Answers from Industry to the Challenge of Homeland Security

Manfred Bartha, Dipl.-Ing.

European Aeronautic Defence and Space Company
Defence and Security System Division
EADS Deutschland GmbH
Friedrichshafen, Germany.
e-mail: manfred.m.bartha@eads.com

Manfred Bartha studied Electronic and Information Technology at the Oskar von Miller Polytechnikum in Munich and received a degree as Dipl.-Ing. in 1972. In the same Year he joined the Aerospace Company Dornier, now EADS, in Friedrichshafen. After some Years electronic development he became project manager for the C3I system HEROS for the German Army and for the command post ARES for the rocket artillery system MLRS. In 1985 he became head of the department "Robotic and Mine Detection." He was responsible for the military robotic experimental program PRIMUS (Program of Intelligent Mobile Unmanned Systems) and for co-operation programs with the USA and France. In Mine Detection he headed the projects for land-based and airborne mine detection MSG, AAMIS and DMH. He was member of several working groups for mine detection as NIAG, AGARD, JRC (European Commission, Joint Research Center) and international Conferences on De-mining Technology. From 1995 to 2002 he worked in sales and marketing to the German forces and for export. In 2002 he joint the new department for Homeland Security and is responsible for marketing and project management for border security systems.

ABSTRACT

The attacks of September 11 in 2001 on the World Trade Center in New York have revealed the vulnerability of nations and of the worldwide economy to large scale terrorist attacks. Such attacks can take on the most unexpected form and consequences. This requires more political, social and also technological efforts to prevent such attacks from occurring in the future. If we are confronted with such threats, we should at least be properly prepared to deal with them. Any response to such threats must therefore be a global one. The threats may focus on sensitive targets offering high political and media impact, such as air, land and maritime transport systems. But, they may also be stealthier and far-reaching which could be an unauthorized penetration of communication networks or IT hacking.

The threat is not limited to terrorism. It may also come from organized crime networks, many of them having terrorist ties. Illicit trafficking of weapons and drugs has a destabilizing influence and is a permanent threat. In addition to terrorism, we can add the uncontrolled migration flows of people, which are often controlled by organized crime syndicates. Other dangers come from accidental or deliberate pollution through industry or transport systems, which can have serious environmental and economic impacts. This is especially relevant for coastal areas, which heavily rely on fishing and tourism.

After the terrorist attacks in 2001, the United States developed the concept of Homeland Security. Under this concept all present and future resources are coordinated through a federal agency to ensure maximum internal defense. The Industry of the United States has also reacted immediately. The large Aerospace and Defense Companies (e.g. Boeing, Lockheed Martin) have formed new organizations with some thousands employees addressing themselves to the tasks for Homeland Security.

While the European Governments only make few financial efforts to overcome these problems the Industry has reacted also directly with new dedicated organizations, even if in a smaller frame. This paper will show the engagement of European Industry at the example of EADS. Answers from Industry in three major segments in public security, which have become an important issue not only within Europe, will be discussed.

- Air transport security in order to guarantee the confidence of clients and the circulation of people and goods.

- Border security on land, coastal borders and border crossing point on borderlines or at air- and sea ports.

- Security management systems to protect major events from terrorist attacks, crime or vandal excesses and to handle natural disasters.

The primary focus of the paper is on Border Security, particularly in Europe.

NEW THREATS FOR HOMELAND SECURITY

The attacks of September 11 in 2001 have dramatically shown that the new terrorism has a new quality. New forms of terrorism bring along new dimensions of threats globally. Every country and every event can be object of a terror attack.

The main new kinds of terrorism are:

- Increasing number of terror and crime cases.

- Threat against civilian population.

- Kind and amount of weapons in use have changed (the use of any weapon, as there are conventional, biological, chemical, or also nuclear and radiological).

- Western industrial countries are the main target for terrorism.

- New asymmetric threats.

- In addition increasing of natural disasters:

 There is a serious need of cross-linking within security structures (Network).

THE SITUATION IN THE USA

THE US GOVERNMENT

The Government of the USA, the target country of September 11th, has reacted immediately. It has started to set up an integrated organization, the Department of Homeland Security. This department will be provided with considerable resources, in the Finance Year 2003 $37.5 billion). This new Organization will have a staff of some 170,000 by regrouping many departments and agencies with there activities.

Major initiatives have been started already, e.g. in border control, transport security, airport security, NRBC defense, intelligence and police operations. In addition a large program for the US Navy has been launched, the Deepwater Program (Figure 1). This program has a volume of $ 17 billion and a timeframe form 30 Years.

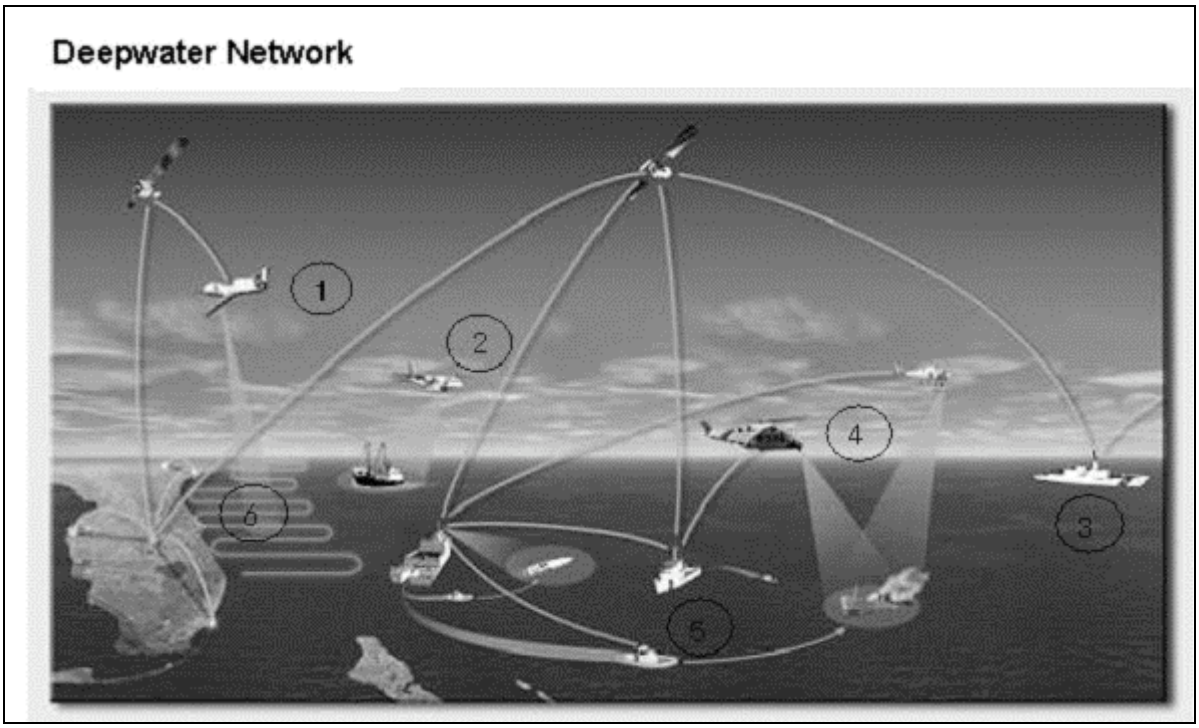

Figure 1: Deepwater Network. Key: 1. HALE UAV Wide Area Surveillance (High Altitude Long Endurance Unmanned Air Vehicle), 2. MPA (Maritime Patrol Aircraft), 3. Interoperability, 4. Multi Task Operation, 5. Over the Horizon Operation, 6. Shore-based Command Center.

The Deep Water realization is a complete upgrade and refurbishing program. It will connect all maritime forces as Navy units and the Coast Guard together as a Network Centric System including airplanes, Helicopters, UAVs, patrol boats and cutters and land-based forces and head quarters as well.

The main tasks of this network are in five areas:

- Maritime Safety.
- Maritime Security.

- Protection of Natural Resources.

- Maritime Mobility.

- National Defense

US INDUSTRY

US Industry has also reacted immediately after September 11th. The large Aerospace and Defense Companies as there are Boeing, Lockheed Martin and Ratheon have formed new organizations with some thousands employees addressing the Homeland Security.tasks. But also smaller supply companies have reacted and are active for Homeland Securety tasks.

Lockheed Martin and Northrop Grumman won the Deepwater contract ($ 17 billon). On the over all budget of $37.7 billion for 2003 in the US, the industry was able to develop wide spread activities with enable it to operate world wide on this new market.

- The US has started significant Initiatives.

SITUATION IN THE EUROPEAN UNION (EU)

POLITICAL REACTION

The European Union responded swiftly to the terrorist attacks of the 11th September 2001. Within days of the attacks on America, a series of concrete measures were tabled by the European Commission, which led to a Plan of Action adopted by a special European Council on the 21st September.

Over the past year, the European Union has sustained its efforts as one of the leading partners in the global fight against terrorism. Implementing the Plan of Action, all EU efforts are guided by:

- Continued solidarity with the US.

- Determination in the fight against terrorism.

- Commitment to the security of all citizens in the EU.

- Efforts to tackle root causes of terrorism.

- Contributions to better understanding between civilizations.

The EU has focused on those areas where it can complement the efforts made by individual Member States. Source[1] EU doesn't have a budget for the security measures of the member states. The members are responsible on their own. EU has money allocated in Programs for border security of candidate counties in order to prepare these for affiliation (PHARE, MEDA).

- EU has reacted politically, for security the member states are responsible on their own.

ENLARGENT OF THE EUROPEAN UNION

On May 1st 2004 the European Union affiliates additional 10 Countries as EU members. The new member states are:

- Czech Republic
- Estonia
- Cyprus
- Latvia
- Lithuania
- Hungary
- Malta
- Poland
- Slovenia
- Slovakia

This affiliation causes new EU external borders to the states of Russia, Belarus, Ukraine, Croatia, Yugoslavia and Rumania, the EU candidate for integration in 2007 (Figure 2). In addition there is Kaliningrad, an isolated enclave of Russia without a connection on land. This requires some political solution e.g. a corridor though Latvia or / and Poland. From the previous EU member states some critical coast lines are still remaining, mainly the Mediterranean coast and also from the former Eastern Germany to the Baltic Sea.

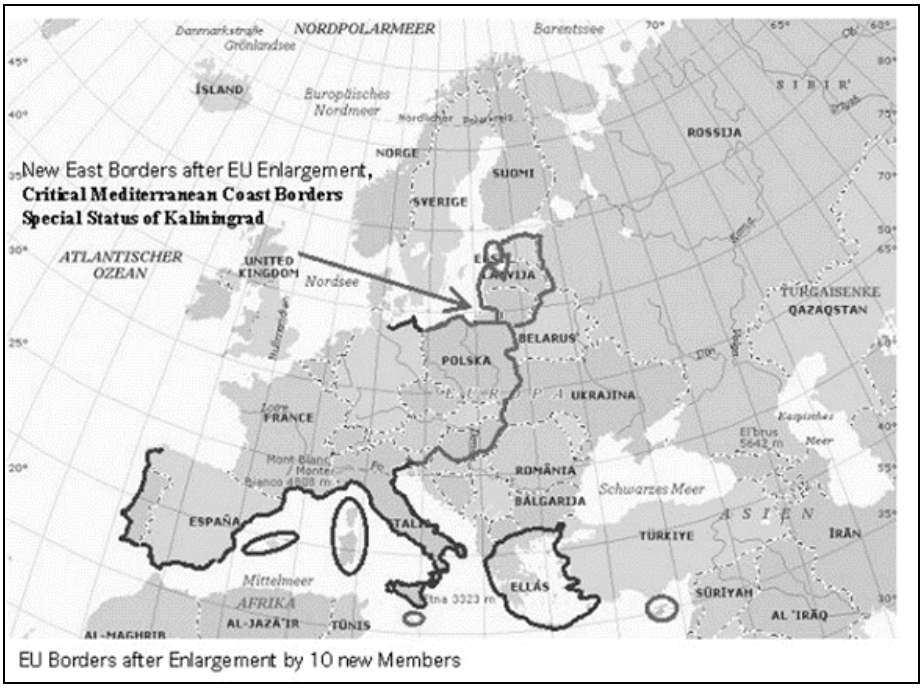

Figure 2: EU Border after Enlargement.

[1] http://europa.eu.int/comm/110901/index.htm

Because of the EU enlargement requirements for the new EU external borders arise. Important pre-conditions for a successful border control are:

- Interoperability of communication equipment (EU project ”Schengen II”).
- Modern standardized equipment (PHARE Program).
- Interoperability of land- and sea based forces (kind of European Deepwater).

These pre-conditions are still not achieved. The Mediterranean coast lines are still not gap less secure. At the coasts of Portugal and Spain frequently immigrants from Africa and at the Italian cost immigrants from Africa but also from Eastern Europe arrive.

The communication and data exchange between the EU member states and in some countries between the services in the county is not sufficient. Radio communication is especially critical. The equipment in use in the different countries is often not compatible and at a low technical performance.

In crises or catastrophic cases an efficient co-operation between the EU member states is difficult. The authorities in the different countries have different responsibilities and are organized differently. Because of lack of interoperability of the various systems in use an effective co-operation is not possible.

- There is a strong need for harmonization of organization, technology in use, and the legal system in Europe.

SCHENGEN AND SCHENGEN INFORMATION SYSTEM

The Schengen area came into effect in 1995. It consists of fifteen countries Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Italy, Greece, Luxembourg, Netherlands, Norway, Portugal, Spain, and Sweden (Figure 3).

The Schengen area:

- Abolishes the internal borders.
- Creates a single external border where immigration checks for the Schengen area are carried out in accordance with a single set of rules.

The Schengen Information System:

- Is a complex information system that allows the competent authorities to exchange data.
- Permits people’s identification and descriptions of stolen objects.
- Consists of a Central System (C.SIS) located in Strasbourg and of National Systems (N.SIS) in each Member State.

Figure 3: The European Community Schengen Information System (SIS).

- SIS 1 was undertaken by a consortium of SEMA, Siemens, and Bull.
- An enhanced version (SIS 1+) was then produced by Atos, Computer Sciences Corporation, and IBM – July 1998.
- Contracting authority for SIS 1 and SIS 1+: The French Ministry of Interior.

SCHENGEN INFORMATION SYSTEM SIS 2

Currently under development (feasibility study is carried out by Deloitte & Touche for the European Commission until April 2003. SIS 2 is necessary because of the following:

- Quantitative reasons: future enlargement of the EU and of the Schengen area.
- Qualitative reasons: SIS is outdated and there are new development possibilities (SIS 2 records may include photos, fingerprints, even DNA profiles).
- Europol may be given access to SIS 2.
- Contracting authority will be the European Commission.

 Schengen 2 will be an important step for interoperability and co-ordinated operations in the European Union.

THE SITUATION IN FRANCE

As other countries in Europe, France has been the objective for terror attacks inside France and abroad. The main known terror organizations are:

- Armed Islamic Group (GIA).
- Salafist Preaching and Combat Group (SPCG).
- The Basque terror organization ETA (stands for ”Basque Region and Freedom”).
- National Liberation Front of Corsica (FLNC).

To overcome these organizations, the ”Secrétariat général de la défense nationale (SGDN) has already 1978 (under Giscard d’Estaing) the plan ”Vigipirate” worked our. This plan has bee reinforced in 1995 and 2000. Vigipirat consists of two phases. Basic (Phase 1) and enhanced (Phase 2). In Phase 1 mainly the measures for the administration will be activated. Sensitization of the authorities for public order, checking the efficiency of procedures of access control to sensitive infrastructure and networks.

The Phase 2 is an intensification of the basic measures. It combines the Military Forces and the Police Forces. Security forces and the customs will be alerted, intensification of patrols and check of public buildings, Air and sea ports, train station, public transportation etc. though military forces and police.First time reinforced Vigipirat was activated starting of ”Desert Storm” in January 1991 and in the following time in 1995 and 1996 when the terror attacks in RER took place.

In addition France has been active in the following fields:

- Low Amendment (LOPSI-Loi, Orientation pour la Sécurité Intérieur).
- Pilot Project for expansion of the Police Communication System ACROPOL for Security and Rescue Agencies.
- Implementation of a standardized Emergency Phone System.
- Improvement of the Coast Control.
- Improvement of Education and Training of persons in charge.
- France also has started Initiatives.

THE SITUATION IN GERMANY

Terrorism is not new in Germany. Germany also was often object of terrorist attacks in the past (e.g. by political left oriented terror group as ”Baader Meinhof” or by Arabic terror units

at Olympic Games 1972 in Munich). Further, additional more serious assaults have to be expected. Only recently, Germany was named as a potential target country for terrorist attacks on the tape, which was recorded by Usama bin Laden presumably. The unthinkable has happened on September 11th 2001. The terrorism has reached a new dimension. But the efforts in Germany are still not sufficient (Figure 4).

The main barriers in Germany are:

- Confirmed Separation of responsibility within the differed authorities.
- The links and processes of co-ordination between the Security Services don't meet the needs. Equipment in use does not match the needs of Security Services.
- Opportunities for co-operation within Germany and Europe are not used.
- Germany also has a security gap in the Baltic coast line of Mecklenburg-Vorpommern, a former Eastern German State.
- Illegal immigration and smuggling takes place at the harbor of Rostock.
- The coast control at the Baltic sea has to be improved.
- Links between Security Services must be improved. Interoperability is not given (Example Czech Republic and Germany).

Figure 4: Germany.

MASS TRANSPORT SECURITY

Terrorism wants to cause sensation with its actions. Therefore it is in most cases aimed at larger person groups, facilities of high value or at danger substances. As experience shows, terrorists find access possibilities primarily then when persons or things are travelling. Therefore Mass Transport Security must be noticed particularly at anti terror measures. This applies to mass transport on land, at sea and in the air. In principle, the responsibility for the public traffic lies with the national governments or subordinate authorities. Therefore the role of industry cannot be in a leading position, but can be a main driver for conception, system realization.

AIRPLANE IN FLIGHT SECURITY

Airplane in flight security covers all security measures inside the aircraft e.g. reinforced cockpit doors, surveillance systems (TV with data link to the ground), improvement of the navigation system, explosives detectors, radio detectors (Figure 5). This work will be carried out by the aircraft industry (e.g. Boeing, Airbus).

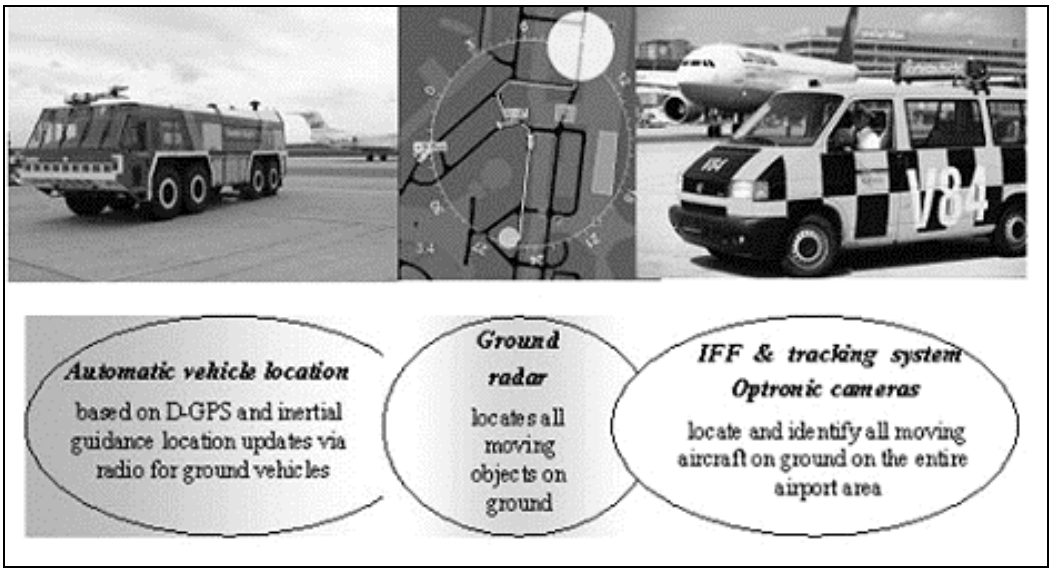

Figure 5: Aircraft Security Systems.

AIRPORT SECURITY

Airports are particularly threatened targets for terrorist attacks. Primarily the large international airports like Frankfurt, Munich, Berlin can be checked only with difficulty. Control of thousand passengers from all countries of the earth, the baggage of the passengers as well as large sets of freight is an enormous challenge to the security services (Border Police and Sub Contractors) every day. In addition the airport staff (at the Fraport approx. 13 000) as well as the employees must of at the airport working companies, e.g. building contractor have to be controlled and monitored active. At accidents or attacks a fast reaction

is necessary with interception forces. To manage this, a comprehensive equipment is required. A comprehensive approach of Airport and Air transport security is needed.

- Identification of persons and availability of background information, such as "a black list," previous convictions (chip card, biometrics, networked databases).

- Baggage and freight control on weapons, hazardous material but also on drugs and smuggling goods (metal detectors, X-ray apparatuses, neutron scanner, analytical instrument).

- Supervision of the complete traffic at the airport (GPS/GALILEO, ground radars, secure communication).

- Supervision of the airport fence and the adjacent areas (electro-optical sensors, radars, ground sensors, shock sensors).

- Operation control of interception and rescue forces (Command center, digital cards, data bases, secure communication).

AIRFIELD SECURITY

The main tasks to secure the airfield are:

- Coordination and control of all ground traffic.

- Check of all personal having access to the airport outside area.

- It has to be ensured that no unauthorized person enters restricted areas. This includes also temporary at the airport working persons e.g. for repair or construction work.

- Detection and location of all moving objects on ground.

- Protection of aircrafts on ground (access control, cargo hold surveillance).

- Protection of aircrafts when take off and landing against missile attacks from outside the airport.

OTHER MASS TRANSPORT SECURITY

Beside of the air transport security all other transport systems have to be controlled. We have seen that ground based systems are often targets of terrorist attacks. Some example are the underground in Paris and Tokio, the train terminal in Madrid, some attacks against train in Germany by distraction of the rails or attack against US Navy with small boats full of explosives.

The list can be enlarged arbitrary. However, the network of train rails, streets, undergrounds, and ship lines are so large that a complete sufficient control is not possible. In Germany all ship traffic coming from the sea and all train traffic inside the country is in the responsibility of the Federal Border Guard (BGS). The Police of the 16 States of Germany will control all the other traffic.

BORDER CONTROL

Border Control protects the territory of a country from illegal entry of unwanted persons and from import of weapons and hazardous material such as NBC and has to inhibit smuggling. This includes all borders on land, on water and from the air but also territory internal borders at airports, harbors and train stations (Figure 6).

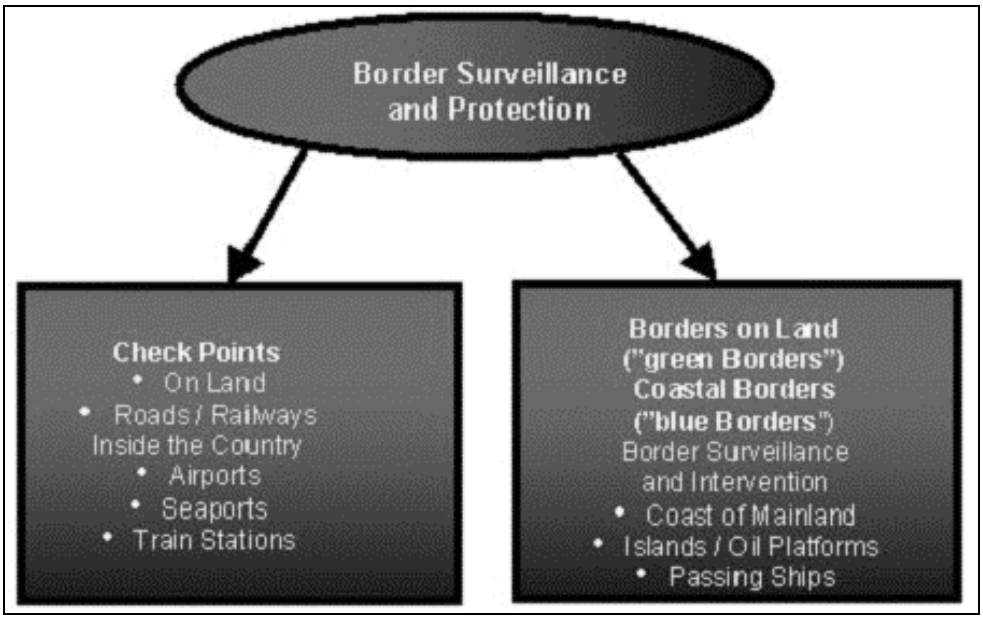

Figure 6: Border Surveillance and Protection.

Even after the coming into force of the Schengen Implementing Convention the presence of border control at the Schengen internal borders remain, in order to effectively counter the changing appearances of trans-border and organized criminality. To accomplish this task a wide range of surveillance and intervention means are necessary such as helicopter, airplanes, boats, radar systems, EO-sensors, screening devices, ground sensors ect. (for example, the German border police has over 100 helicopter). In addition, C2 – C4IR systems secure communication and data bases are needed.

A huge market is established, and after 11th of September 2001 this market is growing by numbers. In US the budget only for border and transportation security will be 23,8 bn in 2003. After enlargement of the EU by 10 countries Europe will have new east borders. For this, border control will be implemented through the Phare program. The budget for this is approx. 150 million to 200 million Euro per year. Beside of this there is an urgent need of an improvement of the coastal surveillance and protection at the Mediterranean countries.

In order to make sure that illegal Immigration and import of goods are impossible both kinds of borders at the mainland (green border) and all coasts (blue border) and the airspace over these borders have to be controlled. In particular at German coasts and in seaports (Rostock) criminal organization imports drugs and illegal immigrants into the country. After the east enlargement of the EU, Germany will have no outer border at the mainland any more (exception Switzerland). However, one cannot be sure that people not try to smuggel in illegally over the East European or from the Mediterranean countries. This means that BGS and police must still carry out border control person check (also inside the country) in future.

To fulfil this tasks a large number of air, sea and land-based reconnaissance and interception means are required (helicopter, MPA-MSA airplanes, boats, vehicles, radars, electro-optical sensors, X-ray equipment etc.). Besides these command and control systems, integrated databases into a network and secure communication are needed. The interoperability between the police, the BGS and security services of other states must be guaranteed.

Border Control has two main areas of responsibility (Figure 7):

- Check Points at all Border Crossing points, including Air- and Sea Ports and Trains.

- Borderlines on Land and Coastlines (green and blue Borders).

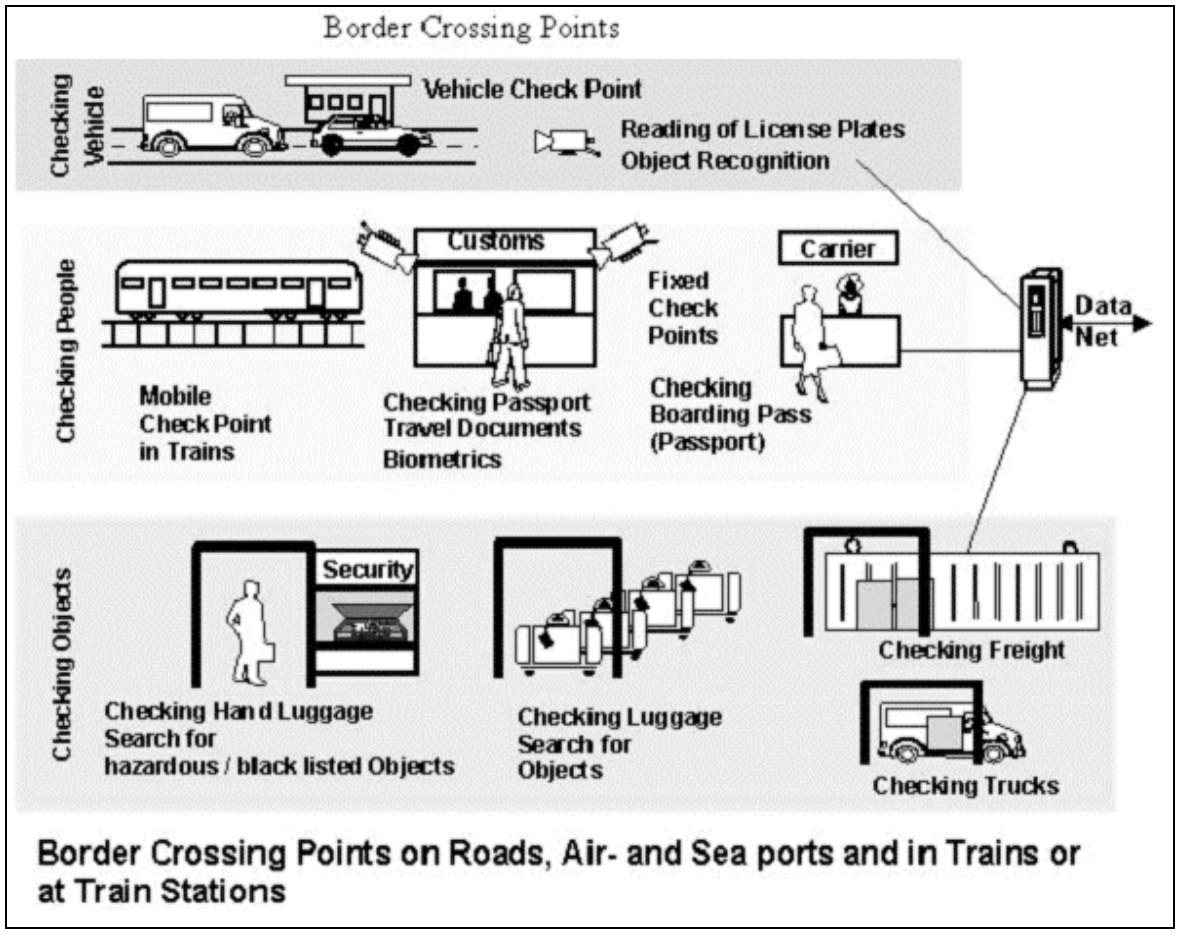

Figure 7: Border Crossing Points.

Border Crossing Points are at the official entries and exits of a country. This can be on land, on roads, in trains or inside the country at train stations, airports and water ports (river Danube).

A Crossing Point has three major tasks:

- To check people (identity and black listed).
- To check goods and luggage.
- To check transportation means (e.g. vehicles or ships).

For people check, passports and travel documents will be controlled. To identify people biometric technologies (fingerprint, iris reading or face identification) will be used. For object checking metal detectors, x-ray systems and other screening equipment is in use (a main player is Heimann, Subsidiary Smith Group, UK). Check of vehicles needs also screening of equipment but in addition license plate reader and object recognition (vehicle identification) are needed. In addition to this, command and control systems, communication systems, and common data basis are needed.

BORDER SURVEILLANCE

Borders are very various. The may be in open land, on mountains, in forest, in rivers or at coastlines. Therefore border surveillance is a very elaborate task. Long distances (hundreds of kilometres) have to be observed constantly. For this there is a need for a large number of land based, air based and sea based surveillance and interception systems.

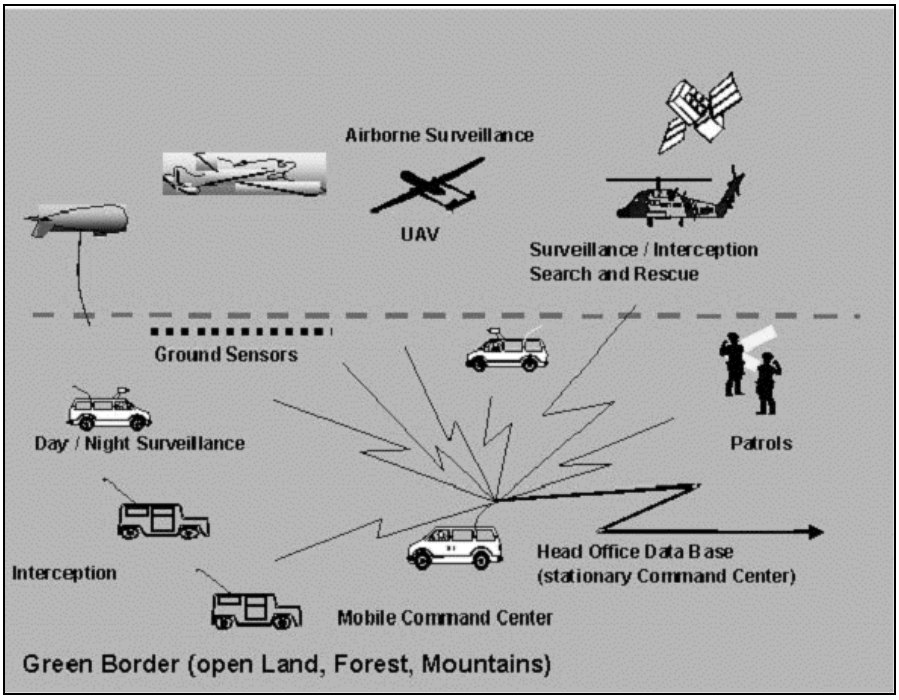

Figure 8: Border Surveillance Systems.

The chart (Figure 8) shows the basic elements of a Border Surveillance System. The main elements are:

- Day / Night Surveillance.
  - Land based sensors for land and water surveillance, infrared for thermal images (IR) and TV sensors (if required radar) mounted on vehicle or stationary.
  - Airborne sensors as IR, TV, Synthetic Aperture Radar (SAR).
- Ground sensors e.g. seismic, photoelectric barrier.
- Interception capability, vehicle, boats.

All surveillance and interception forces are connected by radio links to one of the twenty Country Inspections.

DAY / NIGHT SURVEILLANCE

Land-based surveillance sensors can be employed either stationary or mobile on land based vehicles.

STATIONARY SURVEILLANCE SYSTEMS

Stationary systems are usually on Surveillance Towers with one Thermal Camera and one TV-Camera on a steerable Turntable. This system is connected by a Beam Radio System or a Cable to the next Country Inspection for Image transmission and for steering command transmission for the Turntable. These Towers can be useful at locations where personnel is around, e.g. at border crossings for watching and recording of the traffic. Stationary sensor systems will be well known after a short time by the facilitators and may be avoided or attacked. Therefore stationary sensors should be used only at locations where personnel is around, e.g. at border crossings for watching and recording of the traffic.

MOBILE LAND-BASED SURVEILLANCE SYSTEM (EXAMPLE FROM ZEISS OPTRONIC)

The System consist of:

- One or two Mobile Surveillance Vehicle (MSV).
- One Mobile Command Vehicle (MCV).
- Five or more Interception Vehicle (IV).

The equipment installed into the MSV (Mobile Surveillance Vehicle) functions independently for at least 14 hours with the integrated equipment, a high performance day- and night sight system Thermal Imager and TV. If requested a Radar System can be integrated (Figures 9 and 10).

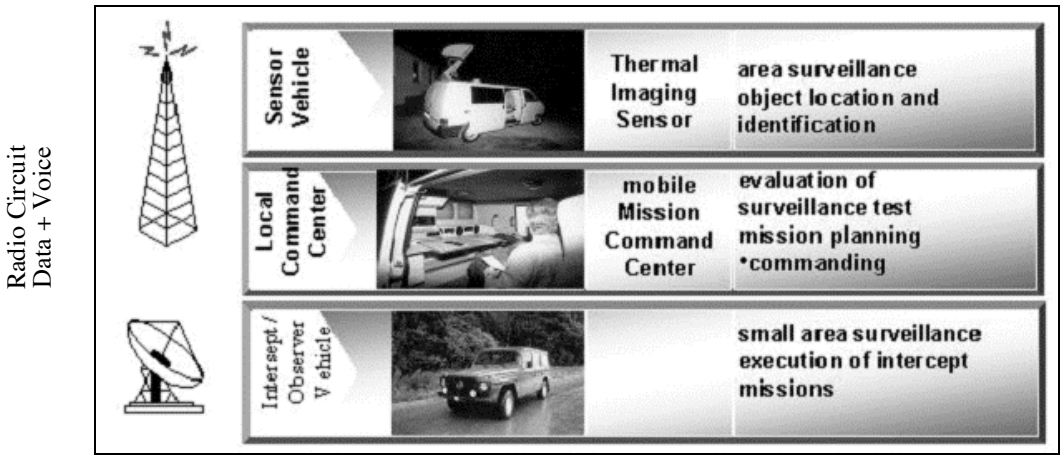

Figure 9: Mobile Surveillance Equipment.

Figure 10: **M**obile **C**ommand **V**ehicle **MCV** (Zeiss Optronics)

TASKS / FUNCTIONS OF A CO-ORDINATION CENTER (COMMAND CENTER)

- Responsible for the day-to-day activities at its border sector.
- Operational control of routine patrols.
- Mission planning.

- Computer aided processing of all incoming / outgoing messages.
- Evaluation and extraction of surveillance results.
- Report of border situation to higher echelons.
- Message display (graphical or digital map), e.g. object and sensor position, tracks, surveillance areas.
- Tracking of surveillance / object information and sensor status.
- Archiving / generation of messages.
- Actualisation of central data storage (by means of manual operation input).
- Interactive object designation and manual correlation of object information.
- Automatic calculation for object cueing / object assignment to sensors.
- Processing of surveillance results, including ”replay” function.

INTERVENTION AND OBSERVATION VEHICLE

Interception capabilities have to be provided for land and for water. For this purpose no special vehicle or boat is required (Figure 11). However for land interception a cross-country vehicle and for interception on water a speedboat should be used.

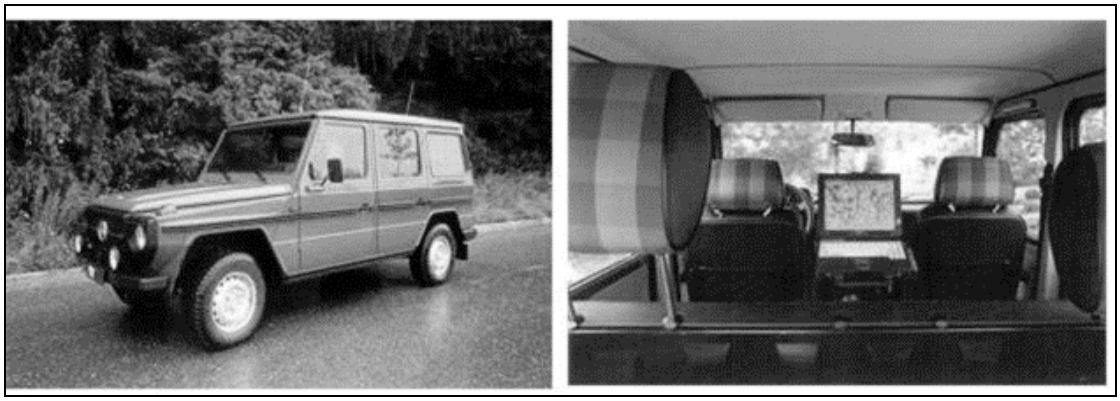

Figure 11: Example of an Observation / Interception Vehicle.

The main tasks are:

- Observation of terrain (autonomously at short range).
- Intercept action.
- Object identification (at short range) and support of object cueing (for others).

- Automated position determination and position messages.
- Manual object observation.
- Computer aided generation and transmission of object messages.
- Receipt and display of object messages (graphically on digital maps).

MOBILE AIRBORNE BORDER SURVEILLANCE

In addition to the sensors used in land based systems (IR, TV) airborne platforms can be used for surveillance of larger areas and to generate an overview situation picture and they are also able to carry a Synthetic Aperture Radar (Figures 12 and 13). This radar delivers a high resolution image, up to 0.3m / pixel and gives all weather capability. These images are very useful for providing clear overview pictures of the situation. The resolution is high enough to recognise vehicles in size and in many cases also the type. In the MTI mode (Moving Target Indication) an estimation of the speed is possible.

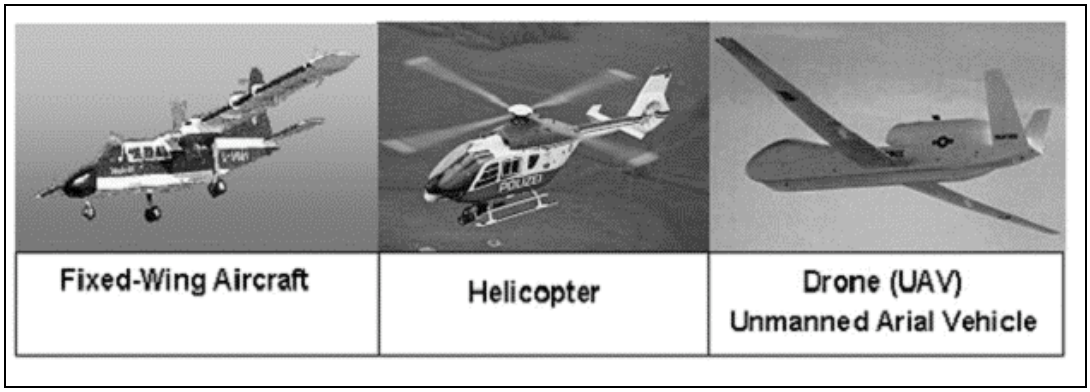

Figure 12: Airborne Border Surveillance.

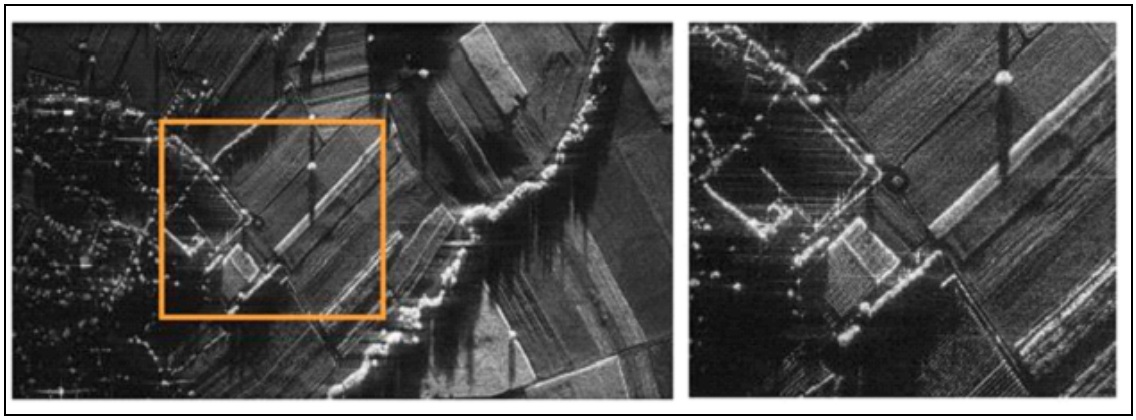

Figure 13: High Resolution SAR Image (0.30m/pixel).

Airborne platforms as fixed-wing aircraft and UAVs are not very practical for border surveillance. They are fast flying and are hardly able to track or follow ground targets

because of their need of large circles for turn around. Useful are helicopter platforms. They are able to "stay" over a target to follow it and transmit continuously position and if required images to a ground station. In addition a helicopter can be used for Search and Rescue Missions.

GROUND SENSORS

There is a broad variety of ground sensors available. Some of them are buried like seismic or electric field measuring sensors; other sensors like photoelectric barriers or light barriers are open installed e.g. on trees or on posts.

These sensors are able to give alarms if anyone crosses the sensor line. But this happens also if animals entering the sensitive field of the sensor. These sensors don't provide any image. In case of an alarm the intervention force has to check or fix installed cameras have to be pre-positioned.

BLUE BORDER SURVEILLANCE

Blue borders are coast lines, rivers, coasts of islands and oil platforms. Many countries have long coastlines (Australia) or a large number of islands (Greek) to protect. At the coast lines the EZZ regulations and international low has to be observed (Figure 14).

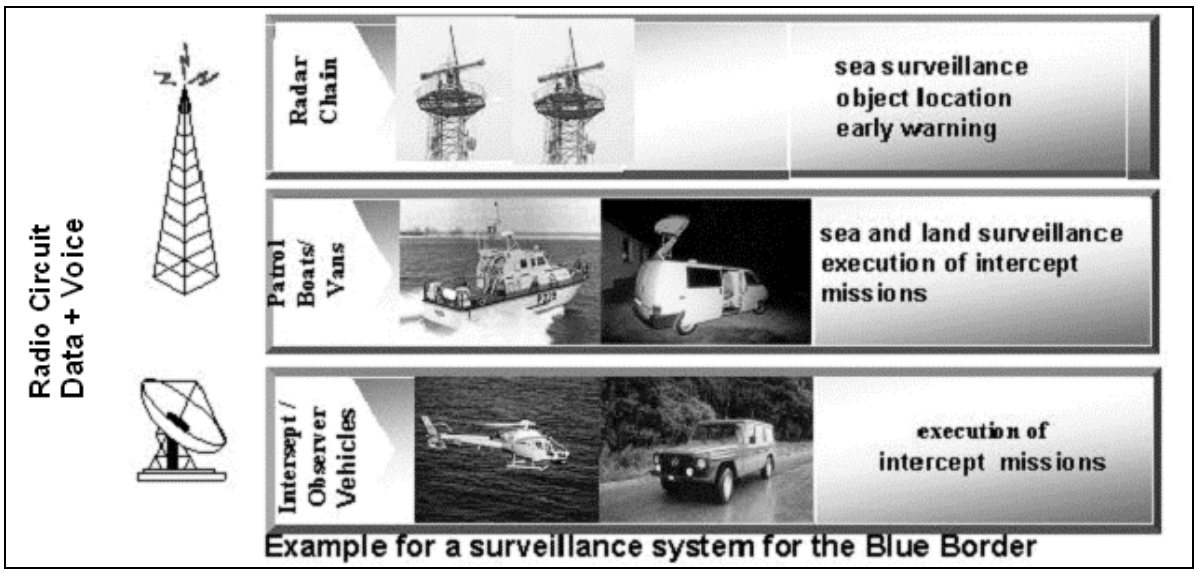

Figure 14: Blue Border Surveillance Systems.

In rivers the borderline generally is situated in the middle, while the riverbanks are mostly accessible by the public, or even inhabited. Therefore there is little room for surveying the area adjacent to the borderline, and a system is required monitoring the border from inside the river or from the own river banks with land-based systems.

For monitoring the river from inside, powerful hydrophobic underwater systems are available. If any target is approaching the sensors, the system provides alarm and information on the target type, but cannot provide much pre-warning time. It must therefore be linked carefully to the local border guard organization on both sides of the border in order to track and apprehend intruders and to prevent commercial and private vessels from ferrying contraband and asylum seekers.

COASTLINE SURVEILLANCE

This is an example foe a coastline surveillance system like Deepwater, a suggestion of industry for Europe (Figure 15). The system could be started as a crenel system from two countries, Germany and France. Later, in steps, other European Countries could join the project.

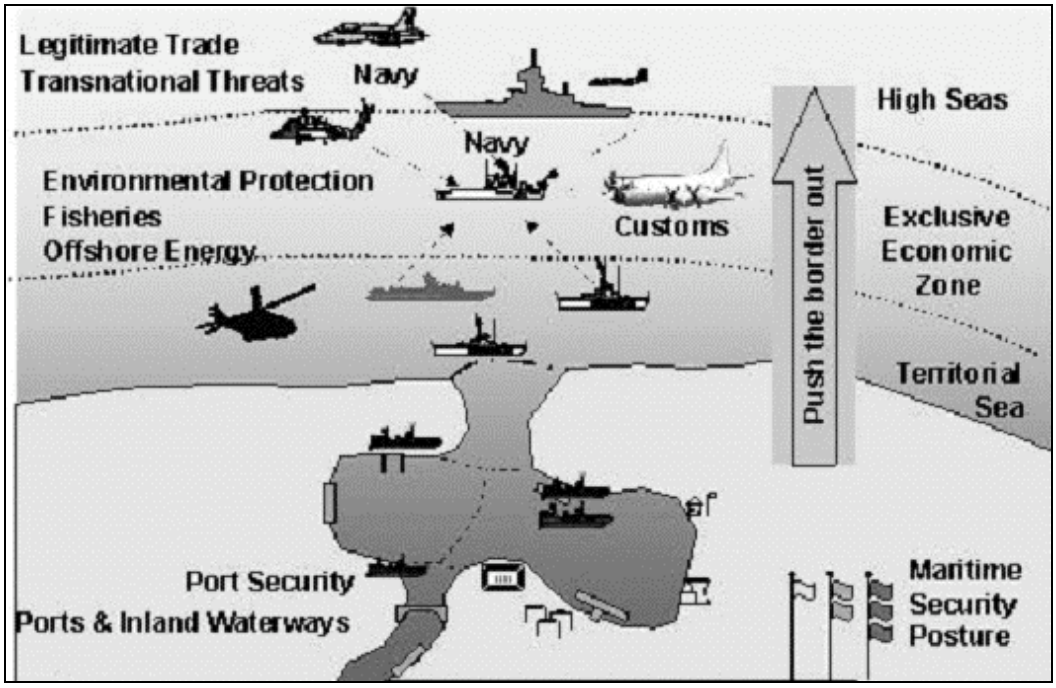

Figure 15: Coastline Surveillance Systems.

The example shows how in this concept the different services can work together. Navy, Border Guard, customs and Port Authorities connected as a Network Centric System (Figure 16).

ANSWERS FROM INDUSTRY

The past has shown that the ”Equipment Approach” not to an overall solution leads, but to a number of technical (”island solutions”) witch are in many times not compatible. A system-based approach, as for the Deep Water project planned, is more efficient.

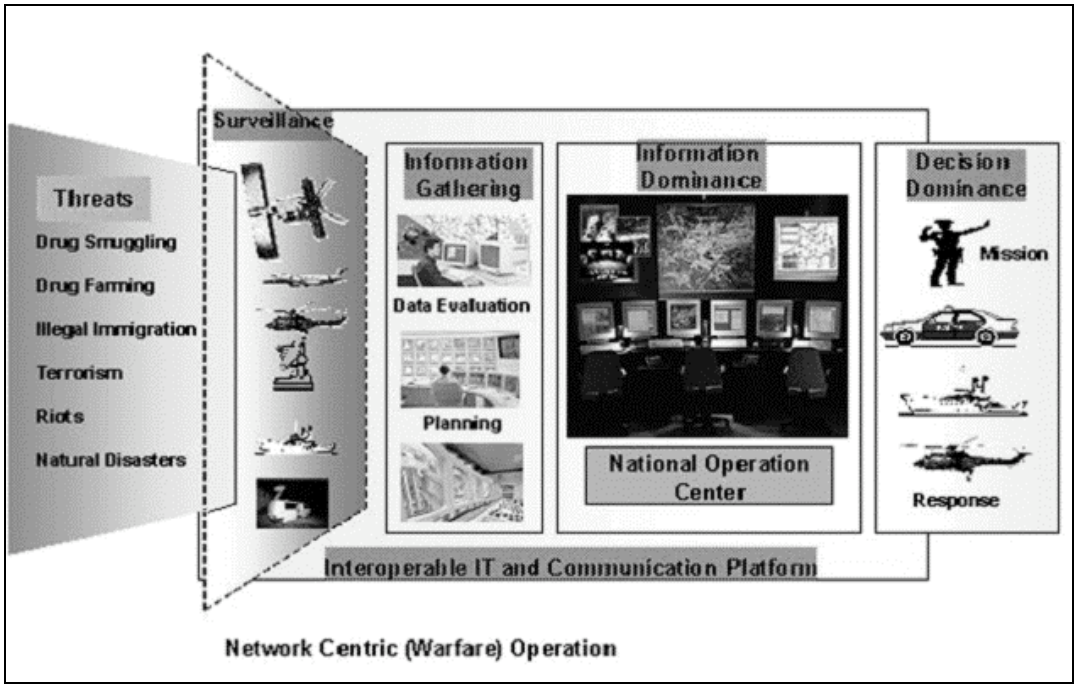

Figure 16: Interoperable IT and Communications Platform.

- First step is a detailed threat analysis. Since the different countries have different locations, neighbors, borders, coastlines, foreigner etc. the threats are also different.

- Second step is the choice of the adequate surveillance equipment.

- Third step choice and layout of the information, evaluation and storage (data base) and access and data handling system.

- Fourth step the layout of the command centers. This has to take into account the e geographical situation, hierarchic structure of the organiation, organisation and cooperation needs with other organisations.

- Fifth step is the choice of the mission equipment.

- During this fife steps, in parallel, an interoperable IT and communication platform has to be designed to ensure a Network Centric Operation.

The next picture (Figure 17) shows an Over All System for Homeland Security. It covers all basic elements as an assortment for the individual needs to overcome the threats.

- Space and Airborne Surveillance.

- Coastal surveillance.

- Checkpoints.

- Interception capabilities.

- Command posts and operation centers.

 The Heart of a Security System are the Operation Centers and at he direct Communication.

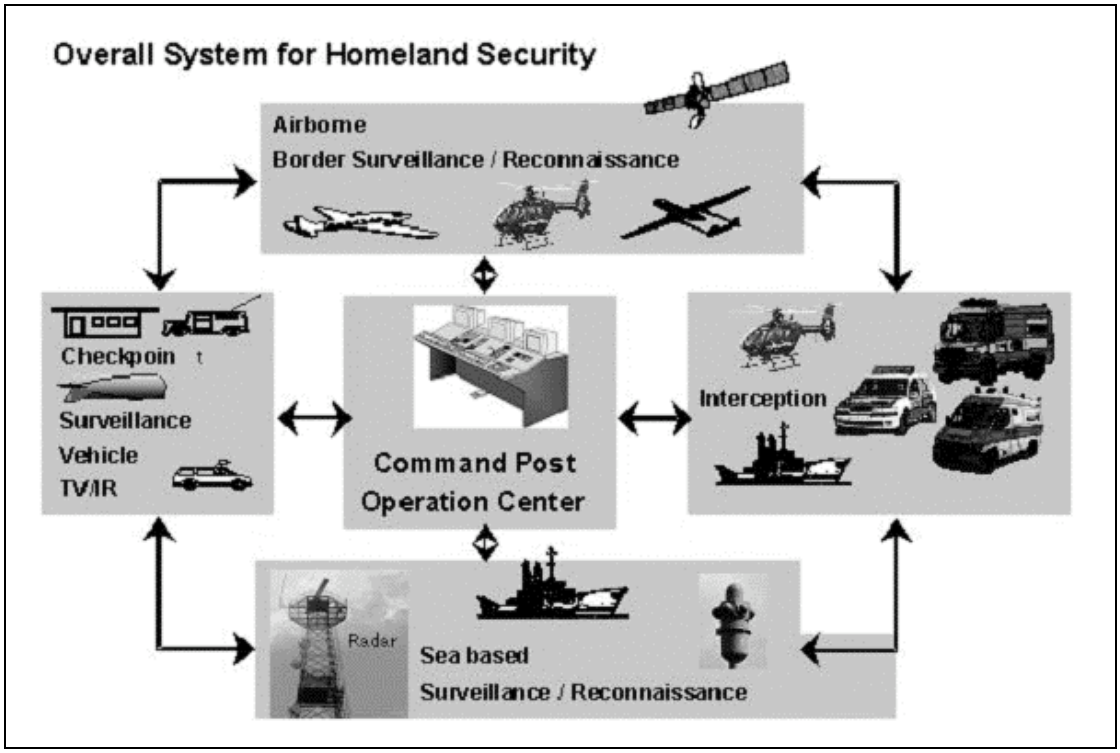

Figure 17: Overall Systems for Homeland Security.

DIGITAL AND ENCRYPTED RADIO NET FOR ALL SECURITY SERVICES

Today most of the communication systems in use with the main security services in Europe, including Germany, are analogues (Figure 18). The main disadvantages of this technology are:

- No point to point communication is possible. Everyone using the same Frequency can listen in to the transmission.
- No encrypting is available.
- The system is easy to disturb.
- The equipment is bulky and heavy.

The TETRAPOL radio communication system has been designed from the beginning to fit Public Safety Users. It is recognised by international bodies and widely deployed on operational networks. This technology includes field proven advantages in terms of radio performance, operational features, and security:

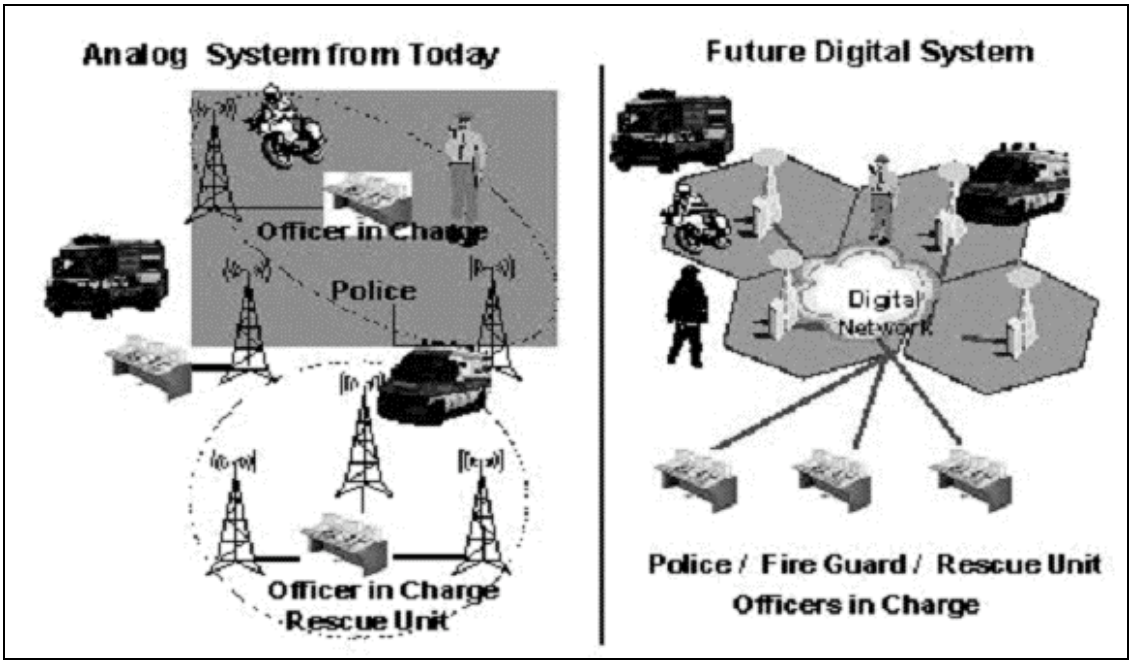

Figure 18: Present Analog Systems and Future Digital Systems.

- Provides a comprehensive range of voice and data services which enable users to enhance their operational efficiency in the field.
- Optimises the use of radio resources.
- Flexible architecture adapts to any administrative structure and allows a progressive network deployment.
- End to end encryption.
- Transmission of voice and data.

IP backbone provides the Customer with benefits like convergence between communication and information systems, improvement of availability due to intrinsic re-routing mechanisms around failed nodes, single type of connection, which is Ethernet and open interfaces. TETRAPOL is in use already in France, Spain, Switzerland, Czech Republic, Slovakia and Romania.

CONCLUSION

Industrial Countries have reacted to asymmetric Threat, Germany (Budget increases); Ministry of Interior has reacted by Increase of Personal (e.g. Sky Marshals, Border Police), Industry is ready to act, e.g. Security Concept for World Cup 2006. The Implementation of the Digital Communication System MPK in June 2003 is a first Step to improve Security.