of a better standard. Some of the improvements common in newer standards are: a) better spectrum usage, in the sense of higher bitrates' using the same bandwidth, b) better encryption standards, and generally security mechanisms (immunity to interferences, authentication mechanisms etc), c) new terminals that use modern hardware modules lower the cost of the replacement parts inventory compared to legacy platforms.

4.3.5 Combinations of approaches

Since each of the four approaches has its strengths and weaknesses, no one approach can resolve all the issues and satisfy all the users' requirements. It is thus natural to examine the advantages and drawbacks of each approach and then design scenarios combining two or more of them in order to provide a technically feasible and financially viable solution. For example, a combination of SDR base stations interconnected with a Core Network Layer would combine the benefits of local area interoperability without the replacement of terminals (through the SDR base stations) in combination with wider-area interoperability through the Core Network Layer. Alternatively, a combination of reconfigurable terminals with a new wireless standard would allow key field agents from different agencies to communicate to each other (through the new wireless standard) while at the same time communicating with the rest of their team through the same terminal (as the terminal would be reconfigurable).

5. Analysis of Data

5.1 General

In general, the EU must provide high and equal level of border security on its external borders. But, do we know how to measure a security level on border? Do we have sufficient – and sufficiently accurate, accessible and well-organized – data related to border security? The system that maintains border security is extremely important for MSs, expensive, and can be seen from various perspectives. In this paper we are focused on the perspective of wireless communication networks used at the EU borders.

On one hand the border wireless networks have to be interoperable, and on the other hand they have to be secure. Thus, the SeBoCom pre-study is aimed at an interoperability and security of the border wireless communication networks. Where the interoperability is the ability of a communication system to work with other systems without special effort, and security is focused on the threats related to the wireless networks.

The part of this pre-study is wireless border communication survey based on questionnaires (see Annex 1) which were sent to each MS in December 2007. The survey is aimed at the functional and technical aspects of wireless border communication networks at the EU border. Eighteen MSs return completed questionnaires:

- Austria,
- Bulgaria,
- Cyprus,
- Dutch,
- Estonia,
- Finland,
- France,
- Greece,
- Latvia,
- Lithuania,
- Luxembourg,
- Poland,
- Portugal,
- Romania,
- Slovakia,
- Slovenia,
- Spain, and
- United Kingdom.

In the first two sections of the next chapter can be seen functional and technical aspects of the wireless border communication networks based on these questionnaires. The last section provides some conclusions and the directions for further work.

5.2 The functionality of wireless border communication networks

5.2.1 The border security forces

The results of the questionnaires show that various border security forces in MSs are responsible for border security, such as border police, border guard, coast guard, military police, custom office, border and immigration agency, aliens and borders service, maritime police, and airport police. In various states, these agencies have different official names, mission, jurisdiction, organizational structure, and human resources. For example, the survey shows that the number of employee in these agencies varies from 40 to more than 16000.

On the other hand, the border security forces need to cooperate with other organizations. The survey shows that the same wireless communication networks are used by border security forces and other organizations such as rescue centers, ministries of the interior, fire brigades, intelligent services, ambulance, ministries of finance, special police forces, and so on. Considering that border security systems are composed of many different organizations, which need to be closely related, providing the interoperable and secure wireless network is important and not always an easy task.

5.2.2 Information relayed through the national wireless border communication networks

Different MSs relay different types of information in wireless border communication networks. The analysis of questionnaires returned by MSs shows that most often are exchanged voice, operational data (status, messages, vehicle registration, criminal records or data files), geo-position data, video data, and data from surveillance sensors. In order to get a better picture about the relayed information types, the MSs are classified in groups in accordance with these information types in Table 1, which shows that the seven national wireless border networks support exchange of voice, operational data, and geo-position data.

Information	MSs
Voice Operational data Video Geo-position data Surveillance sensors	3
Voice Operational data Geo-position data Surveillance sensors	5
Voice Operational data Geo-position data	7
Voice Operational data Surveillance sensors	2
Voice Geo-position data	1

Table 1. MSs classified in accordance with information types relayed through the networks.

5.2.3 Surveillance sensors connected to the wireless border communication networks

The wireless border communication networks are mainly used for voice communications. Considering that wireless border communication networks can be extremely costly, the owners and users try to find alternative uses for them. Thus, various surveillance sensors can be connected to these wireless networks.

With Professional Mobile Radio (PMR) users can get a single interface to all alarms, regardless of where they came from. In this case all alarms are piped into PMR related alarm control system, logged, inspected and dispatched via PMR terminal to the on-call staff most appropriate to deal with the problem in question[13].

The returned questionnaires show that the five national wireless border networks include surveillance cameras, and motion detectors; two MSs declare that their networks include ground sensors; and two MS networks include radars. The graph on Fig. 1 shows the number of MSs that include certain sensors in the wireless networks.

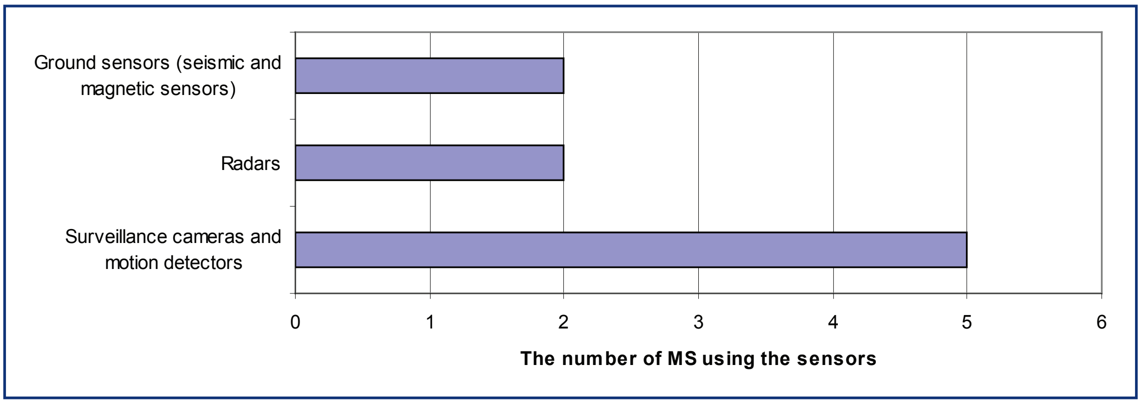


Fig. 1. Various sensors connected to the wireless border communication networks.

5.2.4 The services used in wireless border communication networks

In general, a wireless communication technology provides different services, such as:

- **Group call** that allows subscribers to communicate to multiple other subscribers at the same time.
- **Audio conferencing** providing two-way voice calls between users and a predetermined group.
- **Broadcast call service** that provides one-way voice calls from an originating user to one or more other users. The target user group may be a subset of all of the system users or it may be all of the system users.
- **Emergency call** button that sets up a high-priority call to a dispatcher or a predefined group of users.
- **Direct mode** that allows communication between two or more mobile stations, without involving a base station (walkie-talkie).

[13] ZONIT, TETRA Alarm Control System, http://www.zonith.com/products/tetra/, April, 2008.

- **Push to talk** (PTT) that provides direct voice communication connected with the push of a key. PTT is used to have a conversation with one person or with a group of people.
- **Global Positioning System** (GPS) that provides location of wireless terminal with GPS detector.
- **Fast call set-up** that is, a fast way to establish a connection. Time when call is set-up, typical for TETRA is less than 250 ms for a single node call, compared with the the many seconds that are required for a GSM network.
- Ambience Listening that allows a dispatcher to place a radio terminal into Ambience Listening mode without any indication being provided to the radio terminal user, which allows the dispatcher to listen to background noises and conversations within range of the radio terminal's microphone. This is an important service to utilize for persons transporting important, valuable and/or sensitive material that could be 'hijack' targets[14].

The analysis of the questionnaires show the services mainly used in the wireless border networks of MSs (Fig. 2). The graph on Fig 2 shows that the group call, PTT, emergency call, direct mode, and GPS location are the most often used wireless network services.

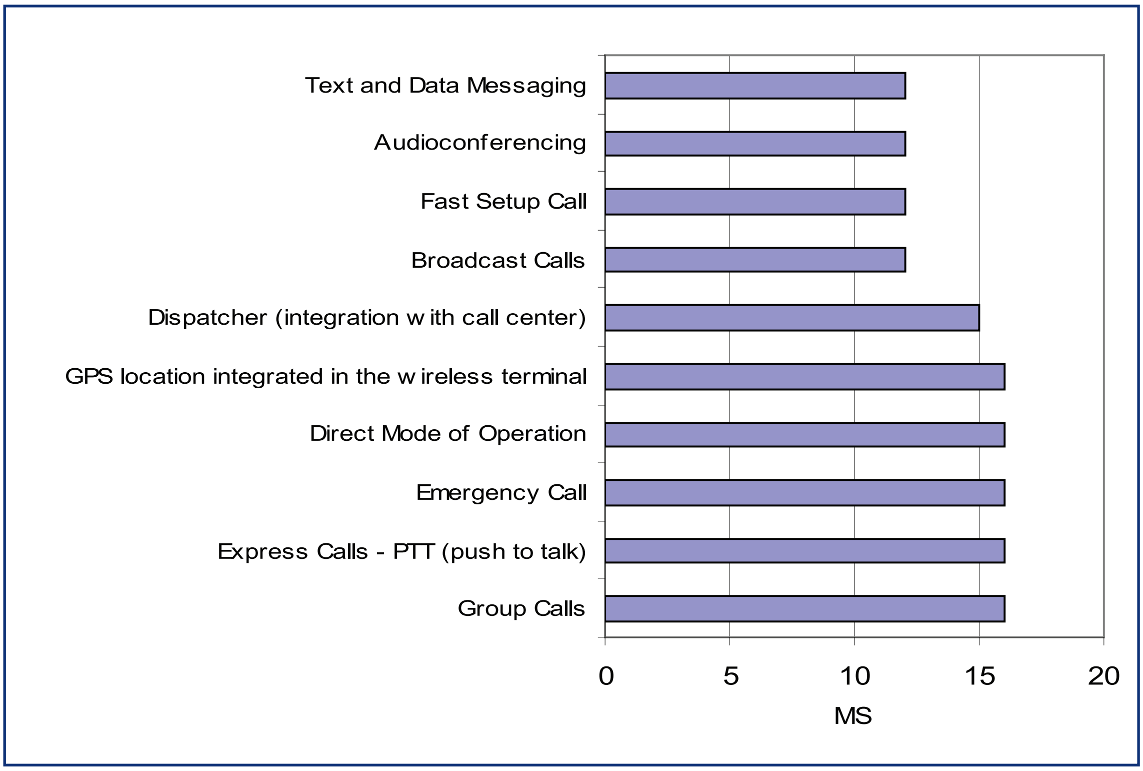


Fig. 2. Wireless communication network services used by border security forces.

5.3 Security

The results of questionnaires show that 15 MSs need to support different security levels of information relayed in their wireless communication networks. Therefore the networks need to provide different security functions designed to protect users' information. In this paper we are focused on authentication and encryption (Air Interface Encryption and End to End

[14] TESS, Key Services, http://www.tess-me.com/tetrakeyservice.html, April, 2008.

encryption).

Mutual authentication is a service required to ensure that a wireless network can control access to it and for a radio terminal to check if a network can be trusted. Authentication - ensures only valid subscriber units have access to the system and subscribers will only try and access the authorized system.

Almost all MSs express a need for Air Interface Encryption or End-to-End Encryption in wireless border networks. The Air Interface Encryption protects all signal, identity and traffic across the radio link; End-to-End Encryption protects information as it is passing through the system. Considering the questionnaires 17 MSs use Air Interface Encryptions, such as TEA2, TEA3, and TEA1. Five of them also use End-to-End Encryptions, such as IDEA and AES.

In this survey we are focused only on authentication and encryption in wireless networks, but further studies need to take into account different categories of security function, such as security mechanisms, security management features, standard cryptographic algorithms, and lawful interception mechanisms[15].

5.4 Technologies used in the wireless border communication networks

The questionnaires show that the wireless border communication networks are based on various technologies and sub-systems, such as:

PMR (Professional Mobile Radio)

- TETRA (Terrestrial Trunked Radio)
- TETRAPOL (Terrestrial Trunked Radio Police)
- APCO25 (standards for public safety digital radio)
- Analog AM/FM (MF, HF, VHF, UHF)
- FM9000
- Air Band Radio
- Maritime Radios
- Global Marine and Distress Safety System (GMDSS)

Satellite Networks

- Inmarsat
- Iridium

Mobile telephony systems

- GSM (Global System for Mobile communications) – 2G
  - » GPRS (General Packet Radio Service)
  - » CSD (Circuit Switched Data)
  - » EDGE (Enhanced Data rates for GSM Evolution)

[15] TETRA MoU Association, TETRA Security, www.tetramou.com, February 2006.

- UMTS (Universal Mobile Telecommunications System) – 3G
  - » CDMA (code division multiple access)
  - » HSDPA (High-Speed Downlink Packet Access)

Wireless Computer networks

- WLAN (Wireless Local Area Networks): WiFi (IEEE 802.11 a, b, g, h)
- WPAN (Wireless Personal Networking): Bluetooth
- WMAN (Wireless Metropolitian Area Network): WiMAX (IEEE 802.16)

The analyses of received questionnaires show that the wireless border communication networks use many different technologies. Providing the interoperability and security between these different networks is not an easy task. The interoperability between them can be provided if crucial technical information is known. Thus we purpose that further SeBoCom study gather detailed technical information about the wireless border communication networks in MSs and suggest technical solutions that provide communication between different networks.

On the other hand, the different technologies used in these networks increase the security threats, such as interference, and indirect connection to the network. Interferences can occur between different wireless transmission systems that share the same frequency band. Indirect connection to the border guard network can represent another major concern for security. Because ad hoc connections, such as WPAN, enable peer-to-peer networking between computers, an unauthorized user can be connected to the border network. This also allows an authorized user to transfer classified documents to the unauthorized user without going over the corporate network. These ad hoc connections make it difficult for security managers to monitor the activities in the wireless network and protect the border guard network from potential attacks. Therefore, the risk of them occurring is high.

5.4.1 Main wireless border communication networks

The graph (Fig. 3) shows main PMR (Professional Mobile Radios) used for wireless border communications in MS. In this paper these systems are: TETRA, TETRAPOL, and APCO25. In accordance with the returned questionnaires TETRA is used by 10 MSs, TETRAPOL is used by 3 MSs, APCO25 by one MS, and two MSs are using both TETRA and APCO25. The graph (Fig. 3) shows the number of MSs (y-axis) that use the certain communication network.

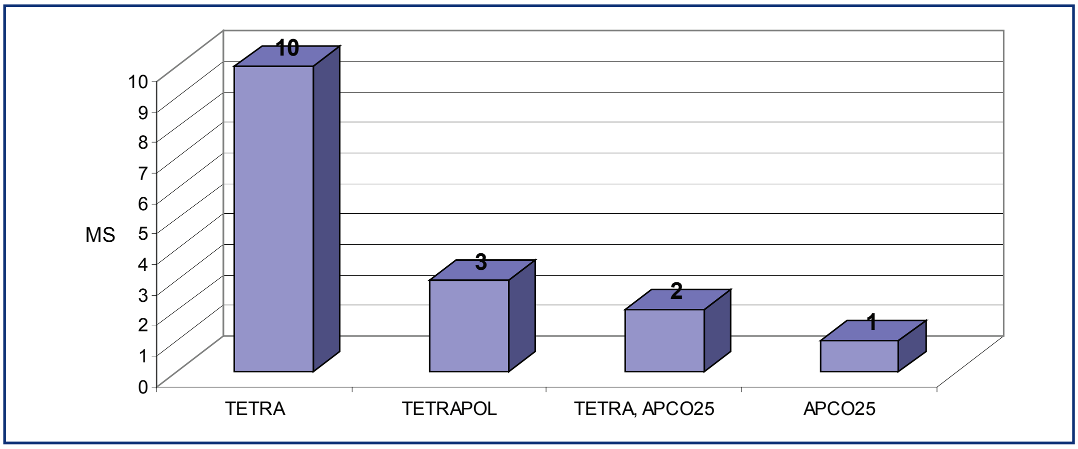


Fig 3. The use of the main wireless border communication systems.

The answers to the questionnaires show that TETRA is the most widely used PMR. Twelve countries are already using TETRA systems; among them six MSs explicitly express their intention to replace old wireless networks with TETRA systems. Some countries already have more 4000 TETRA handheld terminals and 3500 vehicular terminals.

Because the implementation of a PMR like TETRA is important and expensive, we suggest that a further SeBoCom study will take into account that TETRA systems could be widely used in the future. Therefore, we also propose a further study which will determine if the exposures to the electromagnetic field generated by TETRA systems have a potential health impact[16].

5.4.2 Operators of main wireless border communication systems

The main wireless border communication systems (TETRA, TETRAPOL, and APCO25) usually need more base stations and more expensive equipment than analog FM VHF systems. Therefore, some of them are operated by non government operators (3 of 11). In accordance with questionnaires the share of the main border communication systems operated by non government operators is shown on graph Fig. 4.

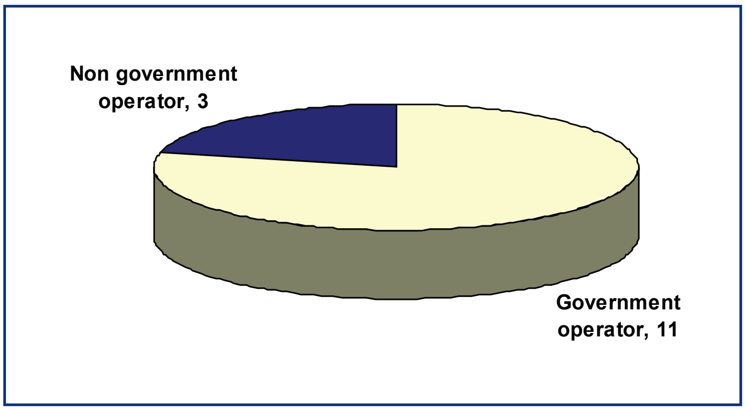


Fig 4. Government and non government operators of main wireless border communication systems.

5.4.3 Wireless border computer networks

Wireless border communication networks could be connected to different wireless computer networks such as WMAN (Wimax), WLAN (WiFi), and WPAN (Bluetooth). In accordance with the questionnaires the most often used wireless computer networks are shown in graph (Fig. 5).

[16] Smith, R. N. et all, An Investigation of the Effects of the Airwave TETRA Signal on Cellular Calcium and Brain Function, Biomedical Sciences Dstl Porton Down, Salisbury, 2005.

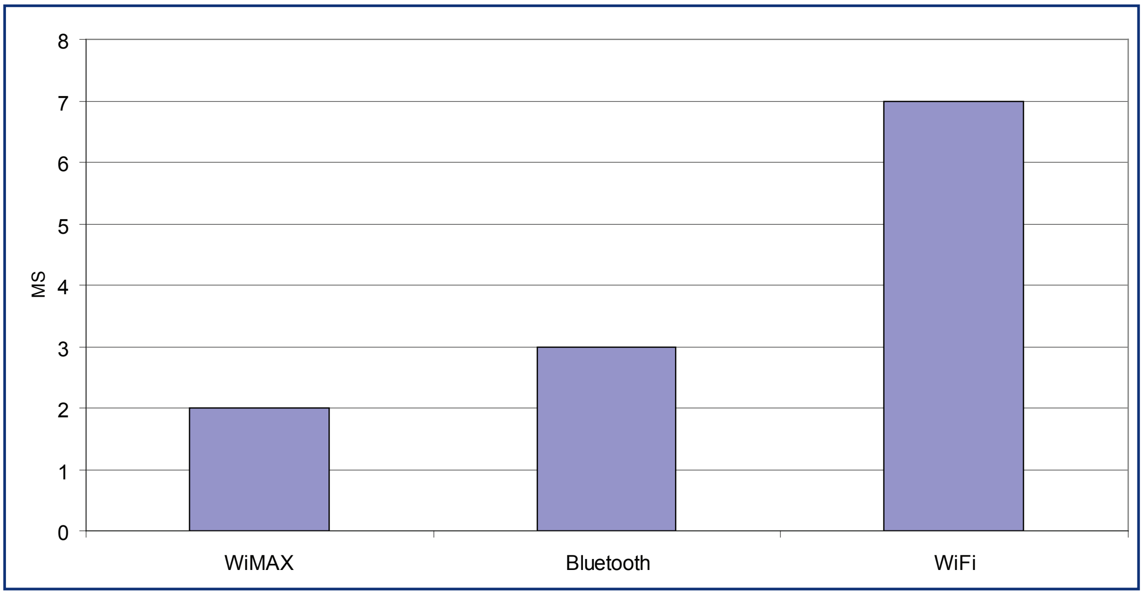


Fig. 5. Wireless border computer networks used in MS-s.

The nature of the radio waves exposes the computer networks to unwanted intruders and potential attacks. For example:

Steal the approved SSIDs and MAC addresses
In an ideal situation, the verification of an authorized user is based on the Service Set Identifiers (SSIDs) and the Media Access Control (MAC) addresses. They, respectively, act as crude passwords and personal identification numbers. However, due to the fact that they are not foolproof, it is easy for intruders to steal the approved SSIDs and MAC addresses to be able to connect to a WLAN as an authorized user. Apart from that, the nature of wireless transmission that travels as a radio wave makes it less complicated to pick up unencrypted messages and to decrypt encrypted messages using available hacking tools.

Flood the radio spectrum with static noise
Secondly, intruders who have been denied access to a WLAN can threaten to jam or flood the radio spectrum with static noise. This attack effectively disconnects stations from Access Points and consequently, shuts down the wireless network. The integrity of the network can also be abused by draining the connection speeds, hindering the overall WLAN performance. However, the possibility for it to occur is not very high.

5.5 Conclusions

Providing interoperability and security in the wireless border communication networks is not an easy task, especially if we take into account that these networks are used by various border security forces and other organizations; different types of information are relayed through these networks; different security functions are implemented in the networks (encryptions and authentications); the networks use various communication technologies; and the networks can be managed by various operators (government and non-government).

In order to provide interoperability between the different communication systems the crucial technical information has to be known. Thus, we suggest that a further SeBoCom study gathers detailed technical information about the wireless border communication networks in MSs, to suggest technical solutions for communications between these networks.

Analysis of the questionnaires shows that many MSs using TETRA communications systems. Because this kind of the network could be very expensive, we suggest that a further study collects the experiences of the current implementations of the network in MSs.

On the other hand, the further study could provide successful examples how new wireless technology could improve border security, for example the networks can include different surveillance sensors or various services.

Considering that TETRA is widely used we propose a further study which will determine if the exposure to electromagnetic fields generated by TETRA systems has a potential health impact[17].

[17] Chadwick, P., Specific Absorption Rate Measurement in Vehicles, An Investigation of the Effect of the Airwave TETRA Signal on Cellular Calcium and Brain Function, Microwave Consultants Ltd, 2007.

6. Way forward - Conclusions

The present document presents the following key findings:

1. presently there is little or no common vision for secure communications among the different bodies dealing with border security;
2. the existing communication infrastructures are quite different even within the same country;
3. there is a large number of completed or ongoing studies aimed at defining communications requirement for Public Safety, but there is none focused on the specific needs of Border Security;
4. plans for Secure Border Communications must focus both on Security and Interoperability.

The above findings prompt the initiation of a study having the following main objectives:

1. Create and populate a database of the existing telecommunications infrastructures;
2. Identify operational scenarios for the different situations which gain consensus from all interested organizations;
3. Identify operational requirements, focusing on the specific needs of Border Security, in the light of knowledge of the present technological state of the art and the legacy systems still in use;
4. Establish a permanent forum, managed by Frontex that officers from the relevant organizations can use to share views and reach consensus on operational procedures.

7. Conclusions of the workshop

During the Workshop, End Users presented their real life experience in Joint Operations and outlined their need for a reliable communication system in order to be able to perform their tasks, while Industries presented the state of the art of technology in the area of secure communications with specific reference to European Projects.

This bidirectional feed-in produced the following points of interest that define what should happen.

- Interoperability, flexibility and reliability are crucial;
- Defining a common procedure is the first step to achieve operational interoperability;
- The focus is on functionalities and ease of use, rather than on technology;
- An incremental approach would be favored against an overarching approach, in order to preserve existing investment and to have at least minimal functionalities as soon as possible;
- Some representatives suggested the activation of ad hoc projects to help member states solve specific issues (e.g.: to get TETRA network and a Tetrapol network to interoperate);
- To be aware of new technologies, but to introduce them into the system only if they are really necessary to cater for an operational need.

Further more, during the SeBoCom Workshop two proposals were put by respective MSs.

- **Maltese proposal**
  Frontex with the help of MSs ought to develop a manual / booklet regarding the common procedures / common ways of communication in Joint Operations.
- **German proposal**
  Germany proposed a pilot project. This project ought to provide equipment that would be tested to bridge different communication means of the participating MSs in a specific Joint Operation. In this way interoperable alternative solutions could be explored and the best “practices” defined.

These proposals, as well as other suggestions presented during the workshop, further reinforce the interest of Member States in SeBoCom in future carrying out a complete study to analyze the following subjects also:

- Human aspects interacting with complex systems under stress, i.e. user friendly systems;
- Level of skills of the users in conjunction with the introduction of solutions such as SDR and the focus on simplification that they introduce.
- Probable mandatory EU legislation implementing a unique “Communication System” in the external borders (financial issues).

8. Reference Bibliography

ETSI documents (http://portal.etsi.org/emtel/status.asp):

- SR 002 180: Requirements definition for emergency call handling.
- TS 102 181: Requirements for communications between authorities during emergencies.
- TS 102 182: Requirements for communications from authorities to citizen during emergencies.
- TS 102 410: Requirements for communications between citizens during emergencies.
- TR 102 445: Requirements for Emergency Communications Network Resiliency.

1. http://www.frontex.europa.eu/
2. “Communication failures hampered London bombing rescues, article” appeared on CNET www.news.com By Andy McCue: http://www.news.com/Communication-failures-hampered-London-bombing-rescues/2100-7348_3-6079889.html as of 14-5-08.
3. “Report of the 7 July Review Committee, Greater London Authority, June 2006”.
4. “The lessons of non-interoperability in public safety communications systems”, Donald A. Lund April 2002, the ATLAS project, Advanced technology in law and society, University of New Hampshire USA.
5. Steve Worrall (2005). An International Study of Radio Interoperability, steve.worrall@shropshirefire.gov.uk.
6. “Protecting Public Safety With Better Communications Systems” Jon M. Peha Carnegie Mellon University IEEE Communications, March 2005.
7. “Mobile Information and Communication Systems in Crisis Situations” Presentation by EPFL (MICS) Jacques Panchard: jacques.panchard@epfl.ch http://www.terminodes.org and IISc HS Jamadagni: hsjam@cedt.iisc.ernet.in http://www.iisc.ernet.in
8. KAMEDO Report No. 88:“Floods in the Czech Republic and Southeastern Germany, 2002” Ulla Näsman; Birgit Zetterberg-Randén; Helge Brändström (ed), KAMEDO = Swedish Disaster Medicine Study Organization.
9. SAFECOMM website: http://www.safecomprogram.gov/SAFECOM.
10. Wireless Technologies and the SAFECOM SoR for Public Safety Communications - Leonard E. Miller - 2005 .
11. MESA Project website: http://www.projectmesa.org
12. Public Safety Communication Europe website: http://www.psc-europe.eu/
13. ZONIT, TETRA Alarm Control System, http://www.zonith.com/products/tetra/, April, 2008.
14. TESS, Key Services, http://www.tess-me.com/tetrakeyservice.html, April, 2008.
15. TETRA MoU Association, TETRA Security, www.tetramou.com, February 2006.
16. Smith, R. N. et all, An Investigation of the Effects of the Airwave TETRA Signal on Cellular Calcium and Brain Function, Biomedical Sciences Dstl Porton Down, Salisbury, 2005.
17. Chadwick, P., Specific Absorption Rate Measurement in Vehicles, An Investigation of the Effect of the Airwave TETRA Signal on Cellular Calcium and Brain Function, Microwave Consultants Ltd, 2007.

9. Annex 1: Questionnaire

A. General Questions

1. Who will be the contact person for SeBoCom pre-study?
2. Which are the agencies involved in Border Security (Coast Guard, Military Police, Army, Custom Office, etc.)?
3. What is the "mission" of each agency [describe in few words the task of each agency with reference to the agency needs for secure communications]?
4. What the numerical force (please detail the different tasks) of each agency?
5. Do you plan to replace your existent radio communication system in the near future (within 3-5 years? If yes, which technology you are planning to acquire?
6. If your system supports data communications, please briefly describe what kind of data are transmitted over the network.
7. Do you have surveillance sensors connected to the communication networks? if yes, please describe them.
8. Are officers enabled to directly access sensors data [raw/filtered] on their handheld devices?D
9. Does your organization already use any of the following technologies?
   WiFi (IEEE 802.11 a,b,g,h)
   HyperLan
   WiMAX (IEEE 802.16 d, e)
   Bluetooth
   ZigBee
   Satellite Network
10. What type of wireless communication services do you need?
    Group Calls
    Broadcast Calls
    Express Calls (push and talk)
    Fast setup call
    Emergency call
    Direct Mode of Operation
    Dispatcher (integration with call center)
    Trunking
    Audio-conferencing
    Text and Data Messaging
    GPS location integrated in the wireless terminal
11. Do you need to support different levels of security in your wireless communications infrastructure?
12. Do you need air interface encryption or end-to-end encryption ?

B. Technical questions

a 1. Technology: Please specify what technology is used by the radio network (networks) you are currently using [i.e. TETRA, Tetrapol, APCO25, etc.]

a 2. Operator of the Network: please specify if the Network is operated by a department of the border police (name of the department) or by an external body (please specify)

a 3. Frequency used: please specify the frequency band (bands) used by the Network (i.e. 380-395 MHz.)

a 4. Organization that mainly uses the network: if the network is used only by the owner, just write the name of the owner, if the network is used by other organizations, please list them

a 5. Contents: please specify whether the network is used for voice or data or both

a 6. Number of Base Stations: please specify the number of Base Stations used in the Network

a 7. Number of Switches: please specify the number of switches used in the Network

a 8. Encryption standards used in the network: please specify the encryption standards used to guarantee the security of Network

a 9. Authentication systems used in the network: please specify the systems used to authenticate the users of the Network (password, etc.)

a 10. Security level: please specify the highest level of security for which the network is enabled

a 11. Number of handheld terminals: please specify the number of handheld terminals used in the Network

a 12. Number of vehicular terminals: please specify the number of Vehicular Terminals used in the Network

a 13. Number of users: please specify the number of users utilizing the Network

a 14. Percentage of external border: please specify the percentage of the external border “covered” by the network

If your organization uses also other radio communication networks, for each of them, please provide the following information:

b 1. Technology: Please specify what technology is used by your radio network (networks) [i.e. TETRA, Tetrapol, APCO25, etc.]

b 2. Organization that mainly uses the network: if the network is used only by the owner, just write the name of the owner, if the network is used by other organizations, please list them

b 3. Content: please specify whether the network is used for voice or data or both

b 4. Interconnection: please describe how this network is interconnected to the other one (Gateway, Automatic switchboard, Manual switchboard, etc.).

10. Annex 2: Joint Operation XXXX

General

Five Member States collaborate in a maritime surveillance joint operation along the coast of MSy1. JO XXXX deals with illegal migration in the YYY maritime borders of the European Union. The MSy1 Island and MSy2 Islands are facing an influx of irregular migrants from the YYY direction.

So, this operation aims specifically at creating a shared operation basis that is considered very critical for the improvement of co-operation and co-ordination.

Objectives

The main objectives are organizing and performing counter illegal immigration operations, carried out by assets of MSy1, MSy2, MSy3, MSy4, MSy5 and MSx2 ,enhancing flow of information among assets, competent departments and co-ordination centers through a secure communication network.

Execution

International Co-ordination Center:

The International Co-ordination Center will be set up at MSy1 with the following responsibilities:

- Coordinate the development of maritime/air operations in respective operation areas;
- Receive reports from assigned asset through the communications network, collect and evaluate the data, and convey the relevant information to other National Coordination Centers;
- Maintain continuous watch on maritime and air radio frequencies.

Director of the Centre will an MSy2 Senior Officer.

Communication:

Communications should be according to international or national regulations in force of the competent agencies of participating EU MS.

These communications should be used for exchange of information according to the given priorities: e-mail; fax; telephone.

More detailed plan of who communicate and with what is presented in the “communication Table of JO XXXX” in the end of this SCENARIO.

Assets employed:

The assets listed below will participate in Joint Operation XXXX.

- MSy1: one vessel type w1
- MSy2: one vessel type w2 and one aircraft type z1

- MSy3: one helicopter type s1
- MSy4: one vessel type l1
- MSy5: one vessel type k1
- MSx2: one vessel type f1 and one aircraft p1

Area of operation:
The Joint Operation XXXX is going to be implemented within the following geographical area:

Maritime Assets:

Lat.	99°22'N	Lon.	99°00'E
	99°11'N		99°99'E
	99°33'N		99°09'E
	99°44'N		99°90'E

Air Assets:

Lat.	99°55'N	Lon.	99°22'E
	99°66'N		99°11'E
	99°77'N		99°33'E
	99°88'N		99°44'E

Time of Operation:
Planed time/date of the operation is:
Start: at 88:88 UTC on 8/8/8888
End: at 99:99 UTC on 9/9/9999

Contact of operations; air patrolling; maritime patrolling:
Air patrolling is to be carried out by assigned air units. Contacts of interest will be forwarded by the air units, to ICC via radio frequencies (VHF or UHF). The average duration of flight missions will vary between “dd” and “ee” hours, according to the type of aircraft used.

Maritime patrolling is to be carried out by assigned naval units. Contacts of interest will be forwarded by the naval units, to ICC via radio frequencies (VHF or UHF) or satellite communication (Inmarsat).

Reported incident:
At 99:99 UTC on 8/8/9999 a migrant boat was detected by aircraft “z1”. It informed vessel “w1” through UHF communications which accordingly informed ICC (through satellite means). ICC informed vessel “k1” patrolling in the specific area to follow the progression of migrant boat and try to identify: size, speed, course, activity and persons on board. The gathered information was transmitted to ICC via satellite phone, as follows:

- Size: 5 m
- Course: YYY North
- Speed: 3 knots
- Persons on board: 15

In second encircle phase vessel “k1” sent an Investigating team with a boat to visually acquire additional information which is to be immediately relayed to the vessel.

The Investigating team didn’t make any physical or verbal contact with migrant boat. It transmitted to vessel through VHF the following information:

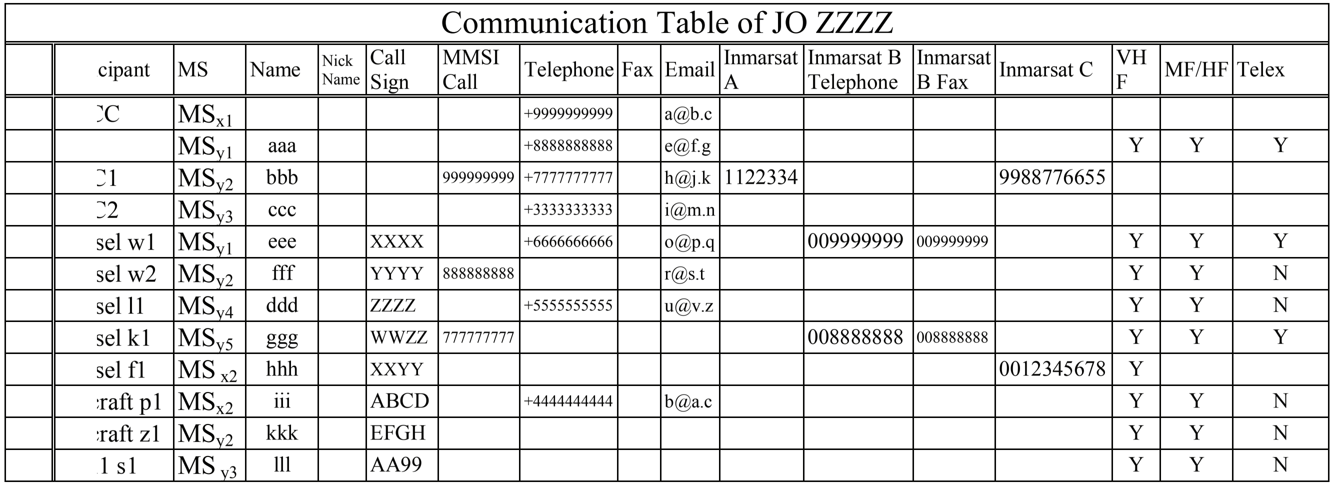
- Rather good condition of persons on board
- Probable existence of driver/facilitator
- No further ship or other equipment facilitating the transportation

In third approach phase the migrant vessel was approached. Upon arrival next to the migrant boat, the Investigating team commander gave clear guidelines indicating his intentions in the following sequence:

- Request nationality of boat from the person driving the boat;
- Request documentation of vessel from the person driving the boat to indicate proof of ownership, registration and legality of voyage;
- Gave life-jackets to all on board and order them to wear life-jackets;
- Informed migrants that entering any EU Member State in this way is illegal and the organizers of such illegal entry would be severely punished;
- Brief the people navigating the boat on the use of the equipment provided and remain steaming parallel until they are heading on the correct course.

The actions undertaken were transmitted immediately through satellite phone to ICC.

Appendix I



Communication Table of JO ZZZZ															
	cipant	MS	Name	Nick Name	Call Sign	MMSI Call	Telephone	Fax	Email	Inmarsat A	Inmarsat B Telephone	Inmarsat B Fax	Inmarsat C	VH F	MF/HF	Telex
	CC	MS_{x1}					+9999999999		a@b.c							
		MS_{y1}	aaa				+8888888888		e@f.g					Y	Y	Y
	C1	MS_{y2}	bbb			999999999	+7777777777		h@j.k	1122334			9988776655			
	C2	MS_{y3}	ccc				+3333333333		i@m.n							
	sel w1	MS_{y1}	eee		XXXX		+6666666666		o@p.q		009999999	009999999		Y	Y	Y
	sel w2	MS_{y2}	fff		YYYY	888888888			r@s.t					Y	Y	N
	sel l1	MS_{y4}	ddd		ZZZZ		+5555555555		u@v.z					Y	Y	N
	sel k1	MS_{y5}	ggg		WWZZ	777777777					008888888	008888888		Y	Y	Y
	sel f1	MS_{x2}	hhh		XXYY								0012345678	Y		
	raft p1	MS_{x2}	iii		ABCD		+4444444444		b@a.c					Y	Y	N
	raft z1	MS_{y2}	kkk		EFGH									Y	Y	N
	1 s1	MS_{y3}	lll		AA99									Y	Y	N

European Commission

EUR 23536 EN - Joint Research Centre - Institute for the Protection and Security of the Citizen
Explosive SeBoCom Pre-Study - a preliminary study on secure border communications
Authors: Dimokritos Tziritis, EU Frontex Agency;
Aleksander Pur, Ministry of the Interior, Slovenia;
Franco Oliveri, EC Joint Research Ispra
Luxembourg: Office for Official Publications of the European Communities
2008 – 59 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593

Abstract

This document contains the outcome of the SeBoCom pre-study. The main objective of the SeBoCom project was to define the way to proceed to a further and complete study. This task was to be achieved through this pre-study and through a Workshop involving end-users to stimulate the discussion and gain input regarding their needs.

This pre-study collects some initial data on the present Communications infrastructures outlining the co-existence of many different systems, some already based on digital technology, others outdated or quite obsolete.

One of the key finding of the present study is the need to define joint procedures to manage communications among different bodies belonging to different Member States: the most reliable and secure telecommunication infrastructure will be useless if there is no agreement on the type and structure of communications that are transmitted over the infrastructure.

The pre-study initially considers the pivotal role played by communications in Border Protection field operations, analyzing the different operational aspects.

It subsequently presents the state if the art of the communication infrastructures of Border Security Forces in Europe as well as the expected future scenarios obtained through questionnaires sent to the contact points in the Member States.

An initial broad view of the requirements for Secure Border Communications is outlined; this is followed by an analysis of the lessons learned in previous events; then a survey of the previous/ ongoing studies on similar topics is also presented.

The last chapters provide a Technology Survey and the conclusions based on the outcome of the pre-study and of the Workshop held in Ispra on May 27th and 28th 2008.

Mission of the JRC

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

Publications Office
Publications.eu.int