Study on the Competitiveness of the EU security industry

Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054

Final Report

Client: Directorate-General Enterprise & Industry

In collaboration with

DECISION Etudes & Conseil

TNO

Brussels, 15 November 2009

Disclaimer: The views and propositions expressed herein are those of the experts and do not necessarily represent any official view of the European Commission or any other organisations mentioned in the Report

ECORYS SCS Group
P.O. Box 4175
3006 AD Rotterdam
Watermanweg 44
3067 GG Rotterdam
The Netherlands

T +31 (0)10 453 88 16
F +31 (0)10 453 07 68
E fwc-scs@ecorys.com
W www.ecorys.com
Registration no. 24316726

ECORYS Macro & Sector Policies
T +31 (0)31 (0)10 453 87 53
F +31 (0)10 452 36 60

Preface

This Final Report has been produced as part of the study "Study on the competitiveness of the EU security industry" commissioned by European Commission Directorate-General Enterprise and Industry, within the context of the Framework Contract on Sector Competitiveness Studies (ENTR/06/054).

The report responds to the original technical specifications for the study and the methodology and scope as set out in the Consortium's initial proposal and workplan, as agreed and discussed with the client. As set out in the Task Specifications, the main purpose of the study is the understanding of the competitive position of the security industry, the main factors influencing its competitive performance, and the reflection on potential policy options to support the development of the security industry in Europe.

The Final Report is divided into two parts: Part A provides a general assessment of the security sector as well as a set of policy recommendations; while Part B describes the main findings emerging from the analysis of the specific segments – which were selected in consultation with the client and the study monitoring committee.

It should be noted that in addition to the normal difficulties associated with obtaining information that may be commercially sensitive, the specific nature of the security sector (from both a demand and supply perspective) presents an additional constraint to the availability of 'in-depth' information and data. In addition, the frequently fragmented nature of markets for security products and services, and often the supply of these products and services also, is a further difficulty for developing a coherent picture of the security sector in Europe.

The information and analysis presented in the report is based on a combination of desk research and consultations with relevant stakeholders from the security sector itself, from users of security equipment and systems, and from relevant policy-related and regulatory institutions. We would like to express our gratitude to all persons and organisations that provided information and valuable insights to the study.

The analysis contained in the report has been undertaken by a team of consultants from ECORYS NL, DECISION Études et Conseil and TNO.

Table of contents

Executive summary

Introduction

The Final Report of the study of the "Competitiveness of the EU security industry" sets out to provide a picture of the current situation of the EU security industry, its structure and organisation, competitiveness position and challenges for the future. The study represents, perhaps, the first attempt to provide a coherent economic analysis of the security industry at the level of the EU. In this regard, the objectives set for the study were ambitious, particularly in view of the absence of existing relevant analysis of the EU security industry, the lack of statistical data on the industry and markets, and even more fundamentally on the definition of security itself. This is reflected in the overall approach adopted for the study, which is based on a general assessment of the EU security industry combined with more detailed analysis of specific segments seen as important given current EU security priorities. Accordingly, though the study cannot be considered comprehensive, it provides a widely representative assessment of the EU security industry enabling a broad range of policy issues and potential responses to be identified.

General scope and perimeters of the security sector

In terms of recognised classifications of industrial activities, the security industry is neither well defined nor clearly identifiable. In fact, the production and supply of security-related equipment and systems, services and applications, may be found under a wide range of industry and services headings that cover both non-security and security-related activities. More fundamentally, underlying concepts of what constitutes 'security' and, in turn, the scope and perimeters of the security industry and market are highly amorphous. This can be attributed, on the one hand, to the fact that the nature of actual and perceived security threats and concerns can differ widely depending on by whom and at what level of 'society' they are evaluated. On the other hand, the nature of threats and perceptions of their seriousness change over time.

Taking into consideration the nature of security threats and priorities, and demand and supply-side characteristics, Figure 1 provides a general overview of the security market as developed within this study. Underlying this Figure, we make a general distinction between two different security threat categories:

- **'Traditional' security**, corresponding to protection against ('endogenous') threats such as 'ordinary' criminal activity, fire protection, etc.
- **'New' security**, corresponds to protection against ('exogenous') threats such as terrorism, organised crime, cyber crime, etc. and also including protection against and response to major catastrophic events.

In terms of a general categorisation of demand-side security 'responsibilities' two distinctions are made: first between 'external' and 'internal' security dimensions and, secondly, between 'civil' and 'private' security responsibilities. These are translated into four main institutional demand segments:

- **Defence (military) support for internal security:** e.g. support in the event of a major crisis incident;
- **Civil security (i.e. public sector non-military administrations):** e.g. counter terrorism, law enforcement, civil order, emergency response, etc.;
- **Mixed public-private sector security:** e.g. critical infrastructure and utilities etc.;
- **Private sector security:** for which a differentiation may be made on the basis of the degree of potential vulnerability to 'new' security threats (i.e. high risk versus low risk activities/sectors).

From a supply-side perspective, three main segments of the security industry are identified:

- **Traditional security industry**: based around the supply of general security applications (e.g. physical access control, intrusion and fire detection, CCTV/video surveillance, etc.) corresponding primarily to protection against 'traditional' security but that, nonetheless, can be an integral part of overall responses to 'new' security threats.
- **Security-orientated defence industry:** based on either the application of defence-related technologies in the area of security or where defence-orientated companies have acquired and/or adapted 'civilian' technologies in order to address capability requirements within security markets. This corresponds primarily to protection against 'new' security threats.
- **New entrants:** for which a distinction may be made between:
  - Suppliers from other civilian industry sectors whose security products tend to be based on the extension of existing (civilian) technologies to security applications;
  - Start-up companies based on the development and commercialisation of new and innovative security technologies.

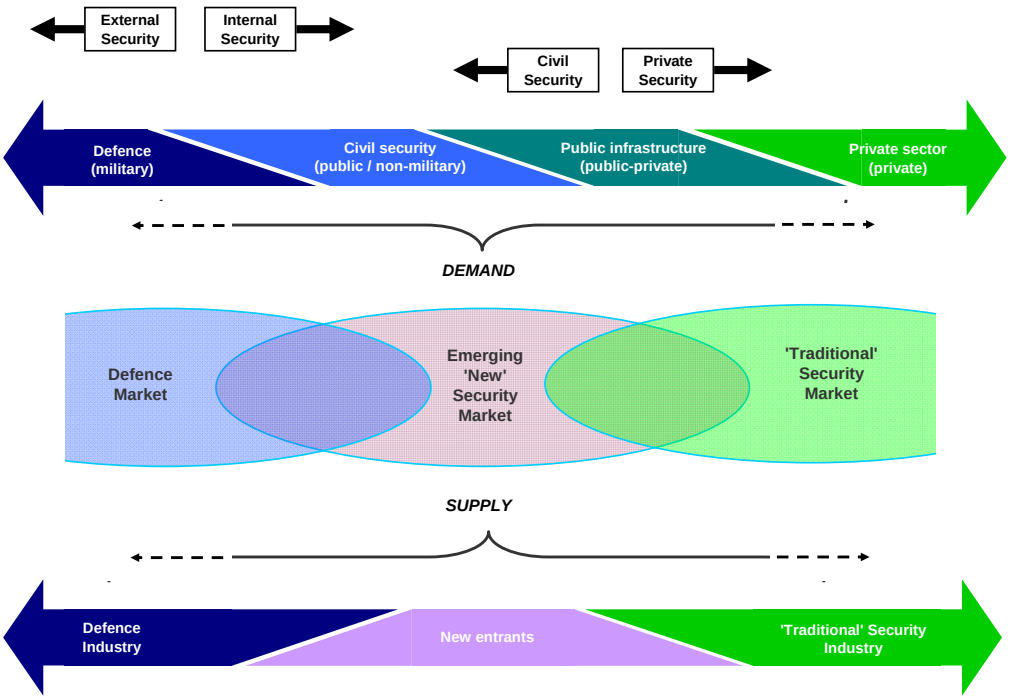
Combining these elements, we arrive at the following market segmentation:

- **'Traditional' security market:** for which supply tends to be broad-based with a high level of transferability of security technologies and equipment across different markets segments (i.e. fairly standardised products). Because of the relatively standardised nature of products, these markets are *prima facie* usually fairly open to competition. However, it is often the case that the logic of 'mass' production applies and economies of scale become an important determining factor in competitive performance. Although production may be highly concentrated, distribution networks – at global and local levels – for these products can be very fragmented.
- **Defence market:** which acknowledges the role of defence forces (military) support for internal security[1].

[1] Note, the defence (military) market is excluded from the overall scope of this study.

- **Emerging 'new' security market:** for which demand is often characterised by a limited number of actors (customers) present in the market, with requirements in terms of security capabilities that can be quite highly specified. In many cases it is national governments and administrations that are *de facto* the ultimate customer for security equipment or they define the shape and structure of demand through security-related regulations (e.g. critical infrastructure protection, border management, or secure communication and biometric identification systems for governmental institutions). The combination of a limited number of customers and the specificity of demand tends to be matched by a corresponding concentration in the supply of security equipment.

Figure 1 Overview of the security market: supply and demand characterisation



As a general point, it is important to note that the boundaries between the different segments identified above are often not clearly defined. From a demand perspective, there can often be overlap (or ambiguity) in terms of the allocation of security responsibilities and the role of different demanders of security products or services. On the supply side we have seen, for example, the acquisition of primarily civilian technology suppliers by defence industry companies thus blurring the distinction between defence and security. At the same time, 'new' security threats have both raised demand for traditional security products and led them to acquire or develop new technologies, such that a clear separation cannot be made between the 'traditional' security industry and a 'new' security industry.

Overall, in relation particularly to 'new' security threats and priorities, the security industry is immature, having developed largely over the last decade or so. Consequently, it is not as yet well structured and often clear distinctions cannot be made between, for example, the security and defence industries, or between 'traditional' and 'new' security

segments. By and large, it appears that the security industry is still in a process of formation and the pattern of merger and acquisition (M&A) activity observed in the recent past suggest that there is still some way to go before a clear and relatively stable shape of its industrial structure is established.

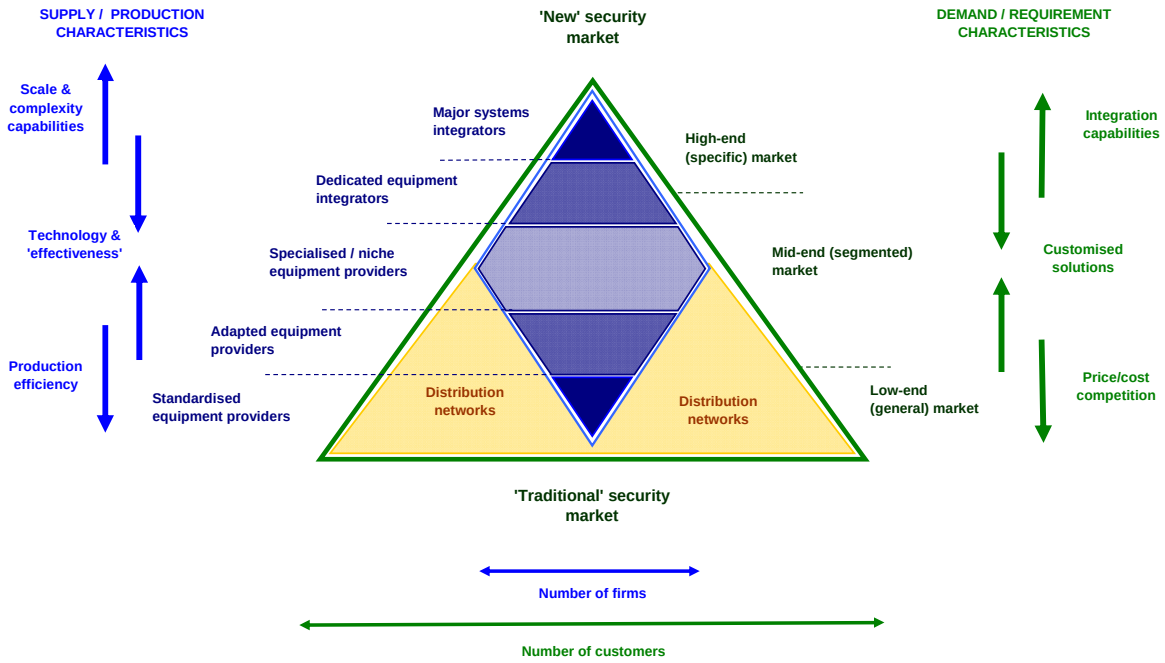
Notwithstanding the lack of maturity and clear structure of the security industry, it is possible to provide a general characterisation of supply (and demand) of security equipment and systems as shown in Figure 2. In terms of the general structure of supply, this is strongly influenced by the structure and characteristics of demand, combined with the overall regulatory environment, which contributes to creating an environment in which there can be very high barriers to market entry, particularly at the 'high-end' of the 'new' security market. These barriers relate notably to:

- High investment costs associated with technology development and, also, with the transition from technology development to placing a product on the market;
- High costs associated with securing markets (e.g. lobbying, marketing, commercial diplomacy). An important aspect to this is related to needs to 'educate' clients on technological possibilities and choices.

A consequence of the high barriers to market entry is that SMEs typically play only a limited role in the security market and are often restricted to highly specialised 'niche' segments. Where SMEs are able to successfully develop innovative technologies it is usually the case that – as a result of the high barriers to entry noted above – they tend to license this technology to larger players (e.g. dedicated equipment integrators) rather than try to enter markets independently; alternatively they may simply be acquired by such players.

In addition to the barriers noted above, there are a number of trends shaping and structuring demand for security equipment and systems that are leading to larger and more integrated security contracts/projects. Such developments would appear to strengthen the position of the major systems integrators (vis-à-vis dedicated equipment integrators) whose strengths lie in ensuring the effective integration of different security systems and customising security systems to meet client requirements. A possible consequence in the longer run could be further consolidation in the future among dedicated security equipment and sub-systems providers.

Figure 2 Characterisation of security equipment supply and demand



Market size estimates for the security sector

Notwithstanding issues related to the definition of the scope of the security sector, a number of difficulties limit the possibility to obtain estimates of the size of the security industry. As mentioned, the security industry is not identifiable from available sources of industrial statistics and, moreover, there is no source of statistical data available at a European level from the industry itself. Moreover, from a supply-side perspective, procurers of security equipment and systems can be reluctant to provide information on security expenditures. Against this background, the study has only been able to offer approximate estimates of the size of security markets at a global and European level and, even here, only for a number of key market segments.

Drawing on existing market report estimates and consultations with industry representatives, a 'consensus' view is that the global security market is worth some €100bn (2008 figure) with around 2 million persons employed worldwide in the security sector. Concerning the European security market, our approach is to provide an indicative range of the size of main security market segments. These estimates suggest a market value within the EU that is in the range of €26bn to €36.5bn (2008 figure).

Table 1 provides a breakdown of the global security market by market segment, and range estimates for the EU security market. From a global perspective, North America (mainly the US) is the largest security market, with a current market share of around 40% or more. Europe is ranked 2nd in the global security market, with a market share ranging approximately from 25% to 35%. Despite the financial crisis, global demand for security equipment is expected to grow at a minimum of around 5% per annum, with the fastest growth in coming years expected to be mainly in Asia and the Middle-East.

Table 1 Relative market size of the global and European security industry markets (indicative € estimates by sector)

SECURITY INDUSTRY			
Sectors	***EU** security market (low estimate)*	***EU** security market (high estimate)*	***Global** security market estimate*
Aviation security	€ 1.5 bn	€ 2.5 bn	€ 5.2 bn
Maritime security	€ 1.5 bn	€ 2.5 bn	€ 6.7 bn
Border security	€ 4.5 bn	€ 5.5 bn	€ 9.9 bn
Critical infrastructure protection	€ 2.5 bn	€ 3.5 bn	€ 12.6 bn
Counter-terror intelligence	€ 4.5 bn	€ 5 bn	€ 19.4 bn
Physical security protection*	€ 10 bn	€ 15 bn	€ 39.2 bn
Protective clothing (first responders)	€1.5 bn	€ 2.5 bn	€10 bn
TOTAL MARKET SIZE	**€ 26bn**	**€ 36.5 bn**	**€ 103 bn**
** It includes CCTV, access control equipment, intrusion and detection systems, etc.*			

Source: ECORYS (2009)

In terms of the repartition of the market according to the importance of public versus private sector demand, Figure 2.3 represents the different sectors of the European security market, taking into account the relative level of spending of both the public and the private sector (horizontal axis) and their consideration as 'traditional' or 'new' security markets (vertical axis). The relative market value estimate of each of the sectors is represented by the size of the coloured spheres.

Figure 3 Public-private involvement in 'traditional' and 'new' security markets

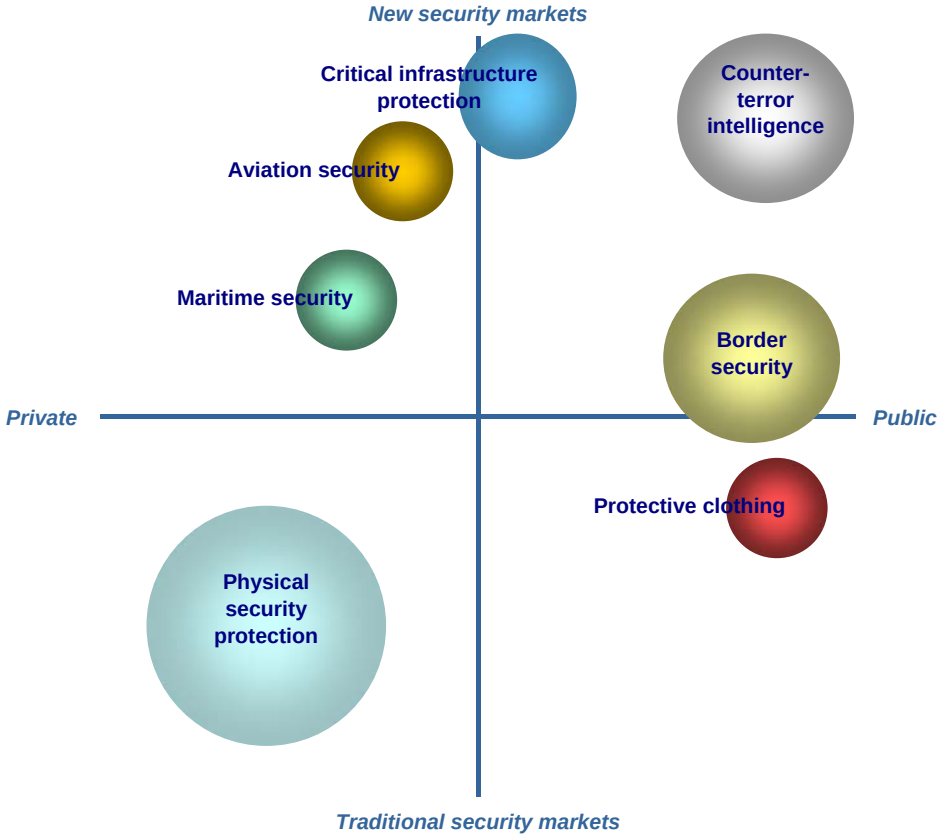


Figure 2.3 shows, among the segments covered, the predominance of physical security protection as the largest market sector[2] in the EU and its importance both in the traditional security market and in the involvement of the private sector as a main purchaser of equipment (CCTV, intrusion and fire detection, access control, etc.) New security markets, such as critical infrastructure protection, counter-terror intelligence and aviation security are expected to be the fastest growing markets.

Competitiveness assessment of selected EU security industry segments

Taking account of the limited availability of existing information on the security industry within the EU and the absence of analysis of the industry's competitive position and performance, the approach adopted by the study was to focus its analysis on 6 segments of the security industry that were considered to be of particular relevance given current security policy priorities. The selected segments are:

- **Air transport of goods (cargo)**: Detection and identification of dangerous or hazardous goods and materials for secure air (cargo) transport;
- **Maritime transport of goods (cargo)**:Tracking and tracing of goods (and ships) for secure maritime transport;
- **CBRNE**: Detection of chemical, biological, radiological, nuclear and explosive substances (other than covered under 'air transport of goods');
- **Biometrics**: Biometric solutions for entrance / barrier control of protected areas, buildings or events;
- **Secure communications**: Secure, mobile, ad-hoc communication systems for operations in case of incident, crisis, disaster or event;
- **Protective clothing**: Protective and intelligent textiles and clothing for dangerous tasks of first responders.

An overview of the analysed segments is provided in Table 2[3]. The general picture that emerges is that the EU occupies a fairly strong position in the various segments analysed. Nonetheless, despite the fact that some of the large EU based companies enjoy strong and world leading positions in a number of the analysed security segments (e.g. cargo screening, biometrics, secure communications), the depth of the EU industry beyond these key players often seems relatively limited. In this respect, it is perhaps important that the apparent success of a few EU companies should not mask potential weaknesses in the underlying competitiveness of the EU security sector.

Drawing on the findings of the segment analysis and, also, a broader assessment of the security industry in Europe, Table 3 provides an overall SWOT analysis of the European security industry.

[2] It is important to note that security of IT infrastructure and systems *per se* is not covered by these estimates. Although a significant part of expenditures can be IT related; for example, particularly in Counter-terror intelligence for which a high proportion of expenditures are IT related.

[3] Detailed analysis of each segment is contained in Part B of this Report. The analysis covers a description of the segment and supply/value chains, key market developments, regulatory frameworks (and other framework conditions), together with an assessment of EU competitiveness situation and position on global markets.

Table 2 Overview of market characteristics for specific equipment segments

OVERVIEW ANALYSIS BY EQUIPMENT MARKET SEGMENT			
	Aviation security	***Maritime security***	***CBRNE***
Analysed equipment segment	Air cargo security	Tracking and tracing devices	Detection and tracing of CBRNE substances
Demand and market trends	Demand is mainly driven by terrorism and related regulatory requirements. Overall demand also influenced by economic conditions (i.e. volume of cargo transported). Obtaining adequate detection capabilities (effectiveness) with required throughput (efficiency) is a key technology driver.	Underlying demand based on supply chain monitoring and optimisation. Increased demand is driven by the protection of the supply chain from terrorism, illegal transportation of goods as well as from new security policies and legislation to increase maritime security.	Demand is mainly driven by terrorism and related regulatory requirements. Key demand segments include airports, critical infrastructures, high profile facilities, etc.
Market (supply) structure	Supply of equipment concentrated among a few international players. Limited number of upstream suppliers of sophisticated components / equipment sub-systems	Relatively diverse equipment suppliers (reflecting main shipping nations). More concentration in data management and systems integration.	Supply of equipment concentrated among a few international players. Limited number of upstream suppliers of sophisticated components / equipment sub-systems
Supply position of EU industry	Strong EU leaders in the global scene. EU position also strengthened by recent takeovers in the market. Lead companies maintain significant manufacturing activities in Europe (mainly in Germany and UK). Main competition from US, also increasing presence of China	Relatively strong EU position worldwide in the supply of new integrated systems (i.e. LRIT). Market for data management systems and tracking devices is dominated by US companies.	Strong EU leader in the global market. EU position also strengthened by recent takeovers. Majority of companies active in this market segment are based in the US.
Competitiveness assessment	Strong position of leading EU companies (and technology development) but limited depth of EU capabilities beyond the main players. EU position handicapped by market fragmentation (e.g. national security regulations, standards and procurement systems).	Strong added value of the EU industry in new integrated systems but remaining threat of outsourcing production and R&D outside Europe. EU position can also be hindered by increased costs due to new regulations and solutions.	Fragmented EU industry in the absence of coordinated policies and inter-industry standards. European companies are increasingly supplying outside the EU (e.g. Asia. Middle East) but market access to the US (biggest market) can be problematic.
EU market position	Some strong EU companies among the leading global players but otherwise weak	Some relatively strong EU global players but potential threat from low cost competitors as technologies mature	Some strong EU companies among the leading global players but otherwise weak

Table 2 Overview of market characteristics for specific equipment segments (continued)

OVERVIEW ANALYSIS BY EQUIPMENT TECHNOLOGY SEGMENT			
	Biometrics	***Secure Communications***	***Protective clothing***
Analysed equipment segment	Large scale / High-end biometric solutions for access control and identification	Large government communication systems	Protective clothing for first responders
Demand and market trends	Demand is driven by increased security needs in both public and commercial markets. Differences in societal acceptance influence overall demand and technology utilisation. The EU seems characterised by lower acceptance of biometric technologies than the US.	Demand is driven by requirements of large governmental systems (police forces, etc.), as well as by a 'technology push' model and standardisation. The PMR market is highly influenced by national structures (centralised market in France vs decentralised market in US).	Underlying demand driven by number of first responder personnel; implies mainly a 'replacement market' with limited demand growth. Fragmented demand side due to variety of risks and multiple purchasing public entities.
Market (supply) structure	High end segments are concentrated among a few leading global suppliers. Component supply structure is more diverse but mainly European, US or Japanese	High-end segments characterised by limited number of players; but wider range for low end applications. Large systems integrators have increased involvement through acquisition of PMR activities mainstream telecom equipment suppliers.	Presence of a large number of players (garments), serving a diverse range of industries and services. Companies are normally focusing on niche markets. Upstream (fibres and fabrics) more concentrated.
Supply position of EU industry	Majority of suppliers are localised in the US (largest market) with the European supply chain having few (but relevant) players in the high-end biometric solutions segment (with EU companies accounting for 50% of global market share in high-end solutions), as well as SMEs and mid-size players in Germany and UK.	EU players are exclusively competing in the high-end segment of the PMR market, with worldwide leadership in high-end governmental applications. US is the global world leader across commercial and governmental applications. Possible challenge from low-cost (Asian) competitors.	Differing position of EU companies in the global market depending on their level in the supply chain. Most fibres produced by global chemical companies with limited direct connection to security. Fabric and garments tend to be fairly localised with limited international competition.
Competitiveness assessment	EU market fragmented and fragile, due to lack of specific regulation and standardisation at EU level to foster demand. US regulatory initiatives, certification and standard bodies have become world references for the entire industry.	An adequate standardisation policy and homogenisation of national markets would permit the EU to remain strongly competitive due to its already good position and leadership in mobile and secure communications.	Strong global position in the fabric and garment market, with EU companies being innovative. However, EU market for garments is very fragmented. EU high-end quality companies may be threatened by illegal copying from the Far East.
EU market position	EU is home to leading EU players in the global scene, but US remains the dominant market	Relatively strong (leadership in mobile and secure communications)	Medium

Table 3 SWOT analysis of the European Security Industry

SWOT ANALYSIS OF THE EUROPEAN SECURITY INDUSTRY & MARKET ENVIRONMENT	
Strengths	***Weaknesses***
▪ EU companies among the global leaders in many security technology/application domains.	▪ Limited depth of EU security industrial base. ▪ Potential vulnerability of SME due both to high market entry barriers and potential international competition. ▪ Low level of EU industry organisation and cooperation. ▪ Low international presence and cooperation (with exception of a few main companies).
▪ Increased public (including EU-level) funding for security-related research, technology development and innovation.	▪ Low aggregate level of EU funding for security-related research, technology development and innovation (i.e. relative to USA). ▪ Conservative EU approach to adoption of new security technologies and solutions. ▪ The size of the security market alone may be insufficient to offset the investment in research and technology development or to achieve the scale of production necessary to remain competitive in the production of specialised components and sub-systems.
▪ Strong EU position in related/enabling sectors (e.g. aerospace, defence, space, telecoms, health).	▪ ICT (security) dominated by American and Asian players. ▪ Component supply located outside EU.
▪ Large overall size of EU market. ▪ Leading EU position in key market segments (e.g. civil security and emergency response, border control, maritime, aviation, land transport, distribution & logistics, etc.) ▪ Variety of market conditions (e.g. multicultural environments, sophistication of end markets, resource levels and funding).	▪ The relative size and growth of the US market and the preference of national administrations for local suppliers – US companies as main global leaders. ▪ Slow growth of EU market compared to other regions. ▪ Uncertainty over allocation of security responsibilities (EU vs. MS, public vs. private provision, civil vs. defence). ▪ Lack of awareness of security procurers and users (e.g. concerning capability requirements and technology needs). ▪ Market fragmentation issues: - Low level of common EU approach to security issues, policy, and regulations; - Lack of common EU approaches to procurement of security systems and services; - Lack of common EU security standards; - Lack of common EU infrastructure for approvals, certification etc.

Table 3 SWOT analysis of the European Security Industry (continued)

SWOT ANALYSIS OF THE EUROPEAN SECURITY INDUSTRY & MARKET ENVIRONMENT	
Opportunities	***Threats***
▪ Increased market requirements for integrated security solutions and interoperability/interconnectivity (i.e. favouring EU expertise in systems integration). ▪ Increasing size in individual security projects with sufficient flexibility to integrate additional capabilities as new threats arise. ▪ New markets emerging from increasing identification needs (for instance, against fraud or terrorism) and online security for e-business will foster development of commercial applications.	▪ Low prioritisation of security within the EU, in general, and at MS level (notably government administrations) combined with constraints on public expenditures may lead low purchase rates for security equipment. ▪ Increasingly high market entry barriers reduce attractiveness of security markets to new entrants and discourage innovation. ▪ Potential exclusion of SMEs from security market for large integrated security projects.
▪ Increasing sophistication of security capability requirements, promotes 'high-end' / 'high value-added' security equipment and systems solutions. ▪ Increasing demand for automated systems requiring less (or more sophisticated) human intervention raises demand for security equipment and systems (relative to security personnel). ▪ Increasing value added of security equipment and systems generated by 'soft' elements (software, data management, processing algorithms, etc.)	▪ Generalisation of security equipment, systems and technologies promotes price/cost-based competition and favours non-EU based low-cost suppliers, or results in relocation of EU-based production to low-cost regions. ▪ Domination of US suppliers and increasing technological sophistication of Asian suppliers – due to larger/increasing home market demand and support for R&D and innovation – raises their relative competitiveness vis-à-vis EU-based suppliers.
▪ Growing international (global) markets for security equipment and systems. ▪ Investing in production facilities in other regions of the world, taking advantage of lower production costs, subject to maintaining the integrity of their control over core production processes.	▪ National preferences and explicit or implicit market access barriers that restrict EU suppliers from competing in international markets. ▪ Economic slowdown and adverse macro-economic conditions could moderate the pace of this growth to some degree. ▪ Outsourcing or the relocation of final assembly activities to low cost locations.
▪ Improved cooperation between regulators, end-users, industrial suppliers and industry fosters innovative approaches and adoption of new technological approaches. ▪ Adaptation of existing and new technological capabilities for applications in the security field (e.g. nanotechnologies for PPE, etc.) ▪ Strengthening of infrastructure for testing, validation, and optimisation of new technological concepts for specific security domains (e.g. field-labs for first responder equipment, forensics, surveillance systems, etc.) stimulates product development and innovation.	▪ EU procurers and users maintain a conservative attitude to the adoption of new technological solutions, thus slowing down their take-up and implementation.
▪ Better IPR enforcement, fostering the interest of companies to be involved in the development of new technologies as early as possible.	▪ The position of EU high-end quality companies might be threatened by the undermining of technology investments by illegal copying, etc.
▪ Greater EU-level cooperation on development and adoption of common security standards and approvals/certification systems. Eventually leading to adoption of EU-based standards international markets to the advantage of EU suppliers. ▪ EU legislation aiming to develop a standardisation framework across all Member States, which would be likely to heighten overall demand for security equipment	▪ US dominance of security supply, creates *de facto* US-based global security standards ▪ Simpler and better developed system for standardisation of security systems and technologies in the US - and a more focussed stimulation of technological innovation for security – supports *de facto* US-based global security standards
▪ Addressing public concerns (e.g. societal issues) stimulates innovation and creates new market opportunities.	▪ Reduced public acceptance of security measures and intrusiveness of security systems etc. and public concerns about preservation of individual rights. ▪ Additional costs associated with addressing public concerns within EU reduce cost competitiveness of EU security solutions

Security market developments and implications for the EU security industry

Main drivers of the security market

The main drivers of overall demand levels in markets for security equipment and systems may be summarised as follows:

- **General economic conditions.** The overall demand for security 'capacity' and, in turn, the security equipment and systems required to deliver this 'capacity' are linked to the overall level of economic activity.
- **Security threat perceptions.** Changes in the *modus operandi* of terrorists, of organised crime, or the occurrence of 'new types' of catastrophic events/crises are major drivers of both the overall level of demand for security equipment and, also, for the types of security capabilities and solutions required by the market. In this respect, the market is largely reactive, with demand responding to specific events that highlight specific security threats. Demand may respond extremely rapidly to a new 'event' but this may be also followed by a relatively rapid decline as threat perceptions diminish. This pattern of 'reactive' demand is foreseeable but, since specific 'events' are by their nature largely unpredictable, the pattern of demand over time can be extremely uncertain.
- **Regulatory frameworks and governmental responses.** While also a response to changes in security perceptions, legislation and regulations setting out security requirements and obligations play a strong role in shaping demand for security products and services. At a most basic level, regulations may serve to set minimum security requirements within the relevant market segments to which they relate. More broadly, they may also serve to set out a 'roadmap' for development of security requirements over time.
- **Technology development.** Technology is a major driver of the development of the security industry. The sector is characterised by proprietary technologies that are a crucial element for the competitive position of companies[4]. Technological development and innovation are not only a response to market requirements but can also serve to stimulate new demand and create new markets.

Changes in the demand for security equipment and systems

Among the main factors determining the shape and structure of demand, the following may be noted:

- **Adoption of integrated approaches to security.** The move towards more integrated approaches to addressing security risks can be seen, for example, in the adoption of supply-chain security approaches based on a more holistic view of the chain of custody throughout the chain. At another level, it is reflected in 'systems of systems' approaches to the integration of security capabilities and corresponding equipment requirements.

[4] In may be noted that, in common with other sectors with a high technology focus, protection of intellectual property is a major concern for the sector. Clearly, also, there is a public policy aspect involved in the protection of intellectual property in terms of ensuring that information on technology capabilities do not fall into the hands of terrorists, organised crime, etc.

- **Enhanced interoperability.** This can be seen at the level of products/capabilities, where the emphasis is on combining technological capabilities; for example convergence of x-ray scanning and biometric applications towards combined 'identification solutions' for both goods and persons. At another level, it is reflected in greater interoperability between systems to enhance the exchange of data and information between different systems and users; for example, in the area of secure communications or biometrics (enabling different users to cooperate and interconnect).
- **Emphasis on 'soft' elements of security systems**. Managing and processing information (e.g. increases in the detail of information, the variety of information, or the quantity of information available to decision processes) becomes increasingly important and, as a consequence, this component of security equipment and systems (i.e. mostly software based) is gaining in importance in overall value added relative to equipment (i.e. hardware).
- **Managing the intrusiveness of security.** Many aspects of security activities are intrusive to everyday life because they impinge on 'normal' activities, which may be reflected in economic costs (e.g. delays created by security procedures) or have implications for personal behaviour and freedoms (e.g. propriety of body scanners). In this respect, issues of public acceptance are of importance, particularly in creating an acceptable balance between levels of security and the corresponding degree of intrusion of security into public and private life.
- **Shift to more automated systems.** For some security applications there is increasing demand to move away from equipment/systems with human operators to more automated systems. Partly this can be in response to the financial (labour) cost of, for example, equipment operators. In addition, human elements can be identified as the weakest link in the overall performance of security systems and processes.

Constraints within security markets

A variety of underlying factors contribute to shaping the market (demand) – and in turn the industrial structure of supply – within the security sector, of which the following may be noted:

- **Demand side concentration:** many markets for high-end security equipment are characterised by a relatively restricted number of customers, with specific performance requirements either for different market segments or for individual customers.
- **Demand side fragmentation:** many markets are fragmented, with a lack of transferability of systems across market segments. This fragmentation may be geographical (e.g. as a result of different national security approaches, regulations and standards) or by type of user (e.g. as a result of different equipment/operating standards across client segments). This may be reinforced by lack of coordination across security domains leading to even smaller market segments.
- **Demand side lack of awareness:** whereas the defence sector, which is much older and well structured, is characterised by high levels of knowledge and understanding of technologies among customers (i.e. military, defence ministries), the corresponding levels in the civil sector – which can be characterised by a wide diversity of customers (e.g. ministries, agencies, operators, private companies) – is often seen to be lower. This can be partly attributed to the relative 'infancy' of the

civil security market. Nonetheless, the high degree of complexity associated with 'high end' security solutions, and the asymmetric level of knowledge between providers and customers, is identified as a cause of delay in procurement procedures and a factor in 'incorrect' or 'inappropriate' procurement decisions.

- **Supply side lack of awareness:** representatives of the security industry and other stakeholder argue that within the EU there is insufficient clarity in public policy making with respect to security and, more generally, a lack of information on the expectations and requirements of users (and/or those setting security regulations) of security equipment and systems.

The factors outlined above also lead into discussion of the role of standards within the security sector. Often the technologies used within the security sector are newly developed or their application in the security field is a recent phenomenon, and standards either do not yet exist or are determined at a local level. Here we can distinguish:

- **Absence of common performance standards:** often performance standards for security equipment are not clearly defined, or differ across market segments (either geographically defined or by type of user). From a supply perspective, this introduces uncertainties for equipment providers in relation to the expectations of customers regarding required performance and, in turn, for determining investments in technology/product development. From a demand perspective, the absence of performance standards makes it difficult to compare and evaluate security equipment and systems.
- **Absence of common technical standards:** the absence of technical standards, or differences in technical standards across market segments (either geographically defined or by type of user) tends to result in potential problems of interoperability and further contributes to market fragmentation.

A closely related issue is that of certification processes for security equipment. In this respect, the following concerns about the current situation in the EU have been identified:

- **Absence of common certification systems:** one complaint within the security industry is that no common system of certification exists at a European level for security equipment, and that there is no mechanism of mutual recognition across countries. Similarly, there is no mutual recognition between EU (national level) and US certification systems. Furthermore complaints have been voiced about lack of transparency in the procedures utilised by national certification bodies and that insufficient feedback is provided from certification testing.
- **Delays in certification procedures:** a related issue – that is of particular relevance given the underlying speed of technological development and the necessity to respond when 'events' occur or new threats are identified – is the overall speed at which approval/certification procedures are implemented. A consequence is that the slow speed of certification process can mean that technologies are already outdated before they receive approval.

Potential EU policy responses to strengthen the security industry and markets

From the insights provided by the analysis of the six segments covered by the report and the general assessment of the industry, as well as from discussions with stakeholders, a set of issues have been identified for which enhanced policy initiatives appear necessary.

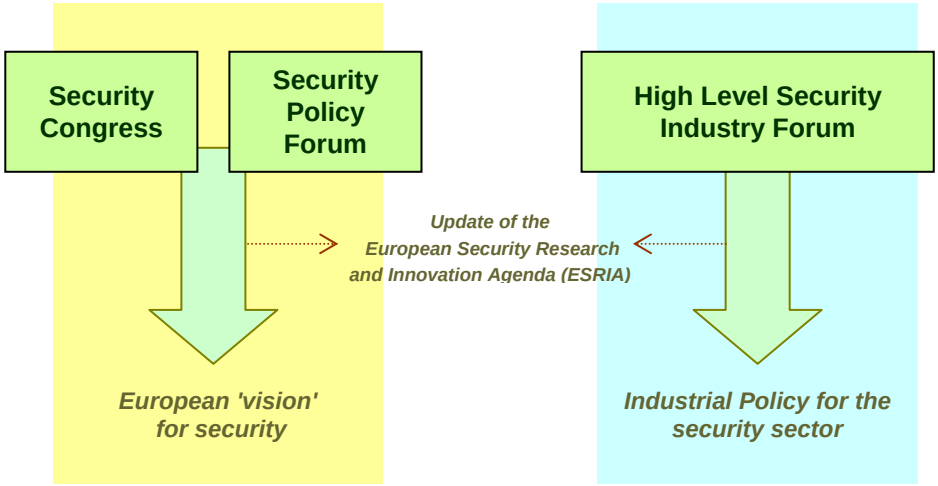
Among the policy initiatives that may be proposed are the following:

- **A European 'vision' for security through enhanced public-private dialogue**. Given the apparent lack of mutual understanding between policy makers and the private security industry sector, greater dialogue seems necessary to match the ambition of public policy makers with the potential and possibilities of the private sector (security industry and service providers). To foster greater understanding initiatives such as a periodically held "**European Security Congress**" and a more permanent and ongoing "**Security Policy Forum**" could foster greater public-private discussion and cooperation on security issues. These two platforms for policy dialogue could serve to map out a clearer European 'vision' for security that would support the security industry and relevant stakeholders to more effectively (and efficiently) contribute to meeting the EU's security priorities. Moreover, set against a European vision for security, these initiatives could provide the context (e.g. in terms of policy priority benchmarks) and setting for monitoring and updating of a European 'roadmap' for future security capability requirements and technologies[5], which could contribute to reducing uncertainty over future market developments while supporting the development of more consistent European and national level security policies.

- **An industrial policy for the security sector**. Against the background provided by the European 'vision' and priorities for security (i.e. emerging from the European Security Congress and the Security Policy Forum) and the roadmap for capability requirements and technologies, a more 'holistic' approach to an industrial policy for the security industry is required. On the one hand, this should aim to improve the functioning of the European security market through supporting the development of more consistent and harmonised national policies, which could reduce market fragmentation and support the development of a single European security market. To set out the coherent and holistic framework for an industrial policy for security, a "**High Level Security Industry Forum**" could formulate recommendations on the basis of comprehensive view of EU security related activities while indicating the policy areas and market issues that need to be further addressed.

[5] The work of ESRIF has already provided an initial 'roadmap' in the form of the European Security Research and Innovation Agenda (ESRIA) which, as they note, will require regular evaluation and revision in response to changing circumstances.

Figure 4 Suggested European framework for security policy formulation



- **Enhanced standardisation framework in the security field.** Many security technologies – reflecting the inherent and changing nature of security threats and capability requirements – are newly developed or only recently applied in the security field. Consequently, standards may not exist or may be determined at a national level. Therefore, one of the most significant problems the industry is facing is the absence of European and common international standards, which creates problems both on the supply and demand side of the security market. There is a general absence of recognised performance standards that should also be aligned to security policy. This could be addressed, for example, through the development of a "**European Security Standardisation Handbook**" or with the creation of a "**European Security Label**". Meanwhile, (industry-based) technical standards are required both to facilitate interoperability and also as a contributing mechanism for promoting greater consolidation of currently fragmented markets. This would require strengthening the activities of European Standardisation Organisations in the security domain.

- **Improved EU level testing and certification scheme with enhanced approvals and certification infrastructure**. With the general objective of either generating new certification strategies or harmonising the existing ones, such a scheme could aim at ensuring that adequate capacity is available to meet EU requirements. Moving to greater mutual recognition between countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.

- **Liability protection.** The lack of a proper liability protection system for both equipment suppliers and users creates considerable uncertainty as to their potential liability in the event of breach/failure of security equipment and systems. This is also seen as having a negative impact on investment and technology development in the European security sector. Closer public-private cooperation on liability issues, together with liability protection schemes for new security technologies should encourage security technology development and innovation.

- **Protection of Intellectual Property Rights.** To meet evolving security requirements and to remain competitive the security industry is required to invest heavily in technology development and innovation. In common with other technology intensive sectors, ensuring the return on this investment through adequate enforcement of intellectual property rights (IPR) is a major concern for the security sector. In this context, initiatives may be considered to support the security industry in the international (global) enforcement of IPR.

- **Market access and procurement systems.** The public sector is a major purchaser of security solutions and often has a strong influence on purchases in other key segments (e.g. aviation, maritime, critical infrastructure, etc.). There is concern, however, that public procurement systems for security equipment and systems are insufficiently transparent and that national procuring authorities may (explicitly or implicitly) favour 'local' suppliers over foreign competitors. In addition, national authorities may adopt different approaches when distinguishing 'defence' from 'security' procurement, which – where different procurement regimes apply - can have implications for market access. Furthermore, public authorities can influence market access through other mechanisms such as export controls (e.g. where security equipment incorporates dual use technologies that are subject to export controls on military technology). Overall, greater clarity in procurement rules for security could contribute to more transparent and efficient markets. This could be achieved, for example, through a "**European Security Equipment Market Initiative**" or the establishment of a "**European Handbook for Security Procurement**".

- **Research and innovation.** Although EU-level and national efforts to support security R&D and innovation have been stepped up, there is concern that current initiatives could be better aligned to more immediate security capability requirements (including those being set through legislative measures). Moreover, the slowness at which research programmes may be adapted means that it is difficult to rapidly mobilise public research funding in response to new security threats. With this scenario, it appears vital to stimulate and create a proper innovation framework in the security domain and establish fast track development procedures for new market technology requirements. In this respect, initiatives that could be envisaged may include: the creation of a "**European Security Technology Platform**", the enhancement of infrastructure to support validation and 'operationalisation' of security technologies and products (e.g. field-labs), and the establishment of a specific "**Fund for EU Security & Resilience**" to serve as a contingency to 'fast-track' research funding in response to new security threats.

- **Linking research to markets**. Security equipment suppliers – notably smaller companies – experience difficulties when transitioning from technology development to full commercial development of products. A consequence is that smaller innovative companies will tend to licence technologies to larger players rather than enter markets directly themselves. Though this type of arrangement may work efficiently in some cases, there is concern that it can reduce the attractiveness of entering the security market and limits growth opportunities for smaller players. Revised public procurement rules (above) and the development of a "**Pre-**

commercialisation Support Initiative for Security", as well as field-labs (above) could be developed as mechanisms to help bridge the gap between R&D and market take-up (commercialisation and full production).

- **Societal dimension of security.** One topic that is receiving increased attention is the societal dimension of security and the need for the inclusion of a 'human dimension' in security applications. From a product development perspective this is reflected in the concept of 'privacy by design', by which new security solution must take into consideration aspects of privacy from the beginning of the design process. More broadly, however, a wider reaching assessment and dialogue on the implications of societal dimensions for EU security policy, for the future development of security applications, and for the competitiveness of the security industry is required.

- **Raising awareness and understanding of EU security issues, policies, and solutions.** Raising and maintaining awareness among private citizens, business and public authorities of security developments is seen as an important area for public policy intervention. As is the promotion of greater awareness and understanding of the potential of security equipment, systems and technologies to deliver necessary capabilities to meet requirements (missions) in a variety of security fields. There is, therefore a role for public campaigns, programmes and projects to promote this awareness and understanding and, where necessary, to address misleading perceptions. At the same time, being aware of the international dimension of security issues, such initiatives could take on a broader international aspect that would promote greater understanding of EU security policy and approaches which, at the same time could 'showcase' EU solutions and raise awareness of the technological expertise and strengths of the EU security industry in international markets.

- **Areas for further research and analysis.** Taking into account the lack of both qualitative and quantitative research carried out in the security field, a number of areas can be identified for the potential provision of a series of studies in the security domain. Such studies would complement and consolidate the work undertaken under this assignment. Some potential topics to be addressed in future research may include: analysis of the role, contribution and competitive position of EU security services; a comprehensive review of security regulatory frameworks in the EU and globally; a mapping of the European Security and Technological Industrial Base (ESTIB); and an analysis of competitors (and potential collaborators) and international competition in global security markets.

Policy recommendations – Summary Matrix

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
Lack of mutual understanding between policy-makers and industry	▪ Development of initiatives to promote analysis, debate and dialogue on security issues and to develop a European 'vision' for security. This would integrate proposals and initiatives that would contribute to matching the ambition of public policy makers with the potential and possibilities of the private sector.	▪ **European Security Congress** (similar in format to the WEF "Davos" meeting) promoting dialogue and debate and raising awareness of security issues. ▪ **Security Policy Forum** would establish a permanent platform for dialogue and exchange between policy-makers, private bodies and service providers; ▪ **Strengthening the European representation of the security industry**, including not only representation from defence orientated players but also other players coming from other fields of activity (e.g. ICT), as well as national associations, and including SMEs.
Lack of a comprehensive EU industrial policy for security	▪ Monitoring and updating of a 'roadmap' for future security capability requirements and technologies aimed at contributing to reducing uncertainty over future market developments; ▪ Development of an Industrial Policy for security, giving a global and coordinated view of EU security related activities, indicating what gaps (technology, operational, societal, legal) are to be filled and what policy initiatives may be taken to improve the position of the EU security industry and functioning of EU security markets.	▪ **High Level Security Industry Forum**, to develop the basic principles and objectives of an industrial policy for security. It is meant to be a platform for discussion, bringing together industry representatives, EU institutions, governments, social partners, academic experts, etc. who would create a framework (proposals and initiatives) for the security industry to effectively respond to EU (and global) security requirements and needs. ▪ **European Security Technological and Industrial Base (ESTIB) mapping**. The identification of a European Security Technological and Industrial Base (ESTIB) and the mapping of its competences is requires as a basis for policy development and for a comprehensive assessment of the industry.

Absence of European and common international standards for security	▪ Enhanced standardisation and certification at EU and international level. This should aim to provide a framework for performance standards that are aligned to security policy, and for technical standards that promote greater consolidation of currently fragmented markets.	▪ **Industry-based solution for the development of technical standards**:
		  ▪ **Strengthening of European Standardisation Organisations' work.** Public authorities could call for the development of new standards in the security field, providing clear mandates to ESOs based on priorities set out in the European 'vision' for security;
		  ▪ **European Security Standards Institute**. Either within existing ESO framework or as an oversight body for security standards. For example, following a similar approach as that adopted by ETSI (European Telecommunications Standards Institute) and aimed at facilitating the self-development of technical standards;

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
		▪ **New Approach legislation for security**: The possibility of establishing a system of voluntary standards in the security industry should be considered. ▪ **Formal approach for the development of performance standards:** ▪ **European Security Standardisation Handbook**, based on the initiative already in place in the defence sector (i.e. European Handbook for Defence Procurement); ▪ **European Security Label**, which would increase confidence and act as a catalyst for investment by attracting new investors to the security industry. As mentioned by ESRIF, this will act as a reference point for manufacturers, end-users and other relevant stakeholders and would provide the frame for a dynamic standardisation process. ▪ **EU-level testing and certification scheme and improved approvals and certification infrastructure**, with the aim at creating a testing protocol and the necessary infrastructure (dedicated labs or testing facilities) to carry out testing practices of security products; ▪ **Exchange of formal and informal information on testing facilities as well as best practices,** with the objective of increasing transparency and cooperation (e.g. following the example of the CREATIF Network initiative); ▪ **Fast-track system for approval of priority technologies and equipment**, to enhance rapid responses to new security threats and challenges.
Lack of dedicated liability regime for the security industry	▪ Develop EU-level principles and systems for security equipment (and services) liability protection. [**NB**: this study – which is 'economic' in focus - has not analysed in detail the legal situation and arguments related liability. A further assessment of potential options is required]	▪ **Liability support for new security technologies:** legal liability protection could also be provided to security technology developers; for example under a specific liability regime for sellers of 'qualified anti-terrorist technologies'.
IPR concerns (e.g. undermining of investments when IPR protection is inadequate)	▪ Develop support to the security industry (in common with other sectors) for international protection of IPR.	▪ **The creation of a European Fund to support protection of IPR**, as an additional support for security companies to enforce IPR (e.g. patents) at international level. ▪ **Better IPR Enforcement** based on the recommendations of the IPR Enforcement – Expert Group that could be implemented at EU level, such as zero tolerance policy in IPR enforcement, promotion

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
		of Intellectual Asset Management, specific training, coordination measures, funding, etc.; ▪ **EU-US Action Strategy for the Enforcement of Intellectual Property Rights,** which is already in existence, could be tailored to security; ▪ **Development of policy towards 'generic' security requirements** for lower income regions could also be considered.
Public procurement systems for security equipment and systems are insufficiently transparent and may be used to limit markets access (i.e. preference for 'local' over 'foreign suppliers)	▪ Enhance the transparency of (public) procurement procedures and improve awareness among users/purchasers of security products and services.	▪ **Greater clarity of 'defence' versus 'security'** from a procurement perspective. ▪ **European Security Equipment Market Initiative** aimed at increased transparency of (public) procurement procedures for security. This initiative should include a **European Handbook for Security Procurement**, containing a 'Code of conduct on Security procurement', a 'Code of best practice in the supply chain', and a 'List of best public procurement practices' while, at the same time, fostering pre-commercial procurement practices; ▪ **Lead Market Procurement Network for Security**, enabling public procurers to improve their knowledge about innovative solutions and to enhance coordination.
Current security research being insufficient and not aligned to immediate security capability requirements	▪ Stimulate security research and innovation; ▪ Promote research that is more tailored to market requirements; ▪ Strengthened cooperation to support the security knowledge area to progressively structure itself, and provide an open platform used to share information and practices.	▪ **European Security Programme** as an overall umbrella ensuring synergies and coherence on research and innovation activities at EU level. It would be responsible for setting the guidelines for research priorities, which would be implemented through funding vehicles such as Framework Programmes. ▪ **Lead Market Initiative for Security**, based on the existing EU framework for LMI, built around the adoption of legislative measures designed to foster innovation, mobilising public authorities to act as 'launching customers', improving standardisation, etc. ▪ **European Security Technology Platform**, to facilitate exchange of information and the development of coherent solutions in specific and relevant knowledge domains in the EU. ▪ **Field-labs for testing innovative security products and systems.** These 'laboratories' should provide real life environments for developing and testing security products and systems. The should also function as meeting points where end-users, security authorities, industry and the research community can take initiatives for joint implementation of improved solutions relevant for their daily work. Such field-labs will can also serve to stimulate SME's in entering the market; ▪ **Fund for EU Security & Resilience**, that could be used as a fast tracking system to respond to the

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
		new security threats as they are perceived. This fund would provide public resources for research and innovation activities addressing new security threats that need a rapid mobilisation of research funding.
Difficulty of transitioning from technology development (research) to full commercial development of products, particularly for small and medium sized suppliers of security equipment and systems	▪ Pre-commercial public procurement may provide an alternative means to bridge the gap from technology development to commercial production.	▪ **Pre-commercialisation procurement support**. This would include the promotion of pre-commercialisation support programmes and the establishment of procurement procedures and rules to stimulate the market for innovate products both in the public and the private sector; ▪ **European Handbook for Security Procurement** (see above) should include pre-commercial procurement as a way of enabling European public authorities to innovate faster in the provision of public services and create opportunities for companies in Europe to take international leadership in new markets; ▪ **Field-labs** (see above) are also an instrument for bridging the gap between R&D (and related innovation activities) and market implementation as well as for stimulating and encouraging SMEs in entering the market.
Lack of knowledge and understanding of the societal dimension of security	▪ Enhance dialogue and understanding of societal issues and impacts aimed at increased incorporation of societal considerations in development of security solutions (e.g. 'privacy by design' and 'security by design').	▪ **EU Platform for Societal Issues** linked to security could effectively support the integration of societal aspects, privacy, ethical, social and human issues, into the design of solutions and services; ▪ **European Security Label** (see above), being a reference point for suppliers, end-users and customers in general, should include a 'societal dimension' to security, incorporating the 'privacy by design' dimensions to security solutions designed and manufactured in the EU; ▪ **Assessment of the impact of the societal dimension of security and competitiveness**. This should analyse the extent to which societal concerns have a positive or negative impact on the cost of security solutions, the competitiveness of the security industry and the effectiveness of security systems.
Absence of public awareness and understanding of security developments (threats), policies and solutions.	▪ Development of programmes and projects to inform and educate target groups and the general public.	▪ **Targeted awareness programmes** reaching out to specific target groups and the larger public, to raise awareness of threats, risks, vulnerabilities, to improve the understanding of the processes and procedures put in place to tackle the challenges that these threats, risks and vulnerabilities bring, to debate the acceptability of technological solutions, etc. An example could be the CPSI project (Changing Perceptions of Security and Interventions); ▪ **International Security Programme** aimed at increasing understanding of EU security policies, approaches and solutions (including themes such as standardisation, procurement, etc.) and

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
		fostering the adoption of joint or common approaches at an international level. The programme would also provide an opportunity to raise the visibility of the European security industry around the world. ,
Lack of training and skills of security equipment designers and users	▪ Assessment of the role of public and private training infrastructure in the security field; ▪ Development of international initiates to improve education and training in the field of security.	▪ **Assessment of the private and public sector training infrastructure in the security field**. This would allow the identification of training facilities and whether there are shortcomings in the current infrastructure or not. ▪ **Development of a European Training Initiative** with the creation of a network of training centres at EU level devoted to training and education on security issues. Such network would provide a platform for exchange and cross-border training, aiming to overcome fragmentation in the security training domain. ▪ **Security industry skills framework initiative,** based, for example on the challenges and action lines suggested in the *e-skills for the 21st century* Commission communication.
Lack of quantitative and qualitative research carried out in the security field	▪ A better understanding of the endogenous conditions of the industry is necessary to complement and consolidate the work undertaken under this assignment.	▪ **External advice through the potential provision of a series of studies in the security domain, which may include:** - Competitiveness of security services and interaction with industry; - Analysis of the security regulatory framework in Europe; - Mapping of the European Security and Technological Industrial Base (ESTIB); - Country-competitor analysis in the security field.

PART A - GENERAL ASSESSMENT

1 Introduction

1.1 General Context

The present study is implemented under the Framework Contract for Sectoral Competitiveness Studies (ENTR/06/054) signed between our consortium, led by ECORYS NL, and DG Enterprise. The general context for the Framework Contract for Sectoral Competitiveness Studies is the growing awareness among European policy-makers of the need to adopt policies to respond to structural weaknesses in the European economy, which led to the adoption of the Lisbon Strategy for Growth and Jobs in 2000. The Commission has committed itself to a horizontal approach to industrial policy but, nonetheless, recognises that the effectiveness of policy needs to take into account the specific context of individual sectors:

- Firstly, by understanding those changes and challenges facing industry that are of a general nature, in that they have important implications across a broad sweep of sectors, and that may be the concern of cross-sectoral policy initiatives;
- Secondly, by understanding those changes and challenges facing industry that are of a more specific nature, or of a general nature but with sector specific implications, and that may warrant the development of sector specific policy approaches.

It is, however, almost self-evident that in a rapidly changing economy, policy development is by necessity a continuous process and the status of an industry needs regular monitoring. Before such monitoring can be conducted, however, it is necessary that a 'baseline' is established that can serve as a reference point against which the situation of the sector can be assessed, both currently and in the future.

The background for this study is set out in the task specifications defined by the client. In particular, the specifications refer to the Commission's commitment – set out in the Communication on industrial policy COM(2005)474 and the mid-term review COM(2007)374 – to take the necessary actions to improve the framework conditions for manufacturing industry and to ensure consistency of various policy areas.

The legal basis for this study is the Specific Theme Cooperation of the 7th Research and Development Framework Programme (2007-2013)[6].

[6] 2006/971/EC: Council Decision of 19 December 2006 concerning the Specific Programme Cooperation implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013), Official Journal, L 400, 30 December 2006, p. 86.

1.2 Study purpose and objectives

The main purpose of the study – as set out in the task specifications – is to *"deliver a snapshot of the global security industry with specific focus on the European security industry regarding its structure (also geographical location), competitiveness and challenges ahead."* In this context, the primary objectives set for the study are:

- to define the **size and main business patterns** of the security industry in Europe;
- to identify clearly **sectors and technologies** where the European companies are world leading, dominant, facing serious challenges and do not play a role;
- to explore decisive **factors influencing the competitiveness** of the European security industry;
- to identify **policy options aimed at supporting European companies**, workers and researchers to respond to the global challenges ahead.

With respect to each of the four objectives set out above, the situation of the European security industry is to be considered within the broader context of the global security industry. Specifically the task specifications indicate the need to assess the situation, competitive performance, and regulatory environment of the European security industry with reference to key competitors such as the USA, Israel, China, Japan and Russia. This comparative analysis should provide the basis for identifying and describing success factors and weaknesses, and major challenges for the European security industry. In turn, this assessment should contribute to identifying and describing if and how EU Member States or the European Community could support the security industry in mastering the challenges that it faces.

1.3 Preliminary scoping of the security industry

The security industry is highly complex, with technological inputs that can either be specific to the security market, or be dual with defence market applications, or increasingly come from a variety of other fields such as health, consumer goods, transport, information and communications, etc. Consequently, the concept of the 'security industry' is somewhat amorphous and does not correspond to any specific industrial classification of activities[7].

At the outset of the study, and in consultation with the client, a number of parameters were set in order to provide a clearer scope of the security industry for the purposes of the study. These parameters relate to three main dimensions:

- **Focus on the provision of (security) equipment and systems**. The study is primarily concerned with the development, manufacture and supply of security equipment and systems. In this respect:
  - The provision of security services (e.g. private security service providers) is not explicitly covered by the study. Nonetheless, security service providers (both public and private) are considered relevant in terms of their role as a market for the security industry, and in terms of the inter-linkages that exist between the

[7] The technical specifications for the study did not provide a definition of the security industry

security industry and security services and other (third) markets for the security industry[8].

- Many markets for security equipment are not sufficiently structured to speak about demand for security equipment *per se*. Rather, in between final markets (customers) for security equipment and producers (manufacturers), an important position is taken by systems integrators and equipment installers[9]. Specifically, systems integrators are considered an intrinsic part of the security industry although the focus of the study is primarily on the development, manufacture and supply of equipment and systems.

- **Focus on addressing 'internal' security requirements.** A distinction can be made between 'internal' and 'external' security, where the former is mainly concerned with the protection of citizens within a country's borders and the latter by threats arising outside its borders[10]. In this respect:
  - The defence (military) sector is excluded from the scope of the 'security industry'[11]. Thus, the scope of the 'security industry' is embedded in the notions of civil (non-military) security and security of civilians. At the same time, it is clear that inter-linkages exist between the security and defence industries from the perspective of industrial structure (i.e. many defence orientated firms are also engaged in the security market); from a technological perspective (i.e. there are many dual application technologies that are relevant for both defence and security purposes); and increasingly also from a political perspective[12].
- **Focus on security requirements stemming from new / high-level security threats.** A distinction can be made between the supply of products destined for the market for general security applications (e.g. general criminal activity, public order, fire detection, etc.) and those destined for more specific markets that reflect 'high level' security threats such as terrorism, organised crime, etc. For the purposes of the study, the main focus – and hence corresponding scope of analysis of the security industry and market – is on 'high-level' security threats, and the corresponding priority security missions and capability requirements to meet these threats. The current European perspective on these threats and priority areas is described in the following sub-section.

[8] It is worth noting that specific segment analysis have also considered the role and impact of security services when relevant, for instance, in the case of security service providers for the air transport security sector, as they are the main operators of screening and security equipment.

[9] For example, for 2007 the Security Industry Association (SIA) indicates that in addition to a market value for security products in the USA of $9.7 bn. (this figure covers access control, CCTV/video surveillance, fire detection, intrusion detection, electronic article surveillance), supporting industries (installers, integrators, etc.) accounted for an additional market worth $8.2 bn.

[10] The space sector is also excluded from the scope of the study. Although there are relevant security aspects related to the space industry, the client specified that the space industry should be excluded from the scope of the 'security industry', as the relevant security aspects are already relatively well know.

[11] The technical specifications note that *"the defence sector must only be covered as far as necessary, for example if data only covering the whole defence and security industry is available"*.

[12] Many governments are adopting an 'all hazards' national security strategy that includes all security threats both 'internal' and 'external'. As an example, The 2008 French White Paper on defence and national security (English abridged version) embraces "[…] both defence and national security. It includes foreign security and domestic security, military means and civilian tools. It responds to risks emanating from either states or non-state actors. In an all-hazards approach, it deals with active, deliberate threats but also with the security implications of major disasters and catastrophes of a non-intentional nature.

Security threats and policy priorities

The terrorist attacks of 11 September 2001, combined with changes in the global political situation and increased global economic interdependence have had a profound effect on perceptions of security threats. On the one hand, it has highlighted the vulnerability of societies to acts of international terrorism or organised crime. On the other, new types of threats such as computer hacking and attacks on information systems or the use of non-conventional weapons (e.g. CBRN)[13] have been identified.

The EU-level policy response to the changed security situation emerging from the 11 September 2001 terrorist attacks has highlighted a number of key threats that confront Europe and – based on these threats and assessments of potential vulnerabilities – a number of priority security missions. The EU's Security Strategy 'A secure Europe in a better world'[14] sets out the following key threats:

- **Terrorism**, in particular catastrophic terrorism that acts worldwide and seems willing to use unlimited violence to cause massive casualties;
- **Proliferation of Weapons of Mass Destruction** (WMD), in particular in combination with international terrorism;
- **Regional Conflicts**, which themselves become a source of other threats like extremism, terrorism, state failure, organised crime and WMD proliferation;
- **State failure**, often due to bad governance, creating the breeding ground for other threats like organised crime and terrorism;
- **Organised crime**, which has developed an important international dimension.

Referring to the above threats, a distinction is drawn between 'external' and 'internal' security. By and large, external security threats (e.g. regional conflicts and state failures) are not so much threats in themselves but rather they are the sources of potential threats (i.e. due to the potential for regional conflicts and state failures to nourish extremism and terrorism and provide opportunities for organised crime). Internal security is, by contrast, a concept that applies directly to the protection of citizens from threats such as terrorism and organised crime[15].

The 'Research for a Secure Europe' Report and subsequent ESRAB Report[16] began the process of setting out – from a research oriented perspective – the linkages between the identified security threats, and a set of security missions, capability requirements and more specific needs in terms of technologies and applications. Based on the ESRAB report, four priority (internal) security missions have been identified by the European Commission[17]:

- **Security of infrastructure and utilities / critical infrastructure protection**. To protect critical infrastructures and utilities systems from being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour.

[13] Chemical, Biological, Radiological and Nuclear.

[14] European Security Strategy – presented by Javier Solana, EU High Representative for CFSP, adopted by the Heads of State and Government at the European Council on 12 December 2003.

[15] See, for example, *"Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research"* (2004), European Communities.

[16] European Security Research Advisory Board (ESRAB) *Meeting the challenge: the European Security Research Agenda.* September 2006.

[17] See Communication on Public-Private Dialogue in Security Research and Innovation COM(2007)511 – final.

- **Security of borders**. To identify and prevent illegal movement of persons, drugs, weapons, illicit substances etc. whist not unduly impeding legitimate trade and movement of persons. This includes addressing issues of traceability and security of goods supply chains and logistics networks standardisation.
- **Security of citizens**. To protect citizens against terrorism and organised crime. This includes uncovering (detection) and tracking (surveillance) of terrorists and organised criminal activities. In turn, there are implications for the secure means to exchange information and funds (e.g. secure communications), including policing of information infrastructures (e.g. the internet). And, also, for the detection, tracking, tracing, identification and neutralisation of CBRNE (Chemical, Biological, Radiological, Nuclear substances and Explosives) and Radio Frequency weapons that may be used by terrorists (or others).
- **Crisis management.** To restore security in a crisis, which may be the result of deliberate acts (e.g. terrorism) but may also arise from accidents/negligence (e.g. industrial accidents) or natural causes. This includes ensuring that governments, emergency services and societies are prepared to cope with unpredictable catastrophic incidents both during and after (i.e. recovery) an incident.

In addition, three cross-cutting mission areas are identified: (i) security systems integration, interconnectivity and interoperability; (ii) security and society; and (iii) security research coordination and structuring. Concerning the latter, the ESRAB Report identifies 5 main flagship "systems of systems" demonstration programmes capable of providing a federative frame to coalesce research in areas of significant European interest:

- **Aftermath Crisis management system:** delivering an integrated and scaleable crisis management system capable of providing comprehensive situational awareness to decision-makers to ensure a timely, coordinated and effective response to large-scale disasters both inside and outside the EU.
- **European-wide integrated border control system:** delivering a comprehensive and integrated border management system capable of providing concentric layers of protection from pre-entry control measures to cooperation inside, and between, Member States.
- **Logistic and supply chain security:** delivering an efficient, reliable, resilient and secure network of supply chains that guarantees the security of the goods produced and transported whilst having minimal impact, in terms of cost and time, on commercial operators and enterprises.
- **Security of mass transportation:** delivering a consistent and integrated suite of mass transportation security systems taking into account the specific requirements for each sector and the particular cross-border dimension of mass transport.
- **CBRNE:** A consistent portfolio of counter measures for CBRNE along the phases from prevention to response and recovery.

As mentioned earlier, the above described threats, security missions, and capability requirements are utilised as a key element in scoping the 'security market' and corresponding 'security industry' adopted for the purposes of the study.

1.4 Principle behind the study approach

Based on the methodological aspects set out in the study work-plan the study utilises a dual approach for the analysis of the security industry:

- **General assessment** of the security industry: aimed at assessing the overall situation of the EU security industry and at describing its main parameters (e.g. size and scope, business patterns and areas of specialisation, etc.).
- **Specific assessment**: corresponding to the specific analysis of different segments of the (security) equipment industry, to permit meaningful insights into the sector and avoid a broad-sweep approach. The specific analysis aims to provide an understanding of the supply/value chain for each segment and to identify the main factors influencing the competitiveness of the particular segment and the security industry more generally.

To implement a preliminary selection of possible segments that would form the basis for the specific assessment, the Staccato taxonomy was used as a starting point, with individual items in the classification assessed against specific criteria that were considered relevant given the context of the study[18]:

- **Fit to security**: match of the item (technology, equipment etc.) to providing security capabilities.
- **Economic potential of security applications for industry**: relevance of the item in terms of market potential, especially with respect to the commercial/industrial market.
- **Availability of mature products**: level of maturity of the item (i.e. is it at a sufficient level of maturity to be utilised in security products / deliver capabilities).
- **Concreteness of supplied products for security market (no services)**: is the item relevant for the supply of security products (as opposed to security services or other related services).

Moreover, other considerations for further focussing taken into account for the selection were based on the spreading of security themes and policy priorities (terrorism, crime, crisis management, civil protection, etc.); a balanced number and representation of major players (large enterprises) and SMEs; a wide-enough market of which an in-depth analysis is possible; and a clear fit to the domains of DG Enterprise.

Selected segments

During the initial phase of the study, and following discussions between DG Enterprise and the Research Team, it was agreed that the specific assessments would be based on the following segments:

- **Air transport of goods (cargo)**: Detection and identification of dangerous or hazardous goods and materials for secure air (cargo) transport;
- **Maritime transport of goods (cargo)**:Tracking and tracing of goods (and ships) for secure maritime transport;
- **CBRNE**: Detection of chemical, biological, radiological, nuclear and explosive substances (other than covered under 'air transport of goods');

[18] An additional criteria may be "potential societal acceptance", i.e. reflecting the fact that proper market diffusion of security systems is possible only if society at large is prepared to accept them.

- **Biometrics**: Biometric solutions for entrance / barrier control of protected areas, buildings or events;
- **Secure communications**: Secure, mobile, ad-hoc communication systems for operations in case of incident, crisis, disaster or event;
- **Protective clothing**: Protective and intelligent textiles and clothing for dangerous tasks of first responders.

1.5 Contents of the Report

This Final Report responds to the original technical specifications for the study, and the methodology and scope as set out in the Consortium's initial proposal and work-plan, as agreed and discussed with the client.

The report is divided into two parts:

- **Part A** (Chapters 2 and 3) provides a general assessment of the security sector as well as a set of policy recommendations.
- **Part B** (Chapters 4 to 9) describes the main findings emerging from the analysis of the specific segments.

Part A

Chapter 2 of the report, first, addresses the definition of security sector and then provides an overview of the main characteristics of the European security market, together with estimates of the size of the European and global security market. A brief analysis of some main competitor countries is also provided. Chapter 3 of the report puts forward a number of issues and possible policy responses and initiatives for enhancing the security sector and markets within Europe. These draw on the findings from the six specific segments, consultations with stakeholders, and the more general assessment of the overall situation of the security sector in Europe.

Part B

Chapters 4 to 9 describe the market and industry situation in 6 specific segments of the (security) equipment industry. For each segment an assessment is made of the (European) supply chain and value-added, the prevailing market and regulatory conditions, and the main trends and developments shaping the segment. Based on this assessment an evaluation is made of the European competitive situation and potential policy issues. The segments covered – as defined above – are:

- **Air transport of goods (cargo)** (Chapter 4);
- **Maritime transport of goods (cargo)** (Chapter 5;
- **CBRNE** (Chapter 6);
- **Biometrics** (Chapter 7);
- **Secure communications** (Chapter 8);
- **Protective clothing** (Chapter 9).

2 General assessment

2.1 Definition of the security sector

A normal starting point for an analysis of an industry's competitiveness is to define the scope of the industry concerned. Usually, this can be undertaken on the basis of well-recognised industrial classifications, for example NACE[19] or ISIC[20], which reflect the activities undertaken and/or products and services supplied by the industry. However, although some security service related activities can be identified[21], the large majority of activities and products related to the supply of security equipment and systems cannot usually be identified from recognised industrial classifications[22]. Consequently, it is not

[19] Statistical Classification of Economic Activities in the European Community (NACE). For details, see: http://ec.europa.eu/eurostat/ramon

[20] International Standard of Industrial Classification (ISIC). For details, see: http://unstats.un.org/unsd/cr/registry/isic-4.asp

[21] For example, NACE Rev 2, , identifies the following security (and defence) related service activities:

- 84.22: Defence Activities (military defence affairs and land, sea, air and space defence forces; civil defence forces; support for contingency plans and exercises in which civilian institutions and populations are involved; defence-related research and development policies and related funds)
- 84.24: Public order and safety activities (regular and auxiliary police forces supported by public authorities and of port, border, coastguards and other special police forces, including traffic regulation, alien registration, maintenance of arrest records; provision of supplies for domestic emergency use in case of peacetime disasters)
- 84.25: Fire service activities (fire fighting and fire prevention: regular and auxiliary fire brigades in fire prevention, fire fighting, rescue of persons and animals, assistance in civic disasters, floods, road accidents etc.)
- 80.10: Private security activities (guard and patrol services, collection and transport of valuables; this includes: armoured car services; bodyguard services; polygraph services; fingerprinting services; security guard services; security shredding of information on any media)
- 80.20: Security systems service activities (monitoring or remote monitoring of electronic security alarm systems; installing, repairing, rebuilding, and adjusting mechanical or electronic locking devices, safes and security vaults in connection with later monitoring and remote monitoring)
- 80.30: Investigation activities (investigation and detective service activities; private investigators)

[22] The current European industrial classification (NACE Rev 2) is not suitable to distinguish economic activities that are specifically security related, as these are usually integrated within broader activity categories. The following list – that loosely takes into consideration some of the specific segments analysed in this report – provides a non comprehensive indication of some relevant NACE categories:

- 25.72: Manufacture of locks and hinges
- 25.99: Manufacture of other fabricated metal products n.e.c. (includes, for example: manufacture of safes, strongboxes, armoured doors etc)
- 26.30: Manufacture of communication equipment (includes, for example: manufacture of mobile communication equipment; manufacture of burglar and fire alarm systems, sending signals to a control station)
- 26.51: Manufacture of instruments and appliances for measuring, testing and navigation (includes, for example: manufacture of physical properties testing and inspection equipment, manufacture of polygraph machines; manufacture of radiation detection and monitoring instruments; manufacture of mine detectors; metal detectors; manufacture of search, detection, navigation, aeronautical, and nautical equipment; manufacture of radar equipment; manufacture of GPS devices; manufacture of environmental controls and automatic controls for appliances; manufacture of measuring and recording equipment (e.g. flight recorders); manufacture of motion detectors; manufacture of radars)
- 32.99: Other manufacturing n.e.c. (includes, for example: manufacture of protective safety equipment, including, for example: fire-fighting protection suits)
- 33.20: Installation of industrial machinery and equipment (includes, for example: installation of burglar alarm systems)
- 62.09: Other information technology and computer service activities (includes, for example: computer disaster recovery services)

possible to rely on standard industrial statistics, or product-based statistics, to indicate the size and performance characteristics of the security sector.

The problems created by the absence of a well-recognised industrial definition and statistical classification of the security industry are compounded by the fact that there is also a lack of common agreement on what activities, products and services should be covered under the scope of the security industry. On the one hand, the nature of actual and perceived security threats and concerns can differ widely depending on by whom and at what level of 'society' they are evaluated. On the other hand, the nature of actual threats and perceptions of their seriousness changes over time. Consequently, the underlying concepts of 'security' and of the security industry and market are highly amorphous.

In order to try to set out some parameters for defining and scoping the security industry, three perspectives (or approaches) appear relevant:

- The nature of security threats and corresponding security missions and capability requirements;
- The characteristics of the market demand for security-related products (and services);
- The characteristics of the supply of security-related products (and services).

These are described in the following sections.

2.1.1 Security threat approach

New vs. Traditional Security

It is clear that over recent years two main categories of threats have been pushed to the forefront of preoccupations concerning security, namely terrorism and organised crime. With respect to both of these categories, their associated threat levels (actual and/or perceived) have increased dramatically and, at the same time, they have taken on an increasingly international dimension. In addition, the rapid developments in information and communications technologies have resulted in increasing concerns over the vulnerability of ICT based systems to criminal and terrorism-related activities; for example in terms of cyber-crime, or attacks on information and communications infrastructure, systems and content.

Hand in hand with the pre-occupations mentioned above, there has been an increase in awareness of the need to develop and maintain the necessary capabilities to effectively respond in the event of a major crisis incident. Such a crisis could be the outcome of a terrorist attack or of criminal activity, but similar capabilities may be called for also in the event of deliberate, accidental or natural causes resulting in a major emergency[23].

As briefly described in Section 1.3, the above mentioned 'threats' have – in the European context – been translated into a number of priority security missions, capability requirements and more specific needs in terms of technologies and applications.

[23] In this respect, we can see an overlap in the security field between protection against 'intentional' acts and protection against 'unintentional' acts and natural disasters. These latter categories of events bring, to some extent, the area of security towards the field of environmental protection.

Notwithstanding the emergence of new security priorities, there exist also more longstanding security concerns related to threats from 'ordinary' criminal acts, public (dis-)order, etc. and other types of risks such as fires, industrial accidents etc. Essentially, the relative importance of these types of risks is related to the (endogenous) profile and activities of different economic and social sectors, rather than to the types of specific (exogenous) threats mentioned above.

Following from the above, a distinction can be made between:

- **'traditional' security**, which corresponds to protection against endogenous threats such as 'ordinary' criminal activity, fire protection etc. (i.e. 'traditional' security threats), and
- **'new' or 'emerging' security**, which corresponds to protection against exogenous security threats such as those underlying current priority security threats – e.g. terrorism, organised crime, cyber crime, etc. – and protection against major catastrophic events (i.e. 'new' security threats)[24].

2.1.2 Demand side approach

External vs. Internal Security

A distinction is often made between 'external' security and 'internal' security, where external security is concerned primarily with addressing threats occurring outside national borders and internal security that is concerned with threats within national borders and thus, for example, applies directly to the protection of citizens from threats such as terrorism and organised crime. At the same time, a major part of the threat potential arising for external events such as regional conflicts or state failures relates to the possibility that they nurture terrorism or organised crime which, in turn, is translated into internal security threats. Moreover, one of the important characteristics of terrorism and organised crime is their increasingly international – and to some extent global – nature, which implies both internal and external dimensions to addressing such threats.

Although there is not a clear separation between 'external' and 'internal' security, the distinction can serve to differentiate responsibilities for addressing security threats between defence (i.e. external security) and civil security (i.e. internal security) administrations. There are, however, certain 'internal' security threat categories that cross the border (in some cases literally) between defence and civil security and which may fall under the responsibility of defence administrations. This would cover, for example, responsibilities categorised under US terminology as 'homeland defence' (e.g. defensive measures against terrorism). Also, defence administrations and, in turn, military forces may play a role in supporting civil security administrations in the event of a terrorist attack or responding to other major crisis incidents. Moreover, even in an 'external' context, defence/military forces may be called upon to undertake missions that are more of a security nature, for example in terms of humanitarian and rescue tasks, peace-keeping, crisis management/assistance.

[24] In this respect, the scope of the relevant security market and corresponding security industry is somewhat broader than that normally linked to the concept of 'homeland security', which typically is associated with preventing, protecting, mitigating and recovery from acts of terrorism (within national borders).

Overall, it is becoming more and more difficult to define the boundaries between internal and external security threats and responsibilities. This, in turn, is reflected in the apparent greater blurring of the boundaries between defence and civil security.

Civil (Public) vs. Private Security

By and large, there exists a range of security responsibilities that are generally considered to be the responsibility of public administrations. These include, for example, law enforcement and crime fighting (e.g. activities of police and forensics, customs and border control, etc.) and 'first responder' tasks (e.g. fire-fighting, ambulance/health-emergency, etc.). At the same time, in the same way as there is some ambiguity in the allocation of responsibilities between defence and civil security, there is also ambiguity between civil (i.e. public sector) and private (i.e. private sector) security responsibilities. This is most evident with respect to security of critical infrastructure and utilities that may either be operated by the public sector, the private sector, or through some form of public-private partnership. Even where such infrastructures are run by private sector operators, they are usually subject to public regulations governing their security arrangements and systems (e.g. aviation, maritime and mass transport sectors, etc.). These regulations have been reinforced significantly in response to terrorism threats and, also, those from organised crime.

A further example of the blurring between public and private sector security responsibilities is in the area of the provision of security services, where there is an underlying trend for public authorities to increasingly look to the private sector to take a role in the provision of services traditionally provided by the public sector or in areas of new or increasing demand (e.g. urban transport, public events, etc.).

Even in areas that are primarily in the private sector domain, such as security of logistics and supply-chain systems, or security of financial, communication and other forms of information systems, there is an increasing awareness of their potential vulnerability to threats from organised crime or terrorism. This is also the case for economic sectors that by their nature are potentially attractive targets for terrorism (e.g. chemicals, oil and gas, civil nuclear facilities, etc). More generally, globalisation of production systems and the societal reliance on ICT networks and systems, means that the security of these systems is not simply a private sector concern but, also, takes on a broader public policy dimension.

Main security demand side segments

From the above description, if we consider the perimeters of the security sector from a demand-side perspective, and limiting the overall scope of 'security' to internal security concerns, then four broad segments can be identified:

- **Defence (military) support for internal security:** e.g. support in the event of a major crisis incident;
- **Civil security (i.e. public sector non-military administrations):** e.g. counter terrorism, law enforcement, civil order, emergency response etc.;
- **Mixed public-private sector security:** e.g. critical infrastructure and utilities etc.;
- **Private sector security:** for which a differentiation may be made on the basis of the degree of potential vulnerability/attractiveness to 'new' security threats.

From the perspective of the 'new' and 'traditional' security threats identified above, their importance as drivers of demand for security products and services differs across segments as illustrated in Table 2.1. Clearly this table only gives a general picture and the importance of particular security threats will differ across sub-segments within the broad segments that have been identified. Nonetheless, it illustrates that the impact of 'new' security threats on demand for security products and services is highest in the public sector (defence support and civil security) and mixed public-private segments.

Table 2.1 Importance of security threats as a driver of security demand

	'New' security threats				'Traditional' security threats
	Crisis Management	Terrorism	Organised Crime	Cyber crime / attack	
Defence support for (internal) security	High	High	Low	Low	Low
Civil security administrations	High	High	High	Medium	Medium
Mixed security (PPP)	Medium	High	Medium - High	Medium	Low - Medium
Private: high vulnerability	Medium	Medium - High	Medium - High	Medium - High	Low - Medium
Private: low vulnerability	Low	Low	Low - Medium	Medium	Medium - High

2.1.3 Supply side approach

In the same way as we can distinguish between 'new' and 'traditional' security threats, an analogous comparison can be made in terms of the security industry itself. In this respect, it should be recognised that products and services supplied by the 'traditional' security industry represent the backbone of everyday security needs and a substantial part of the overall market for security equipment, solutions and services. This is the case, for example, in terms of demand for physical access control, perimeter protection and surveillance of premises, intrusion detection, fire detection, identification of goods, etc. Moreover, the emergence of 'new' security threats has undoubtedly resulted in increased demand for traditional security products (and services), for example for perimeter protection and access control for critical infrastructure such as airports, maritime facilities etc. or, more broadly, as a consequence of security requirements of economic sectors that could be potential targets for terrorism or organised crime.

Many of the 'new' security threats call for solutions and technologies from outside the traditional security domain. This has created opportunities for players from the defence sector to build on their established role as suppliers of equipment and systems to the military and expand their activities into the field of security. In particular they have been able to build upon established relationships with governments, their mutual confidence, and familiarity with technologies from the defence sector (e.g. explosive and CBRN detection) that could be applied in the area of 'internal' (or 'homeland') security.

At the same time, many defence-oriented companies sought to expand their range of solutions and technologies in order to take advantage of the rapid increase in demand, particularly after September 2001. To some extent this resulted in a scramble among the major defence contractors to acquire access to 'new' technologies; for example, as was seen with the acquisition of companies specialised in x-ray scanning[25]. Similarly, we have witnessed major defence/aerospace players making acquisitions in the fields of mobile communications[26] and biometrics[27].

Alongside opening up the security market to players from the defence sector, new security threats have also created opportunities for companies coming from neither the defence nor the traditional security industry. On the one hand, this concerned new 'start-up' companies focussed directly on the security market and, on the other, the entry into the security market of companies originating from other civilian industry and service sectors. Concerning this latter group, this has been the case in fields such as 'high end' secure communications, container tracking equipment and systems, and IT-related security applications. In other areas where non-defence related technologies (e.g. health related technologies; industrial technologies) may have applications in the security field there does not appear to have been much direct entry of companies from outside the defence domain. By and large, it seems that the entry of new players into the security market has been rather limited and there are only a few fields in which firms originating from the civilian/commercial market are major players (Motorola, in the field of secure communications, is an example)[28].

Although the overall picture is one in which the major 'defence orientated' companies occupy an important position in the supply of equipment and systems to address 'new' security threats, it would seem misleading to conclude from the perspective of industrial structure – and hence potential policy – that defence and security are largely synonymous. Many of the major 'defence orientated' companies are active in a range of fields, notably aerospace (e.g. EADS, Finmeccanica, Safran, Thales, etc.), and maintain a distinction between these activities and those in the 'defence and security' area but differ in the extent to which security is identified as a specific business segment as compared to defence[29]. By and large, however, as their portfolios of security related activities increase the trend among such companies is for greater organisational separation between defence and security activities. Also, from a technological perspective, though synergies may exist between defence and security capabilities, the range and specificities of technology requirements for these two areas are different. Moreover, many security technologies originate from outside the security domain and thus, from the perspective of the broader

[25] For example, Smiths Detection acquisition of Heimann; L3's acquisition of PerkinElmer's detection equipment business.
[26] For example, EADS acquisition of Nokia's PMR activities; Thales acquisition of Alcatel's PMR activities.
[27] For example, Sagem acquisition of Morpho.
[28] To some extent, the limited entry of new players into the security market can be attributed to the characteristics of demand, particularly in the USA after September 11 2001 but, also, in Europe. To a very large extent, the expansion of demand in response to 'new' security threats, particularly terrorism, has been driven by major public procurement contracts. In turn, this appears to have favoured the major defence contractors that were well familiar with relevant public procurement procedures and established relationships with public authorities and decision makers.
[29] For example, both the annual accounts and company information of Thales clearly identify security as a specific business area, while Safran groups 'Defence & Security' in its financial accounts (but provides additional information on the breakdown of its defence and security activities) while clearly identifying security as a separate business area from defence in the presentation of its business activities. By contrast, Finmeccanica and EADS make little separation between their defence and security related activities.

industrial and technological base underlying the security sector there are - and can be expected to be in the future – strong linkages between security and other 'civilian' industrial and service sectors.

From the above description, if we consider the perimeters of the security sector from a supply-side perspective, then three broad segments can be identified:

- **Traditional security industry**: based around the supply of general security applications (e.g. physical access control, intrusion and fire detection, CCTV/video surveillance, etc.) that correspond primarily to protection against 'ordinary' criminal activity, fire protection etc. (i.e. traditional security threats) but that, nonetheless, can be an integral part of overall responses to new security threats;
- **Security-oriented defence industry:** based on the utilisation of defence technologies in security applications or through the acquisition and conversion of civilian technologies to security applications. These correspond primarily to protection against 'new' security threats;
- **New entrants:** mainly companies originating from other civilian industry and service sectors but some start-up companies also. They end to be based on the extension of existing (civilian) technologies to security applications. Protection capabilities against 'new' security threats may be developed out of more general capabilities developed for consumer or private (industry) sectors.

It is, however, important to recognise that – in relation to 'new' security threats and priorities – the security industry is immature, having developed largely over the last decade or so. Consequently, it is not well structured and, as is the case with the supply side, boundaries between different segments are not clearly defined; for example, between the security and defence industries, or between 'traditional' and 'new' security segments. By and large, it appears that the security industry is still in a process of formation and the pattern of merger and acquisition (M&A) activity observed in the recent past suggests that there is still some way to go before a clear and relatively stable industrial structure is established. Transfers of activities through acquisitions among companies within the sector indicate a process of positioning within specific market segments that is probably still not complete. At the same time, the combination of the current economic slowdown and a marked degree of uncertainty as to the final requirements set by policy-makers and other key customer segments for some types of security applications, may result in a slowdown in the (re)structuring of the sector.

2.1.4 General scope and perimeters of the security sector

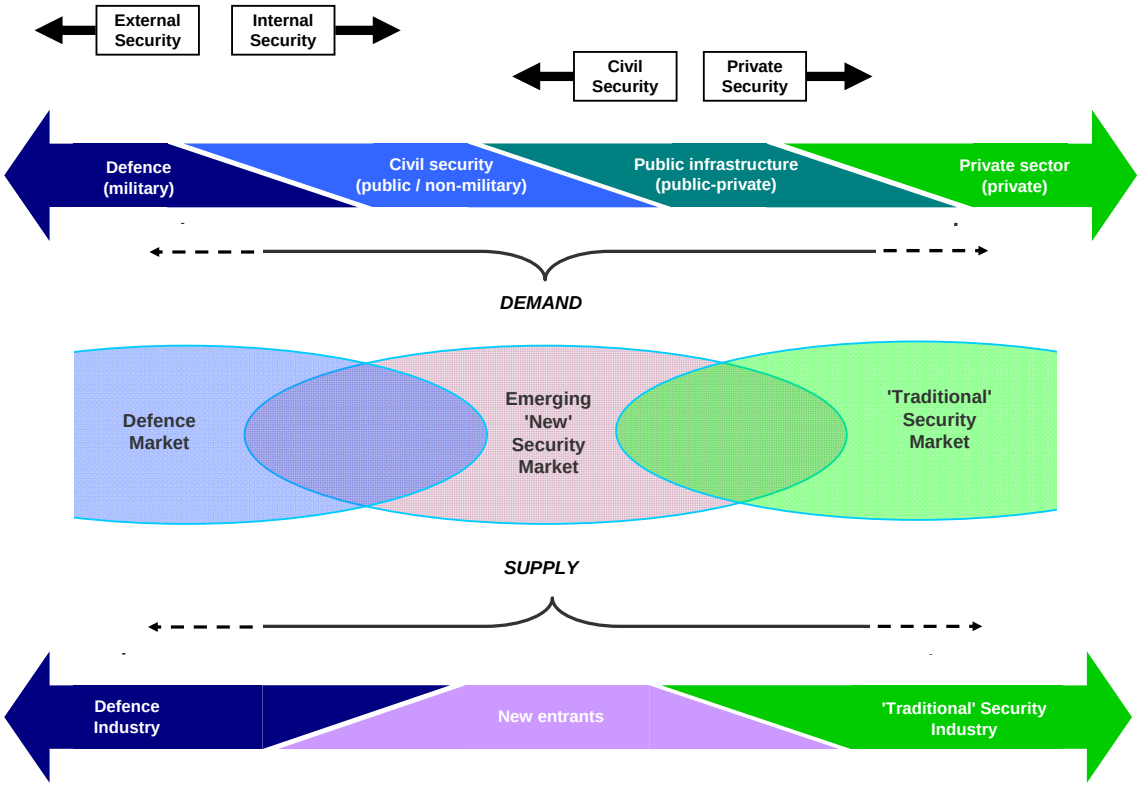
Drawing on the various elements described in the preceding sub-sections, Figure 2.1 seeks to illustrate the demand and supply sides of the security market.

The demand side is shown at the top of the Figure. In terms of a general categorisation of security two distinctions are made: first between 'external' and 'internal' security and, secondly, between 'civil' and 'private' security. From these, the four segments of security demand described in Section 2.1.2 are shown. Taking account of the broad range of security 'threats', there is the possibility for overlap (or ambiguity) at the boundaries between segments in terms of the allocation of security responsibilities and, in turn, their position as demanders of security products and services.

In terms of supply, the three segments of security supply described in Section 2.1.3 are shown at the bottom of Figure 2.1. Again, there is overlap between the segments; for example we have seen the acquisition of primarily civilian technology suppliers by defence industry companies thus blurring the distinction between defence and security. At the same time, 'new' security threats have both raised demand for traditional security products and led them to acquire or develop new technologies, such that a clear separation cannot be made between the 'traditional' security industry and a 'new' security industry.

Overall, both from a supply and a demand perspective, the emerging 'new' security market cuts across both defence and (traditional) security.

Figure 2.1 Overview of the security market: supply and demand characterisation



2.1.5 General description of security equipment and supply

As described above, a distinction can be made between the 'traditional' security equipment market and the emerging 'new' security equipment market. Briefly, these markets can be characterised as follows:

- **'Traditional' security markets** based around general security applications – for example corresponding to protection against 'ordinary' criminal activity, fire protection etc. (i.e. traditional security threats) – tend to be broad-based with a high level of transferability of security technologies and equipment across different markets segments (i.e. fairly standardised products). This is the case, for example, for products for physical access control, intrusion and fire detection, CCTV/video

surveillance, etc. Because of the relatively standardised nature of products, these markets are *prima facie* usually fairly open to competition. However, it is often the case that the logic of 'mass' production applies and economies of scale become an important factor for competitive performance. Here the tendency is towards concentration of production of standardised products among the most efficient producer. At the same time, though production may be highly concentrated, distribution networks – at global and local levels – for these products can be very fragmented. Specialised (SME) suppliers exist around the fringes of the market, where they serve niche segments with specific requirements; typically where higher security performance is required than is provided by standard products.

- **'New' security markets** that concern 'high level' security threats – e.g. terrorism, organised crime, etc. which are the main focus for this report – are often characterised by a limited number of actors (customers) present in the market, while their requirements in terms of security capabilities can be quite highly specified. In many cases it is national governments and administrations that are *de facto* the ultimate customer for security equipment or they define the shape and structure of demand through security-related regulations. This is the case, for example, in areas such as critical infrastructure protection, border management, or secure communication and biometric identification systems for government or quasi-governmental institutions. The combination of a limited number of customers and the specificity of demand tends to be matched by a corresponding concentration in the supply of security equipment. Again, specialised (SME) suppliers exist around the fringes of the market, where they serve niche segments with specific requirements; frequently these are commercial 'spin-offs' from research institutions, offering specific technological solutions[30].

  An additional feature of security markets – particularly in relation to 'new' security markets – is the role and position of **security systems integrators**. In general, markets for security products tend to be oriented towards the provision of security solutions, which are concerned not so much with the provision of security equipment *per se*, but with the integration of security equipment and technologies in order to provide security capabilities, as well as "operational concepts" (i.e. ways and procedures to effectively use the equipment) . In this context, security systems integrators play an important role in ensuring the effective integration of different security systems and customising security systems to meet client requirements.

Building on the elements described above, Figure 2.2 provides an illustrative characterisation of security equipment supply and demand:

- The demand-side of the market is represented as a triangle with, at the bottom, a broad base of demand for general 'low-end' security equipment and systems. This would cover standardised products destined to a broad base of customers or customer segments; typically this segment of the market is seen as quite price/cost-sensitive. At the top of the triangle is the 'high-end' of the market, characterised by demand for specialised types of security equipment and systems, for which the number of customers (or customer segments) is relatively limited but where security 'projects' can be very large in terms of their individual size and can require high levels of integration between different types of security applications. In between the 'general'

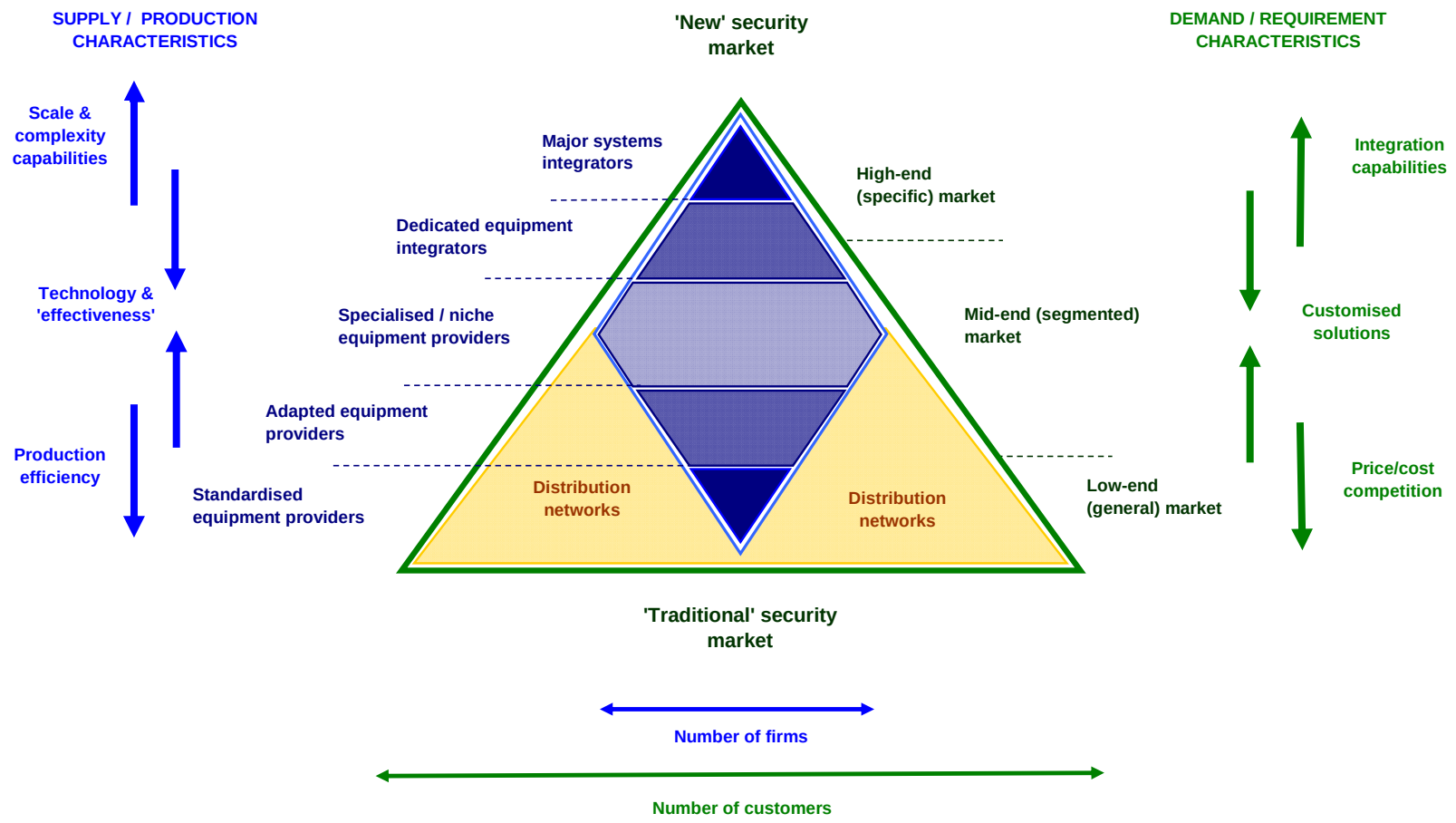
[30] See, for example, Section 4.3.2, footnote 187.

and 'specific' market segments, there is a 'mid-end' market with demand for customised equipment and systems providing larger security capabilities than provided by 'general' (or 'mass-market') type applications but that are not as highly specific as the top-end.

- The supply-side of the market (security industry) is represented by the central diamond; here we distinguish[31].
  - **'Standardised equipment providers'**. At the bottom of the diamond – corresponding to supply of standardised equipment aimed at the general/mass market, production tends to be limited to a few major companies (see above).
  - **'Adapted equipment providers'**. These providers typically supply products that are of a similar type to standardised equipment but with a greater degree of adaptation to different market/customer requirements (e.g. modular approaches or partial customisation).
  - **'Specialised / niche equipment providers'**. These are providers of specialised and highly-customised security equipment and systems, typically for particular market segments with specific sector-based or technology-based requirements. Given the high customer-specific requirements (which imply relatively small demand base for individual equipment/systems) there tend to be many suppliers but each addressing specific segments/niches. Alternatively, such providers may provide security applications on the basis of technologies that have wider applications in other fields.
  - **'Dedicated equipment integrators'**. These are also providers of specialised security equipment and systems but typically have a broader portfolio of products (or customer base) than specialised providers.
  - **'Major systems integrators'**. These are the major security systems integrators responsible for coordinating the implementation of major security projects/solutions (e.g. systems of systems). Their main characteristic is the capability to manage large-scale and complex projects and they may provide only a limited part of the security equipment and systems themselves, but 'buy-in' systems from other (dedicated or specialised) providers.
- Linking the supply and demand side of the market there are also a range of distribution networks. These are particularly important for the 'low-end' of the market, where production is often fairly concentrated but markets are fragmented. Towards the very bottom of the market these may include retail and wholesale distribution networks, but moving up the market would cover also security equipment/installers and other security service providers. Towards the top-end of the market the role of such 'intermediaries' is increasingly limited, with more direct linkages between demand and supply of equipment and systems.

[31] It should be noted that depending on their portfolio of security products, technology expertise, and sector/market specialisation, individual companies may be positioned under different supplier categories for different types of security equipment and systems.

Figure 2.2 Characterisation of security equipment supply and demand



2.2 Characterisation of the (European) security market

2.2.1 Main drivers of the security market

The main drivers of overall demand levels in markets for security equipment and systems may be summarised as follows:

- **General economic conditions.** The overall demand for security 'capacity' and, in turn, the security equipment and systems required to deliver this 'capacity' are linked to the overall level of economic activity. For example, the current economic slowdown has seen a considerable downturn in volumes of international transport of cargos and passengers that, in turn, has implications for the required level of installed capacity necessary for security screening at airports and ports. In addition, while security-related expenditures may be seen as affordable when economic conditions are good, they may come under increased scrutiny during difficult times. Particularly where the private sector is the main purchaser, demand for security equipment – at least on the basis of current experience – is strongly cyclical.
- **Security threat perceptions.** Changes in the *modus operandi* of terrorists, of organised crime, or the occurrence of 'new types' of catastrophic events/crises are major drivers of both the overall level of demand for security equipment and, also, for the types of security capabilities and solutions required by the market. In this respect, the market is largely reactive, with demand responding to specific events that highlight specific security threats. Demand may respond extremely rapidly to a new 'event' but this may be also followed by a relatively rapid decline as threat perceptions diminish. This pattern of 'reactive' demand is foreseeable but, since specific 'events' are by their nature largely unpredictable, the pattern of demand over time can be extremely uncertain.
- **Regulatory frameworks and governmental responses.** While also a response to changes in security perceptions, legislation and regulations setting out security requirements and obligations play a strong role in shaping demand for security products and services. At a most basic level, regulations may serve to set minimum security requirements within the relevant market segments to which they relate. More generally, they serve to set out a 'roadmap' for development of security requirements over time. As such, when properly conceived, the regulatory framework provides a mechanism for providing more predictable demand conditions.

The inter-relationship between the underlying uncertainty of demand conditions and regulatory frameworks has a profound influence on the security industry, particularly in terms of investment patterns and behaviour. In the face of unpredictability of 'events' that shape demand levels, regulatory frameworks (including developments in the area of standardisation) can provide the security industry – and other relevant agents (e.g. demand-side) – with greater clarity on expectations of future demand levels and requirements. Accordingly, this provides a more certain environment for companies to make investment decisions and, more broadly, for the structure of the industry to develop. One criticism of the current regulatory environment within the EU, particularly when compared to that in the US, is that it is failing to provide the necessary level of clarity required by industry to undertake investment decisions. A related comment is that the US seems to be more demanding (and more accommodating) in terms of technological requirements; for example, the US approach appears to be one of pushing technology 'to

the limit' while Europe apparently adopts a more conservative *a minima* position. This implies an environment in the US that is more attractive for companies to invest in technology development.

2.2.2 Changes in the demand for security equipment and systems

In addition to the factors identified above that provide the main drivers for overall demand, among the main factors determining the shape and structure of demand, the following may be noted:

- **Adoption of integrated approaches to security.** At one level, the move towards more integrated approaches to addressing security risks can be seen, for example, in the adoption of supply-chain security approaches based on a more holistic view of the chain of custody throughout the chain. At another level, it is reflected in 'systems of systems' approaches to the integration of security capabilities and corresponding equipment requirements. In this respect, there is a trend towards a higher degree of integration of equipment/capabilities and services. An example is the development of *"Service Orientated Architecture"*[32] and *"Modular Architecture"*[33] schemes by major systems integrators, which is based on modular approaches in system design that aims to allow easier control, integration and upgrades of systems.
- **Enhanced interoperability.** This can be seen at the level of products/capabilities, where the emphasis is on combining technological capabilities; for example convergence of x-ray scanning and biometric applications towards combined 'identification solutions' for both goods and persons. At another level, it is reflected in greater interoperability between systems to enhance the exchange of information etc. between different systems and users. For example, in the area of secure communications or biometrics (enabling different users to cooperate and interconnect), or for monitoring flows of goods and persons across borders (e.g. exchange of information on movement of goods and persons).
  With respect to both integration and interoperability, standardisation – and, accordingly the development of technical standards that promote integration and interoperability – becomes extremely important. Firstly, this occurs at the level of linking different types of equipment to each other within systems and, secondly, in allowing different users (e.g. police, customs, border control, rescue forces, infrastructure operators, etc.) to interconnect their systems to each other.
- **Emphasis on 'soft' elements of security systems**. A key aspect across security segments is how to manage information; for example, increases in the detail of information, the variety of information, or the quantity of information available to decision processes. This can be reflected, for example, in more complex algorithms for processing information, or in increasingly combining information from different sources. Data fusion is certainly one of the key technological fields in the security market, which is directly linked to interoperability issues (see above), but also to increasingly massive volumes and flows of information available. Managing and

[32] Service Orientated Architecture (SOA) is here understood to refer to the ability of a system to easily add (or plug) new services based on specific information system architecture (based on web technologies). SOA refers consequently to software capabilities rather than hardware ones. Such an approach is used by large systems integrators in order to propose a full range of security services for large infrastructure customers (airports, governments, etc.), by which a range of "off-the-shelf" standard services can then be easily plugged into a dedicated customised system solution depending on the client needs.

[33] 'Modular Architecture' is a broader approach than SOA, which includes both hardware and software components within the system.

processing information becomes increasingly important and, as a consequence, this component of security equipment and systems (i.e. mostly software based) is gaining in importance in overall value added relative to equipment (i.e. hardware).

- **Managing the intrusiveness of security.** Many aspects of security activities are intrusive to everyday life because they impinge on 'normal' activities, which may be reflected in economic costs (e.g. delays created by security procedures) or have implications for personal behaviour and freedoms (e.g. propriety of body scanners). In this respect, issues of public acceptance become important and a trade-off may be created between levels of security and the corresponding degree of intrusion. This translates into demand for less intrusive security equipment and systems (e.g. use of passive over active systems[34], use of smarter system (e.g. enhanced risk profiling)).
- **Shift to more automated systems.** Frequently there is increasing demand to move away from equipment/systems with human operators to more automated systems. On the one hand, this reflects mainly economic arguments linked to the high costs associated with human operators (either in terms of labour costs *per se* or due to speed of human operators compared to automatic systems). A further factor is that human elements can be identified as the weakest link in security systems.

When one considers the overall direction of these developments that are structuring demand for security equipment and solutions, it raises an issue of the future position of security equipment suppliers in the market vis-à-vis that of the large systems integrators. The fact that the market moves towards demand for larger projects that deliver more comprehensive and integrated security solutions means *a priori* a strengthen of the relative position of the major systems integrators. At the same time, these integrators are unlikely to develop and manufacture security equipment and systems themselves, as they will rather source them from security equipment suppliers. Thus, in addition to developing and delivering specific equipment and technical expertise, the challenge for equipment suppliers is to provide the systems capabilities that correspond to the requirements of larger projects.

2.2.3 Characteristics and constraints within security markets

There is a variety of underlying factors that contribute to shaping the market (demand) – and in turn the industrial structure of supply – of many segments of the security industry:

- **Demand side concentration:** many markets for high-end security equipment are characterised by a relatively restricted number of customers, with specific performance requirements either for different market segments or for individual customers.
- **Demand side fragmentation:** many markets are fragmented, with a lack of transferability of systems across market segments. This fragmentation may be geographical (e.g. as a result of different national security approaches, regulations and standards) or user-based (e.g. as a result of different equipment/operating standards across client segments). This may be reinforced by a lack of coordination across security domains leading to even smaller market segments.

[34] For example, replacing ad hoc physical search of air passengers (active) by walk-through or walk-by screening portals (passive).

- **Demand side lack of awareness:** whereas the defence sector, which is much older and well structured, is characterised by high levels of knowledge and understanding of technologies among customers (i.e. military, defence ministries), the corresponding levels in the civil sector – which can be characterised by a wide diversity of customers (e.g. ministries, agencies, operators, private companies) – is often seen to be lower. This can be attributed to some extent to the relative 'infancy' of the civil security market. Nonetheless, the high degree of complexity associated with 'high end' security solutions, and the asymmetric level of knowledge between providers and customers, is identified as a cause of delay in procurement procedures and a factor in 'incorrect' or 'inappropriate' procurement decisions.
- **Supply side lack of awareness:** representatives of the security industry and other stakeholders argue that there is insufficient clarity in public policy making with respect to security and, more generally, a lack of information on the expectations and requirements of users (and/or those setting security regulations) of security equipment and systems. This is reflected in a lack of transparency in decision processes, which results in an uncertain environment for the security industry to implement investment decisions, for example in relation to investments in research and technological development.

The factors outlined above, make us return to the issue of standards within the security sector. Where technologies and markets are reasonably mature, standards – either regulated or adopted *de facto* in the industry – already exist. Often, however, the technologies used within the security sector are newly developed or their application in the security field is a recent phenomenon, and standards either do not yet exist or are determined at a local level. Here we can distinguish:

- **Absence of common performance standards:** often performance standards for security equipment are not clearly defined, or differ across market segments (either geographically defined or by type of user). From a supply perspective, this introduces uncertainties for equipment providers in relation to the expectations of customers regarding required performance and, in turn, for determining investments in technology/product development. From a demand perspective, the absence of performance standards makes it difficult to compare and evaluate security equipment and systems.
- **Absence of common technical standards:** the absence of technical standards, or differences in technical standards across market segments (either geographically defined or by type of user) tends to result in potential problems of interoperability and further contributes to market fragmentation.

Part of the problem relates to the fact that differences in standards across countries or regions seem in part to be linked to the authorities' desire to retain control over technology and to either avoid dependence on external technological supply or to 'protect' domestic industry.

There is a broader question that relates to the appropriate role of regulations vis-à-vis standards. Regulations are – or should be – a reflection of a societies security needs that may be imposed in response to market failures (e.g. that private costs for security do not correspond to the benefits to society). Regulations are therefore 'good' for society as a whole. Standards are a mechanism for facilitating the achievement of the results set

through regulation and, as such should benefit industry by assisting it to meet requirements set in regulations. There is a trade-off, however, as standards – if not properly aligned to regulatory ambitions – can limit the perimeters of regulation; for example, where standards limit choices over technology solutions. There appears to be some concern expressed within the security industry that the lack of awareness (see above) of technology capabilities within some administrative bodies responsible for setting standards is resulting in the adoption of standards that are divergent from the ambitions of security regulations.

A closely related issue is that of certification processes for security equipment. Where regulatory standards are introduced, this requires the establishment of a certification system and infrastructure. In this respect, the certification process is itself a reflection of choices made over security requirements, applications and often technologies. It should, therefore, be aligned to long-term objectives and serve to provide guidance to equipment providers. In this respect, the following comments have been made concerning the current situation in the EU:

- **Absence of common certification systems:** one complaint within the security industry is that no common system of certification exists at a European level for security equipment and there is no mechanism of mutual recognition across countries. Similarly, there is no mutual recognition between EU (national level) and US certification systems. Furthermore there is a complaint that within the EU there is a lack of transparency in the procedures utilised by national certification bodies and that insufficient feedback is provided from certification testing. Consequently, even though common overarching requirements may be established at an EU-level, national differences in equipment approvals/certification persist.
- **Delays in certification procedures:** a related issue – that is of particular relevance given the underlying speed of technological development and the necessity to respond when 'events' occur or new threats are identified – is the overall speed at which approval/certification procedures are implemented. A consequence is that the slow speed of the certification process can mean that technologies are already outdated before they receive approval.

2.2.4 Some implications of market conditions on the structure of the security industry

The structure and characteristics of demand in the security sector, combined with the overall regulatory environment (and standards), as outlined above, contribute to creating an environment in which there can be very high barriers to market entry:

- High investment costs associated with technology development and, also, with the transition from technology development to placing a product on the market (i.e. high transitioning cost);
- High costs associated with securing markets (e.g. lobbying, marketing, commercial diplomacy). An important aspect to this is related to needs to 'educate' clients on technological possibilities and choices.

In addition, it should be noted that the size of production runs for many types of security equipment models can be quite small. Production of equipment for security applications is often reliant on leveraging technologies that also have applications in other non-security fields (e.g. defence, but also commercial/industrial applications). This can imply

meeting the product performance criteria and systems architecture necessary for security applications already requires that providers of security equipment are able to build upon existing capabilities/capacities from other markets. Further, the possibility for established equipment providers to build on existing equipment/systems and components may provide additional reassurance to clients in terms of continued supply and support (e.g. component replacement, easier maintenance, etc.) In other words, direct entry as a dedicated provider of equipment for security market segments may be extremely difficult.

A consequence of the high barriers to market entry is that SMEs typically play only a limited role in the security market and are often restricted to highly specialised 'niche' segments. Where SMEs are able to successfully develop innovative technologies it is usually the case that – as a result of these high barriers to entry – they tend to license this technology to larger players rather than try to enter markets independently; alternatively they may simply be acquired by such players.

2.2.5 Technology development issues and support

Technology is a major driver of the development of the security industry. The sector is characterised by proprietary technologies that are a crucial element for the competitive position of companies. In common with other sectors with a high technology focus, protection of intellectual property is a major concern. This is reinforced in areas where technologies are characterised by dual applications with the defence sector, and defence sector secrecy rules are applied. Clearly, also, there is a public policy aspect in terms of ensuring that information on technology capabilities do not fall into the hands of terrorists, organised crime, etc.

The commercial importance of technology development and innovation, together with secrecy requirements, has (obvious) implications for the type and level of collaboration and cooperation within the sector. Also, issues arise concerning the allocation of intellectual property rights resulting from joint research, whether among companies or between companies and (public) research organisations. By and large, companies in the security sector indicate that research cooperation among them is extremely limited. In addition, some security industry representatives (and other stakeholders) express scepticism as to whether public support for research (including European research programmes) is adequately focussed on addressing actual security needs and reflecting industry (and market) realities. One concern, for example, is that priorities for security research funding do not take sufficient account of the direction of development of security legislation regulations and that there could be better coordination between the two.

An equally, if not more pressing, concern relates to the protection of IPR in a wider international environment. There is a widespread belief that competitors – China being the specific example pointed to – have used reverse engineering to develop products and enter the security market. When combined with lower production costs, considerable access to national research infrastructures, and supported by strong commercial diplomacy, this places such competitors in a strong market position.

2.2.6 Comparison of EU and US market environments

It is arguable that the US approach to homeland security put in place after 11 September 2001 (e.g. SAFETY Act[35], creation of the Dept. of Homeland Security) has provided a more effective framework for structuring the security marketplace than has been the case in Europe, and for providing an environment for fostering the development of technologies and solutions to address new and changing security threats. The following features of the US approach can be identified as contributing to an environment that is more conducive to the development – and ultimately the competitiveness – of the security industry:

- **Market structure and conduct.** Through the Dept. of Homeland Security (DHS) and agencies such as the Transport Security Administration (TSA), both the overriding determinants for structuring the 'security' market and for setting the conditions of market conduct are largely established at a central Federal level. This is not the case in the EU, where the EU may set out overarching principles in the security domain but, by and large, responsibilities for security *per se* and implementation of security policy remain the prerogative of individual Member States. As a consequence, EU markets are seen as more fragmented and subject to differing market conditions and requirements.
- **Technology development and innovation.** The purpose of the US SAFETY Act is specifically to encourage the development of new and innovative anti-terrorism products and services by providing liability protections. Critically, this reduces the risks to providers that are (normally) associated with the deployment of innovative products. At the same time, through the certification processes, a 'seal of approval' is provided that serves as an indicator of performance of products and services. In turn, this approach has a broader impact as it contributes to the 'creation of a value' associated to the 'quality' of security provided by higher performance products and services. This may be contrasted with the situation in the EU where the question of liability remains a contentious issue in the security field, and where there is no system for European certification of security products and services.
- **Finance for technology development:** levels of financial support for security research and technology development in the US are significantly higher than in the EU. The US seems also less concerned by the distinction between 'defence' and 'security', with defence budgets being utilised to support security research and technology development. By contrast, there appears to be some ambiguity among EU Member States in financing of 'dual application' technologies (i.e. allocation of responsibilities between defence and security ministries). An additional advantage of channelling funding via defence budgets is that it can provide a means of bypassing multilateral (WTO) trade rules on industry support.
- **Restricted market access.** Through the requirements placed on the origin of security products and services (e.g. the restriction that the DHS should not enter into contracts with foreign incorporated entities), much of the US homeland security market – which is currently the most important market in value terms – is closed to non-US companies. While various justifications may be proposed to support this situation, it has the impact of creating a protected market for US companies while at the same time encouraging the location of security technologies (and to some extent their

[35] Support Anti-terrorism by Fostering Effective Technologies Act (2002)

development) within the US. It is difficult to evaluate the impact of these types of restrictions on European companies, since there are clear cases where they are able to have a significant presence in US markets (e.g. Smiths Detection for screening and detection, Sagem Sécurité for biometrics). At the same time, there is an associated market access related to differences between EU and US standards that may or may not allow the use of equipment and systems based on EU standards.

An assessment of US market conditions – when compared to the EU – is that US policy reflects a more strategic appreciation of the importance of the security industry and to creating conditions that will foster its development. Overall, the US market is structured in such a way that it is almost designed to be a 'consumer' of technology. Thus, not only does the US provide support for the development on new technologies – which may also be the case at the EU level or through support provided at Member State level – but it also creates conditions that are more supportive for the adoption and deployment of new technologies; for example through active participation of security agencies in the testing and evaluation of security equipment.

In respect of the above, there can be some concern that although Europe still retains a strong position in many areas of security-related technologies, there may be an increasing drift of technological development towards the US. This drift may not only affect dedicated security technologies – or technologies primarily applied in the security field – and also for technologies with a broader-based application but where providers see the (US) security market as an important component of total demand.

2.3 Market size estimates for the security sector

In order to provide an overview of the global and European security sector, the study has analysed a number of available reports and documents, as well as consulted with relevant industry representatives. It is, however, difficult to obtain a clear overall picture due to a range of factors, such as different concepts and scope of security, sensitivity of information on both production (sales) and spending on security, etc. Overall, given the sensitive nature of the security industry, sector-specific and company-specific information is often not readily available, and where estimates are provided it is often not possible to verify their accuracy.

In the absence of publicly available and verifiable data on both the demand and the supply side of the market, it is necessary to rely on 'best guess' estimates of the size of the security sector.

2.3.1 Methodology

Taking into account the above considerations, the methodological approach used in order to obtain indicative estimates of the size, structure and performance of the security industry (and main sub-sectors) has been based on a combination of the following sources:

- Information, facts and figures from available market studies;
- Expert knowledge of relevant industry stakeholders, some of whom have provided market size estimates;

- Output of our own analysis of the specific security segments;
- The utilisation of underlying 'hypotheses', usually based on identifying relevant factors that might indicate the size and levels of expenditure on security by demand sector and/or type of security product or services.

Therefore, and according to the afore-said methodology and the limitations arising from data collection, the estimates provided in the following sub-sections should be considered as indicative, based on a 'consensus' view drawn from a range of sources.

Accordingly, these estimates should be treated with an appropriate degree of caution.

Security sectors, technologies and segments

Estimates are given in relation to security sectors, technologies and segments. To clarify the figures presented in the next pages and the segment analysis, in part B the following definitions[36] apply:

- **Security sectors:** refer to economic sectors and demand based markets (e.g. aviation security, critical infrastructure protection, etc. and their respective markets);
- **Security technologies:** relate to those technological applications used in a specific – or in various– sector(s) (e.g. tracking and tracing, biometrics, CBRNE detection, etc.);
- **Security segments:** refer to the combination and the interaction created between security sectors and security technologies (e.g. tracking and tracing of maritime cargo, secure communication systems for first responders, etc.).

2.3.2 The global security market

The global security sector is estimated to represent a market worth some **€100bn** in 2008, employing around 2 million people worldwide[37].

There appears to be a reasonable consensus that the overall size of the global security market has a value of approximately €100 billion. Using estimates from Homeland Security Research (HSRC) and our own analysis, we estimate an indicative value of the markets at around €103bn, in 2008. Table 2.2 provides an approximate breakdown by segment, though these are not entirely mutually exclusive since some 'product' related segments (e.g. physical security) are also relevant for 'market' type segments (e.g. physical security applied in the aviation sector). Nonetheless, these estimates indicate that physical security protection equipment is, by far, the leading security market sector, counting for nearly 40% of the total global market, with a value estimate of approximately €40bn. Counter-terror intelligence comes second, with €19.2bn spent worldwide.

[36] It is worth noting that the presented definitions are not mutually exclusive.

[37] EOS, *Priorities for a future European Security Framework*, August 2009; Homeland Security Research Corporation (HSRC), *Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018*. Published in 2008; ECORYS estimates.

Table 2.2 Relative market size of the global security industry market (indicative € estimates by sector)

GLOBAL SECURITY INDUSTRY – Sectors	
Sectors	*Market value estimate*
Aviation security	€ 5.2 bn
Maritime security	€ 6.7 bn
Border security	€ 9.9 bn
Critical infrastructure protection	€ 12.6 bn
Counter-terror intelligence	€ 19.4 bn
Physical security protection*	€ 39.2 bn
Protective clothing (first responders)	€10 bn
TOTAL MARKET SIZE	**€ 103 bn**
** It includes CCTV, access control equipment, intrusion and detection systems, etc.*	

Source: HSRC (2008) and ECORYS

Concerning the security market by geographical region, North America (mainly the US) is widely recognised as having a leading position, with most available data sources indicating a current market share of around 40% or more. **Europe is ranked 2nd in the global security market, with a market share ranging approximately from 25% to 35%.** Although the recent financial crisis could imply a slowing of growth in 2009-2010, global demand for security equipment is expected to grow at around 5% annually through the coming years. Strongest gains are expected to occur in 'underdeveloped' markets of Asia, Africa/Middle East and Latin America.

2.3.3 The EU security market

The European security sector is estimated to represent a market value ranging from **€26bn to €36.5bn** in 2008.

Owing to the diversity of sources and variation of available estimates, our approach is to try to provide an indicative range of values for the size of different market segments (see Table 2.3). On this basis, our 'low' estimate indicates a European market size of €26bn and a 'high' estimate of €36.5bn, for 2008. The physical security protection, a traditional security market based on general security applications such as CCTV, access control, intrusion and fire detection, counts for nearly 40% of the total European market, with a market value ranging from €10bn to €15bn. Border security as well as counter-terror intelligence are both estimated to, at least, represent €4.5bn of the European security market, while critical infrastructure protection has a market value within a €2.5bn to €3.5bn interval. Last but not least, the aviation and maritime security sectors are both estimated to have a market value ranging from €1.5bn to €2.5bn.

Table 2.3 Relative market size of the European security industry market (indicative € estimates by sector)

EUROPEAN SECURITY INDUSTRY – Sectors		
Sectors	*Low estimate*	*High estimate*
Aviation security	€ 1.5 bn	€ 2.5 bn
Maritime security	€ 1.5 bn	€ 2.5 bn
Border security	€ 4.5 bn	€ 5.5 bn
Critical infrastructure protection	€ 2.5 bn	€ 3.5 bn
Counter-terror intelligence	€ 4.5 bn	€ 5 bn
Physical security protection*	€ 10 bn	€ 15 bn
Protective clothing (first responders)	€1.5 bn	€ 2.5 bn
TOTAL MARKET SIZE	**€ 26bn**	**€ 36.5 bn**
** It includes CCTV, access control equipment, intrusion and detection systems, etc.*		

Source: ECORYS

Involvement of public and private sector

One of the main features of the 'new' security market (i.e. protection against 'high level security threats') is the heavy involvement of the public sector. With the exclusion of physical security protection, the public sector is understood to be the main purchaser of security equipment and services, accounting for around 80% of the market and implying public spending of an approximate size of €13bn to €17bn. Consequently, the private sector accounts for around 20% of the market, representing purchases of equipment with a value ranging from €3bn to €4.5bn. With the inclusion of physical security protection, an area of relatively high private sector spending, the role of the public sector is, nonetheless, predominant, with public spending accounting for €15.5bn to €21.5bn compared to private spending, which reaches estimates raging from €10.5bn to €15bn.

In order to give a general appreciation of public and private involvement in the European security sector, Figure 2.3 represents the different sectors of the European security market, taking into account the level of spending of both the public and the private sector (horizontal axis) and their consideration as 'traditional' or 'new' security markets (vertical axis). The relative market value estimate of each of the sectors is represented by the size of the coloured spheres.

Figure 2.3 Public-private involvement in 'traditional' and 'new' security markets

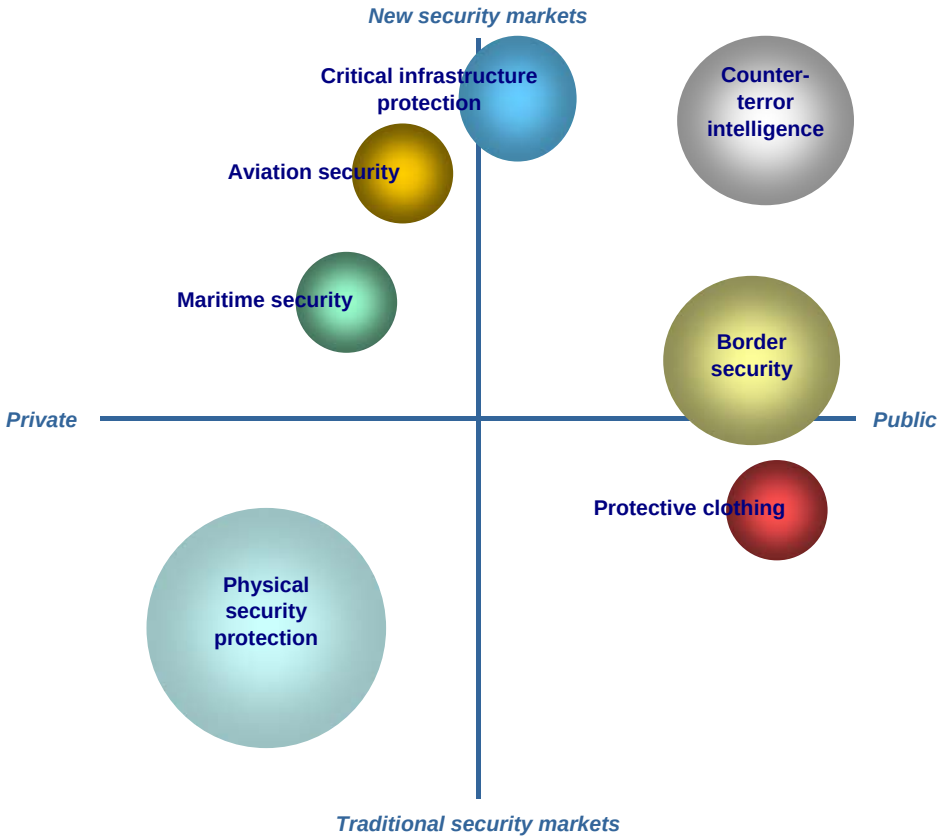


Figure 2.3 shows the predominance of physical security protection, as the largest market sector in the industry and its importance both in the traditional security market and in the involvement of the private sector as a main purchaser of equipment (CCTV, intrusion and fire detection, access control…). Yet, the sector is expected to have a relatively slow rate of growth.

New security markets, such as critical infrastructure protection, counter-terror intelligence and aviation security are expected to be the fastest growing markets. The market for products to address 'high level security threats' is in its relative infancy. However, as demand is mainly coming from the public sector and security issues continue to be high on the political agenda, a sustained growth is predicted, which would imply that these sectors increase their market share in comparison to more traditional security markets.

European market size by technologies

Many underlying technologies applied to the security field are applicable across different sectors (for example, detection and identification technologies such as screening or scanning devices are applicable to both the aviation and the maritime sector; CBRNE and biometrics play also a role in security for the aviation sector; IT and secure communications is essential for counter-terror measures but related technologies are also applied to many other segments).

Leaving aside physical security protection, and focussing on technologies used to address 'high-level security threats' (such as terrorism, organised crime, critical infrastructure protection, etc.), the role of IT and Secure Communications is predominant in the market, with an estimated market size of around €6bn to €7bn. Screening and scanning equipment (including, for instance, x-ray and scanners) account for around 20% of the market, with market value estimates ranging from €3.5bn to 4.5bn. Tracking and tracing devices represent a similar market share, with their market accounting for roughly €3bn to €4bn. We can also note that the market for protective clothing (for first responders) has an estimated market size of €1.5bn to €2.5bn which can the compared to the market size for other technology fields such as biometrics (€1bn to €1.5bn) or CBRNE (€1bn to €2bn).

Table 2.4 Relative market size of the European security industry market (indicative € estimates by technologies)

EUROPEAN SECURITY INDUSTRY – Technologies*		
Technologies	*Low estimate*	*High estimate*
Screening and scanning	€ 3.5bn	€ 4.5 bn
Tracking and tracing	€ 3 bn	€ 4 bn
CBRNE	€ 1 bn	€ 2 bn
Biometrics	€ 1 bn	€ 1.5 bn
IT & Secure communications	€ 6 bn	€ 7 bn
Physical security protection	€ 10 bn	€ 15 bn
Protective clothing	€ 1.5 bn	€ 2.5 bn
TOTAL MARKET SIZE	**€ 26bn**	**€ 36.5 bn**
** This table represents technologies used to address 'high level security threats'. However, physical security protection (the traditional security market, targeting 'low level security threats') has been included to match the total market value of the sectoral analysis presented in Table 2.3.*		

Source: ECORYS (2009)

2.4 Overall assessment of the position of the European security industry

In order to build up an understanding of the security industry within Europe, the study analysed 6 segments of the security industry that were considered to be of particular relevance given current security policy priorities. The selected segments are:

- **Air transport of goods (cargo)**: Detection and identification of dangerous or hazardous goods and materials for secure air (cargo) transport;
- **Maritime transport of goods (cargo)**:Tracking and tracing of goods (and ships) for secure maritime transport;
- **CBRNE**: Detection of chemical, biological, radiological, nuclear and explosive substances (other than covered under 'air transport of goods');
- **Biometrics**: Biometric solutions for entrance / barrier control of protected areas, buildings or events;
- **Secure communications**: Secure, mobile, ad-hoc communication systems for operations in case of incident, crisis, disaster or event;
- **Protective clothing**: Protective and intelligent textiles and clothing for dangerous tasks of first responders.

These are described in detail in Part B (chapters 4 to 9) and summarised in Table 2.5. Table 2.6 provides an overview of the main characteristics of supply chains within the segment.

Table 2.5 Overview of market characteristics for specific equipment segments

OVERVIEW ANALYSIS BY EQUIPMENT MARKET SEGMENT			
	Aviation security	***Maritime security***	***CBRNE***
Analysed equipment segment	Air cargo security	Tracking and tracing devices	Detection and tracing of CBRNE substances
Demand and market trends	Demand is mainly driven by terrorism and related regulatory requirements. Overall demand also influenced by economic conditions (i.e. volume of cargo transported). Obtaining adequate detection capabilities (effectiveness) with required throughput (efficiency) is a key technology driver.	Underlying demand based on supply chain monitoring and optimisation. Increased demand is driven by the protection of the supply chain from terrorism, illegal transportation of goods as well as from new security policies and legislation to increase maritime security.	Demand is mainly driven by terrorism and related regulatory requirements. Key demand segments include airports, critical infrastructures, high profile facilities, etc.
Market (supply) structure	Supply of equipment concentrated among a few international players. Limited number of upstream suppliers of sophisticated components / equipment sub-systems	Relatively diverse equipment suppliers (reflecting main shipping nations). More concentration in data management and systems integration.	Supply of equipment concentrated among a few international players. Limited number of upstream suppliers of sophisticated components / equipment sub-systems
Supply position of EU industry	Strong EU leaders in the global scene. EU position also strengthened by recent takeovers in the market. Lead companies maintain significant manufacturing activities in Europe (mainly in Germany and UK). Main competition from US, also increasing presence of China	Relatively strong EU position worldwide in the supply of new integrated systems (i.e. LRIT). Market for data management systems and tracking devices is dominated by US companies.	Strong EU leader in the global market. EU position also strengthened by recent takeovers. Majority of companies active in this market segment are based in the US.
Competitiveness assessment	Strong position of leading EU companies (and technology development) but limited depth of EU capabilities beyond the main players. EU position handicapped by market fragmentation (e.g. national security regulations, standards and procurement systems).	Strong added value of the EU industry in new integrated systems but remaining threat of outsourcing production and R&D outside Europe. EU position can also be hindered by increased costs due to new regulations and solutions.	Fragmented EU industry in the absence of coordinated policies and inter-industry standards. European companies are increasingly supplying outside the EU (e.g. Asia. Middle East) but market access to the US (biggest market) can be problematic.
EU market position	Some strong EU companies among the leading global players but otherwise weak	Some relatively strong EU global players but potential threat from low cost competitors as technologies mature	Some strong EU companies among the leading global players but otherwise weak

Table 2.5 Overview of market characteristics for specific equipment segments (continued)

OVERVIEW ANALYSIS BY EQUIPMENT TECHNOLOGY SEGMENT			
	Biometrics	***Secure Communications***	***Protective clothing***
Analysed equipment segment	Large scale / High-end biometric solutions for access control and identification	Large government communication systems	Protective clothing for first responders
Demand and market trends	Demand is driven by increased security needs in both public and commercial markets. Differences in societal acceptance influence overall demand and technology utilisation. The EU seems characterised by lower acceptance of biometric technologies than the US.	Demand is driven by requirements of large governmental systems (police forces, etc.), as well as by a 'technology push' model and standardisation. The PMR market is highly influenced by national structures (centralised market in France vs decentralised market in US).	Underlying demand driven by number of first responder personnel; implies mainly a 'replacement market' with limited demand growth. Fragmented demand side due to variety of risks and multiple purchasing public entities.
Market (supply) structure	High end segments are concentrated among a few leading global suppliers. Component supply structure is more diverse but mainly European, US or Japanese	High-end segments characterised by limited number of players; but wider range for low end applications. Large systems integrators have increased involvement through acquisition of PMR activities mainstream telecom equipment suppliers.	Presence of a large number of players (garments), serving a diverse range of industries and services. Companies are normally focusing on niche markets. Upstream (fibres and fabrics) more concentrated.
Supply position of EU industry	Majority of suppliers are localised in the US (largest market) with the European supply chain having few (but relevant) players in the high-end biometric solutions segment (with EU companies accounting for 50% of global market share in high-end solutions), as well as SMEs and mid-size players in Germany and UK.	EU players are exclusively competing in the high-end segment of the PMR market, with worldwide leadership in high-end governmental applications. US is the global world leader across commercial and governmental applications. Possible challenge from low-cost (Asian) competitors.	Differing position of EU companies in the global market depending on their level in the supply chain. Most fibres produced by global chemical companies with limited direct connection to security. Fabric and garments tend to be fairly localised with limited international competition.
Competitiveness assessment	EU market fragmented and fragile, due to lack of specific regulation and standardisation at EU level to foster demand. US regulatory initiatives, certification and standard bodies have become world references for the entire industry.	An adequate standardisation policy and homogenisation of national markets would permit the EU to remain strongly competitive due to its already good position and leadership in mobile and secure communications.	Strong global position in the fabric and garment market, with EU companies being innovative. However, EU market for garments is very fragmented. EU high-end quality companies may be threatened by illegal copying from the Far East.
EU market position	EU is home to leading EU players in the global scene, but US remains the dominant market	Relatively strong (leadership in mobile and secure communications)	Medium

Table 2.6 Overview of supply chain characteristics for specific equipment segment

	STANDARD VALUE CHAIN		
	Aviation Security	***Maritime security***	***CBRNE***
	Air cargo security	*Tracking and tracing devices*	*Detection and tracing of CBRNE substances*
Research and technology development	Technology development within larger equipment providers linked to technology expertise within the company (or group). SMEs present as developers of new/innovative technologies but limited market presence. Increasing importance of software development as a driver of value added **MEDIUM CONCENTRATION**	Technology developments mainly within large companies and some public institutions. Limited presence of innovative SMEs, related to high costs of technology development. Increasing focus on data management and integration aspects (large computing/data management systems companies) **MEDIUM TO HIGH CONCENTRATION**	Technology has been developed for military purposes and the market (development) is still driven by military or homeland defence (and security) concerns. **MEDIUM CONCENTRATION**
Key components and sub-systems (pre-assembly)	Main specialised components and sub-systems may be produced 'in-house' (or from within the group). Increasingly, some OEMs moving away from vertically integrated production towards integration of sub-systems whose production is sub-contracted out to specialised providers. **MEDIUM CONCENTRATION**	Main specialised components production often undertaken 'in-house' but may be outsourced to external components and sub-system suppliers based on the OEMs specifications. **MEDIUM CONCENTRATION**	Main specialised components production often undertaken 'in-house' but may be outsourced to external components and sub-system suppliers based on the OEMs specifications; this practice tends to be geographically limited. **MEDIUM CONCENTRATION**
Manufacturing (incl. final assembly) of equipment and systems	Limited number of equipment suppliers (OEMs), with manufacturing activities normally undertaken 'in-house' and at the main business locations of equipment suppliers. **HIGH CONCENTRATION**	Several medium to large players present in both LRIT and AIS (AIS less concentrated). SMEs appearing mainly only in the market for vessel tracking systems. **LOW TO MEDIUM CONCENTRATION** Few large players dominate data management and satellite services. **HIGH CONCENTRATION**	Limited number of equipment suppliers (OEMs), with manufacturing/assembly activities. These often cover detection of a range of 'agents' but may be specialised in specific areas **MEDIUM TO HIGH CONCENTRATION**
Systems (of systems) integration	Growing demand for more integrated systems and most of the larger equipment producers are active as 'integrators'. Major systems integrators can often be primary contractors when CBRNE equipment/systems are required to be integrated into larger systems/solutions (e.g. airports, critical infrastructure, border control, etc.). **HIGH CONCENTRATION**	Systems integration (and management of various data streams) is essential to provide all needed data at the right time. This is a major source of value added and is considered one of the most profitable areas of the overall supply/value chain. **HIGH CONCENTRATION**	Growing demand for more integrated systems and most of the larger equipment producers are active as 'integrators'. Major systems integrators can often be primary contractors when CBRNE equipment/systems are required to be integrated into larger systems/solutions (e.g. airports, critical infrastructure, border control, etc.). **HIGH CONCENTRATION**
Linkage to final markets (sales & distribution)	OEMs typically supply directly to the market, based on their range of available products/equipment. The degree of customisation for specific clients is limited. The shift towards larger projects and more modular approaches increases the importance of systems integrators as an interface (contractor) with final markets **MEDIUM TO HIGH CONCENTRATION**	The structure of the distribution channels and intermediaries differs between the different product types. Many AIS producers use various distribution channels and intermediaries, while other types of tracking equipment are sold nearly exclusively by the producers. **MEDIUM CONCENTRATION**	OEMs typically supply directly to the market, based on their range of available products/equipment. The degree of customisation for specific clients is limited. The shift towards larger projects and more modular approaches increases the importance of systems integrators as an interface (contractor) with final markets **MEDIUM TO HIGH CONCENTRATION**

Table 2.6 Overview of supply chain characteristics for specific equipment segment (continued)

	STANDARD VALUE CHAIN		
	Biometrics	***Secure Communications***	***Protective clothing***
	Large scale / High-end biometric solutions for access control and identification	*Large government communication systems*	*Protective clothing for first responders*
Research and technology development	Range of biometric technologies available but fingerprint (and secondly face recognition) expected to remain dominant for large public systems. Added-value in high-end biometric identification solutions lying in the biometric engine (focus on anthropometry and software). Contrast with 'commercial' applications where integration capabilities are more important. **MEDIUM CONCENTRATION**	Traditionally technology development linked to military applications but increasingly driven by commercial applications (mobile communications). Advantage of PMR technologies lies in the encryption of communications and the security of service: hardware redundancy and dedicated network infrastructures. **MEDIUM CONCENTRATION**	Fibres are an important technology, but technology now allows also manufacturing companies to add 'fibre characteristics' to the fabric. Technology development, which requires very specific technical expertise and very high investments, is concentrated in major (global) fibre/chemicals companies. **HIGH CONCENTRATION**
Key components and sub-systems (pre-assembly)	Traditionally hardware components developed specifically for biometric applications. Now, increasingly commercial technology (i.e. for consumer applications) is used based on semiconductor technology. **MEDIUM CONCENTRATION**	Most components rely on semiconductor technology with manufacturing heavily localised in Asia. **HIGH CONCENTRATION** Electronic board assembly largely subcontracted to dedicated players. **MEDIUM CONCENTRATION** Specific components (esp. integrated circuits providing data encryption functions) usually retained 'in-house' by main PMR suppliers	Supply of fibres dominated by relevant (global) players. **HIGH CONCENTRATION** Supply of low-end fabrics mainly in Asia. European companies have focussed on fabrics for high-end quality protective clothing. **MEDIUM CONCENTRATION**
Manufacturing (incl. final assembly) of equipment and systems	Equipment and sub-systems are developed to match specific application or operational constraints. Depending on the equipment integrator strategy, manufacturing can be either delegated to sub-contractors in electronic equipment industry, or kept 'in-house' **MEDIUM CONCENTRATION**	For high-end applications, entry barriers are high and the number of players is limited. Manufacturing can be either kept internal or outsourced to specialists. **HIGH CONCENTRATION**	Market concentration in the garment production is low, both for high-end and low-end quality products. Production often undertaken by companies serving 'local' markets or imported from low-cost manufacturing locations **LOW CONCENTRATION**
Systems (of systems) integration	System integrators are the primary contractors for large biometric solutions programs. Most of market value (high recurring costs) often concentrated in hands of these (major) systems integrators.. **HIGH CONCENTRATION**	System integration for high-end PMR market (e.g. for serving large government systems) requiring PMR equipment to be integrated in or interconnected to an existing information system. Major systems integrators from different backgrounds (e.g. IT, defence/aerospace, PMR) **MEDIUM TO HIGH CONCENTRATION**	Low level of systems integration regarding protective clothing **NOT APPLICABLE**
Linkage to final markets (sales & distribution)	Major systems integrators (equipment and software integrators) are in direct contact with the end-user, providing complete security infrastructure including biometric identification systems. **MEDIUM TO HIGH CONCENTRATION**	The high-end market is directly addressed by the equipment manufacturer; this can be contrasted with low-end PMR solutions that are provided by specialist distributors to a fragmented demand. **HIGH CONCENTRATION**	End-users have (via their public procurement process) direct contact with the garment companies and there hardly seem to be any wholesale/distribution market in between. **MEDIUM CONCENTRATION**

2.4.1 SWOT analysis of the security industry

The general picture emerging from the analysis is that the EU occupies a fairly strong position in the various segments covered. Nonetheless, despite the fact that some of the large EU-based companies enjoy strong and world-leading positions in a number of the analysed security segments (e.g. cargo screening, biometrics, secure communications), the depth of the EU industry beyond these key players often seems relatively limited. In this respect, the apparent success of a few EU companies should not mask potential weaknesses in the underlying competitiveness of the EU security sector. Taking a broader assessment of the security industry in Europe, Table 2.7 provides an overall SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis of the European security industry.

Strengths and Weaknesses

Considering the overall strengths and weakness of the EU security industry, as noted above, there are several EU companies that are among the global leaders in their fields of activity or technological domain. What is less evident is the depth of the industrial base that lies beyond these leading companies. In many segments where smaller (SMEs) are present there are often high entry barriers to 'top end' market segments where customers' – often from the public sector – procurement behaviour and procedures favour larger established suppliers or, from an international perspective, favour local suppliers. At the same time, for security equipment and systems that rely on more mature technologies and/or where cost/price is a key competitiveness factor, such companies may be vulnerable to competition from lower cost suppliers; for example from Asia.

Another pertinent factor in terms of the structure and organisation of the security sector, which can partly be attributed to its relative immaturity but also relates to the fragmentation of the sector (on both geographical and segment/technology levels), is the relative low level of organisation and cooperation within the industry. From this perspective, the potential role of the industry as a partner in the formulation of security policy (and security-related industrial policy) is weakened, while potential synergies within the industry may go unidentified.

A positive development with the EU – both at national and EU level – is the increased recognition by policy makers of the need for public support for security-related research, technology development and innovation. At the same time, though funding for security research has and is planned to increase further, its overall level for the EU lies considerably below the efforts made in the USA[38]. Efforts to strengthen the technological and innovation base of the security industry need, however, to also be matched by developments within the markets and among the users of security equipment and systems. In this respect, it appears that attitudes within EU markets tend to be relatively 'conservative' concerning the adoption and implementation of new technologies and innovative solutions. Such attitudes clearly dampen the incentive to EU firms to invest in research and technology development.

[38] We can note here the recommendation made in 2004 by the High-level Group of Personalities that the EU should provide a budget of a minimum of € 1 billion for research in the security area.

Notwithstanding the overall size of the EU market (see above), a further factor influencing the behaviour and performance of the sector is that the market size for specific types of equipment and systems, and the number of potential customers, may be small when compared to the investments necessary in research and technology development. Thus the relationship between potential security and non-security applications of technology becomes important, as is the degree of synergies that may be achieved between the security industry and other sectors in terms of technology development and innovation. In this respect, the strong EU position in many important related and/or enabling sectors (e.g. aerospace, defence, space, telecommunications, health etc.) is – actually or potentially – a strength of the EU security industry provided that the possibilities for synergies and widening markets can be achieved. At the same time, however, the EU appears to have fallen behind US and Asian competitors in the field of ICT security that is important as market segment *per se* but, also, increasingly in terms of the enabling role of ICT in linking and integrating other types of security equipment, systems and information flows.

Though the USA is generally identified as the largest single market for security equipment and systems, the EU is the second largest global market which, in principle, provides the EU security industry with a substantial 'home' market. Moreover, for many key market segments (e.g. civil security and emergency response, border control, maritime and aviation transport, distribution and logistics, etc.) the EU occupies an important position in terms of its market size, relative maturity and experience, and overall organisation and technical 'sophistication'. At the same time, the diversity of EU markets not only requires adaptability of supply of security 'solutions' but, also, enables security equipment and systems to be tested and 'operationalised' under a range of market conditions.

Against the above mentioned positive aspects of the EU market, past growth and future prospects are seen to be lower than in the USA and when compared to many other global regions. Moreover, despite the overall size of the EU market, fragmentation at national levels (and even sub-national levels) can increase costs and reduce the opportunities for efficiency gains through economies of scale, for example. This market fragmentation is observed in a variety of areas, such as: lack of common approaches to security policy, procurement systems, security standards, etc. At a more overarching level, organisational uncertainties on the demand side of markets (e.g. over allocation of security responsibilities and budgets) combined with apparently low levels of awareness and knowledge of procurers and users of security technologies and capabilities are seen to restrict the efficient and effective functioning of markets.

Opportunities and Threats

As identified in Section 2.2.2, there a number of factors or trends influencing developments in the security market (e.g. integrated approaches, enhanced interoperability) that, combined with shifts to larger size of individual projects/contracts, potentially favour the EU industry given its expertise in systems integration. At the same time, expectations are for substantial growth in markets for identification and online security while new, but often unpredictable, market demands can be expected to emerge in the future. These opportunities are, however, most strongly associated with major projects in the public (or quasi-public) sector market, for which there is a risk that public

administrations will place a low priority on security, particularly in a period when public sector budgets are expected to be constrained in coming years. Moreover, a shift towards larger more integrated projects that raises market access barriers (see Sections 2.2.2. and 2.2.4) could pose a potential threat, not only to SMEs but also to larger equipment and systems providers.

Another underlying trend in the market, which partly relates back to the previous point, is the increasing sophistication of security capability requirements. This provides an opportunity for the EU security industry, given that firms are typically positioned at the technological 'high-end' of the market. Enhanced sophistication of requirements should further strengthen the value-added component in security solutions coming from technological development, systems design, and other 'soft' elements. Moreover, this could be of increasing importance if a 'generalisation' of demand and increased capabilities of competitors to replicate security technologies promotes greater competition on a price/cost basis. This would favour low cost suppliers, notably from Asia where growing local markets and government support for R&D and innovation can be expected to raise their relative competitiveness vis-à-vis EU-based (and US) suppliers.

Associated to technological development and the high levels of investments that this represents within the security sector is the issue of protection of intellectual property rights. Although not specific to the security sector, there is a risk that investments in research and technology development by EU companies could be undermined through inadequate IPR protection. In turn, this would reduce the incentives to undertake such investments which could have a negative impact on the longer term competitiveness of the EU industry.

Growth in international markets for security equipment and systems offers increasing opportunities for EU exports while, at the same time, may promote foreign investments by EU companies in countries/regions with good market prospects and offering opportunities to take advantage of lower production costs (while maintaining the integrity of their control over core production processes and technologies). Of course, the possible relocation of production activities can be seen as a double edge sword, on one side it could reduce production within the EU and, on the other side, it may enhance the competitive position of companies originating from the EU. At the same time, there is a risk that EU suppliers could be excluded from growth markets if foreign governments (explicitly or implicitly) create or strengthen market access barriers; in this respect, market access is already an issue with respect to the USA and in other potentially important markets such as China, also.

A variety of opportunities have been identified that relate to strengthening the development and adoption of security-related technologies and for fostering innovation. On the one hand, these include improving the level of cooperation and mutual understanding between the various actors involved within the security sector. On the other hand, they relate to strengthening capabilities to identify and adapt existing (and new) technologies with potential security applications. At the same time, initiatives may be taken for strengthening the infrastructure for testing, validating and optimising new technological concepts (e.g. field-laboratories for security) in order to facilitate their adoption in the market. Such efforts will be of little avail, however, unless the market is

open to the adoption and take-up of new solutions and innovations. In this respect, the possibility that attitudes of procurers/users remain or become more unfavourable to technological solutions is a potential threat to development of the security industry.

Standards are an area that is seen of particular relevance in terms of reducing market fragmentation within the EU and that may also contribute to strengthening the competitive position of the EU security industry. There are a wide range of issues related to this topic but, given the relative absences of industry and product standards in the security sector both in the EU and at a global level, an underlying theme is that appropriate standards would facilitate both the functioning of the market in terms of interactions between suppliers and procurers/users and, also, within the industry itself. As standards have an impact in terms of shaping market demand, the development of EU standards that become widely recognised as a 'benchmark' in broader international markets could strengthen the competitive position of EU suppliers. Such a development seems all the more necessary when considering the potential risk that US dominance of the security sector (both in demand and supply terms) could result in US standards being adopted *de facto* as global security standards which could be to the disadvantage of EU suppliers where EU and US standards are not aligned. At the same time, the development of standards should not simply be seen as a head-to-head confrontation between the EU and US since there appear to be many areas where cooperation between the two (and more broadly with other countries and regions) could be mutually beneficial in terms of reducing market fragmentation and increasing transparency[39].

One issue that is being subject to increasing attention is 'societal issues' (e.g. individual rights, privacy of personal information, etc.) and, more broadly, public acceptance of security measures and the intrusiveness of security systems into both public and private environments. Here there is a risk that, if not properly addressed, growing public concerns could lead to lower acceptance of security measures that would limit development of the market. Addressing these public concerns could be either an opportunity or a threat to the competitive position of the EU security industry. On the one hand it may stimulate innovation and create new market opportunities both within the EU and, also, internationally if similar concerns are a factor in market demand elsewhere in the world. On the other hand, such concerns may effectively halt the development of certain technologies or may raise the cost of providing acceptable security solutions in a way that reduces the price/cost competitiveness of EU suppliers.

[39] It should be noted, however, that there is a general 'sensitivity' towards standards in the security domain and the need to maintain a degree of secrecy in order that knowledge of industry standards could be used to the 'advantage' of criminals, terrorists, etc.

Table 2.7 SWOT analysis of the European Security Industry

SWOT ANALYSIS OF THE EUROPEAN SECURITY INDUSTRY & MARKET ENVIRONMENT	
Strengths	***Weaknesses***
▪ EU companies among the global leaders in many security technology/application domains.	▪ Limited depth of EU security industrial base. ▪ Potential vulnerability of SME due both to high market entry barriers and potential international competition. ▪ Low level of EU industry organisation and cooperation. ▪ Low international presence and cooperation (with exception of a few main companies).
▪ Increased public (including EU-level) funding for security-related research, technology development and innovation.	▪ Low aggregate level of EU funding for security-related research, technology development and innovation (i.e. relative to USA). ▪ Conservative EU approach to adoption of new security technologies and solutions. ▪ The size of the security market alone may be insufficient to offset the investment in research and technology development or to achieve the scale of production necessary to remain competitive in the production of specialised components and sub-systems.
▪ Strong EU position in related/enabling sectors (e.g. aerospace, defence, space, telecoms, health).	▪ ICT (security) dominated by American and Asian players. ▪ Component supply located outside EU.
▪ Large overall size of EU market. ▪ Leading EU position in key market segments (e.g. civil security and emergency response, border control, maritime, aviation, land transport, distribution & logistics, etc.) ▪ Variety of market conditions (e.g. multicultural environments, sophistication of end markets, resource levels and funding).	▪ The relative size and growth of the US market and the preference of national administrations for local suppliers – US companies as main global leaders. ▪ Slow growth of EU market compared to other regions. ▪ Uncertainty over allocation of security responsibilities (EU vs. MS, public vs. private provision, civil vs. defence). ▪ Lack of awareness of security procurers and users (e.g. concerning capability requirements and technology needs). ▪ Market fragmentation issues: - Low level of common EU approach to security issues, policy, and regulations; - Lack of common EU approaches to procurement of security systems and services; - Lack of common EU security standards; - Lack of common EU infrastructure for approvals, certification etc.

SWOT ANALYSIS OF THE EUROPEAN SECURITY INDUSTRY & MARKET ENVIRONMENT	
Opportunities	***Threats***
▪ Increased market requirements for integrated security solutions and interoperability/interconnectivity (i.e. favouring EU expertise in systems integration). ▪ Increasing size in individual security projects with sufficient flexibility to integrate additional capabilities as new threats arise. ▪ New markets emerging from increasing identification needs (for instance, against fraud or terrorism) and online security for e-business will foster development of commercial applications.	▪ Low prioritisation of security within the EU, in general, and at MS level (notably government administrations) combined with constraints on public expenditures may lead low purchase rates for security equipment. ▪ Increasingly high market entry barriers reduce attractiveness of security markets to new entrants and discourage innovation. ▪ Potential exclusion of SMEs from security market for large integrated security projects.
▪ Increasing sophistication of security capability requirements, promotes 'high-end' / 'high value-added' security equipment and systems solutions. ▪ Increasing demand for automated systems requiring less (or more sophisticated) human intervention raises demand for security equipment and systems (relative to security personnel). ▪ Increasing value added of security equipment and systems generated by 'soft' elements (software, data management, processing algorithms, etc.)	▪ Generalisation of security equipment, systems and technologies promotes price/cost-based competition and favours non-EU based low-cost suppliers, or results in relocation of EU-based production to low-cost regions. ▪ Domination of US suppliers and increasing technological sophistication of Asian suppliers – due to larger/increasing home market demand and support for R&D and innovation – raises their relative competitiveness vis-à-vis EU-based suppliers.
▪ Growing international (global) markets for security equipment and systems. ▪ Investing in production facilities in other regions of the world, taking advantage of lower production costs, subject to maintaining the integrity of their control over core production processes.	▪ National preferences and explicit or implicit market access barriers that restrict EU suppliers from competing in international markets. ▪ Economic slowdown and adverse macro-economic conditions could moderate the pace of this growth to some degree. ▪ Outsourcing or the relocation of final assembly activities to low cost locations.
▪ Improved cooperation between regulators, end-users, industrial suppliers and industry fosters innovative approaches and adoption of new technological approaches. ▪ Adaptation of existing and new technological capabilities for applications in the security field (e.g. nanotechnologies for PPE, etc.) ▪ Strengthening of infrastructure for testing, validation, and optimisation of new technological concepts for specific security domains (e.g. field-labs for first responder equipment, forensics, surveillance systems, etc.) stimulates product development and innovation.	▪ EU procurers and users maintain a conservative attitude to the adoption of new technological solutions, thus slowing down their take-up and implementation.
▪ Better IPR enforcement, fostering the interest of companies to be involved in the development of new technologies as early as possible.	▪ The position of EU high-end quality companies might be threatened by the undermining of technology investments by illegal copying, etc.
▪ Greater EU-level cooperation on development and adoption of common security standards and approvals/certification systems. Eventually leading to adoption of EU-based standards international markets to the advantage of EU suppliers. ▪ EU legislation aiming to develop a standardisation framework across all Member States, which would be likely to heighten overall demand for security equipment	▪ US dominance of security supply, creates *de facto* US-based global security standards ▪ Simpler and better developed system for standardisation of security systems and technologies in the US - and a more focussed stimulation of technological innovation for security – supports *de facto* US-based global security standards
▪ Addressing public concerns (e.g. societal issues) stimulates innovation and creates new market opportunities.	▪ Reduced public acceptance of security measures and intrusiveness of security systems etc. and public concerns about preservation of individual rights. ▪ Additional costs associated with addressing public concerns within EU reduce cost competitiveness of EU security solutions

2.5 Development of strategies and business models

Given the wide diversity of products and services that are encompassed within the scope of the security industry, the variety of companies involved, and the differing characteristics of final markets, it is a rather difficult task to identify common approaches and directions in the development of strategies and business models. Also, as mentioned in Section 2.1.3, having developed largely over the last decade or so, the security industry in its 'modern' form is immature and does not have a clearly identifiable structure. In this respect, developments over the past decade in terms of transfers of activities through mergers and acquisitions among larger companies within the sector indicate a process of positioning within specific market segments that is probably still not complete. At the same time, it needs to be recognised that individual firms may occupy different positions (and pursue different strategies) in different market segments.

A general underlying factor influencing strategies in the security sector is the need to address the variable and unpredictable nature of demand, being strongly influenced by specific events and threat perceptions (see Section 2.2.1)[40]. Moreover, although underlying growth prospects for security products and applications remain strong, current economic conditions are having a clear negative effect on demand in many segments, which represents an additional challenge for security companies. This is already resulting in companies looking to rationalise production and supply chains and step-up cost reduction efforts, including possible relocation or outsourcing of production (especially manufacturing) activities. At the same time, it appears that the crisis will focus attention on inherent differences between market conditions and cycles in the security fields and other business areas, notably defence. There is an argument that the crisis may actually bring about a greater separation between operations in security and those in other areas as firms seek to increase flexibility and capacity to respond to (differences in) market developments[41].

The above being said, it is evident that EU strengths lie primarily towards the 'high-end' of the security market and that the EU has a very limited position in the market for more generalised 'low-end' security products (see Section 2.1.5). Where EU suppliers are present in low-end segments, actual manufacturing activities within the EU are often limited with most having been relocated or outsourced to lower-cost locations (i.e. Asia). Even within 'high-end' segments, the value-added in actual hardware (i.e. physical equipment) is typically low when compared to 'soft' elements. By and large, from a product perspective the strategies of EU suppliers of security equipment and systems are orientated towards technology development, systems design, and software-related aspects rather than towards manufacturing.

[40] Despite this unpredictability, it can be noted that for defence companies faced by reducing military spending and uncertainties over major development programmes the security sector was seen as an attractive opportunity to diversify and, to some extent, reduce uncertainty and variability in revenue flows.

[41] Another argument is that a clearer separation between defence and security activities (and technologies) may also be influenced by export controls applied to military sales but that may also be applied where the separation between military and non-military sales (exports) is unclear. A clear separation may reduce instance where (military) export controls are applied to security related technologies/exports.

Following from the above, we can see a divergence between those companies that have a more integrated technological base that incorporates a high degree of internal RTD – often where companies have a broader portfolio of activities and can leverage technology in other fields to the security domain – and those that focus more on the adaptation of 'bought in' technology to the specific requirements of the security market[42]. For the former, business strategies are typically orientated towards continuous technological development and innovation aimed at enhancing existing applications and bringing new products (and technologies) to the market. For the latter, business strategies are orientated towards specialisation based on enhancing the security-related aspects of existing technologies, often through customisation for specific market segments and clients.

As noted in Section 2.2.2, growing market requirements for greater integration and interoperability of security systems are a general feature of demand. This has implications for the nature of the market (e.g. fewer but larger sized projects/contracts) and also for vertical relations within the security industry. This development tends to favour the large systems integrators many of whom come from the defence sector but it may also increase opportunities for civilian companies with experience and expertise in delivering large scale complex projects. These systems integrators may deliver only a small part of the security equipment and applications themselves, but will coordinate the integration of equipment and sub-systems from a range of sources. As previously mentioned, for equipment suppliers the challenge is to meet both the security capabilities and systems capabilities (in terms of facility of integration within larger systems) required for such projects. A related issue for the business strategies of equipment suppliers is to identify an optimal portfolio of products given the potential trade off between, on the one hand, depth of technological expertise and, on the other, breadth of the 'offer' of security capabilities (equipment and systems).

A further issue that it is thought will become of increasing importance in the future is the interrelationship between security equipment and related operational services. To date, there has largely been a separation between the provision of security equipment and the provision of services (e.g. private security services). The overall effectiveness of security systems relates, however, not only to the hardware (and its embedded soft/service elements) but also to provision of the related operational (user) services. Although the importance of services for the performance of security equipment and systems is readily recognised, it appears not to be widely reflected in business models and strategies. In this respect, service provision (either directly or through sub-contracting to dedicated service providers) is an area that could grow in strategic importance and as a factor in determining overall competitiveness within the security sector.

[42] We can see, for example, approaches where companies use COTS (Commercial Off The Shelf) components and modules that they adapt for the security market (e.g. enhancing inherent security capabilities or increasing robustness).

2.6 Brief analysis of main competitors

The following section presents a brief analysis of the main country competitors of the European security industry.

The strongest player and most important competitor for the EU is the United States. The US is not only the biggest market (approximately 41% of global turnover), but US companies are often technical frontrunners in high-end security equipment. Israeli and Japanese companies have a strong position in high-end security equipment, but mainly cover specific niches such as IT and communication security. The Chinese and Russian markets show strong growth rates in the traditional physical security protection segment (CCTV, access control). However, Chinese and Russian companies produce mainly low-end security equipment and do not really compete with the high-end oriented EU companies.

Table 2.8 summarises the main findings, which are presented in more detail in the next sections.

Table 2.8 Summary table: Main competitors

OVERVIEW ANALYSIS OF MAIN COUNTRY COMPETITORS			
Country / Region	***Market size***	***% of global market***	***Remarks***
EU	≥ € 26 bn	25.2%	• Estimation of EU-turnover is € 26-36.5 bn.
US	€ 42 bn	40.8%	• World's largest market, strongly influenced by US regulations and US federal security policy. • US security agenda (9/11, war on terror/drugs) and federal security budgets are main drivers. • US companies have strong competitive position, are often frontrunners in high-end security equipment and active around the globe.
China	€ 13.5 bn	13.1%	• Estimation refers to turnover for 2006, high growth expectations. • Economic growth, massive construction projects and public demand are main drivers for growth. • Traditional physical security protection is largest sector. • Chinese companies mainly produce low-end equipment for home market; for high-end equipment China is dependent on US and EU companies.
Japan	€ 3.8 bn	3.7%	• Estimation refers to turnover for 2008; estimation for total security industry is € 8.3 bn (data for 2005, including security services); high growth potential. • High crime rates (also IT-related) are main drivers for growth. • Advanced (physical) security protection, with sensors, image/monitoring, access control, being the main markets. • Japanese companies have strong position in IT security; focus on home market, but also export to Russia, China, Us and EU.
Israel	€ 2.7 bn	2.6%	• National security is (political) top priority, due to terrorist threats. • Homeland security industry is an important 'spin off' from the strong military and defence industry. • Israeli companies have strong position in high-tech IT, telecommunication and software technology. • Government budgets, but also military training (IT-related) and US military aid are important factors for competitive position. • Security equipment is an important export product, e.g. to EU.
Russia	€ 1.1 bn	1.1%	• Estimation refers to turnover for 2006; estimation for total security industry is € 4.5 bn (data for 2006, including security services), with high growth rates expected. • Traditional physical security protection, including CCTV and video surveillance, is the largest sector. • Russian market players mainly focus on home market and produce low-end equipment.
Rest of the world	€ 13.9 bn	13.5%	
TOTAL	**€ 103 bn**	**100%**	

Source: ECORYS based on different sources

2.6.1 United States

General overview

The United States is the world's largest market for safety and security equipment, with a market mainly influenced by US regulations and the US federal security policy. The aftermath of the 9/11 attacks as well as other terrorist threats, the 'war on terror' and also the 'war on drugs' are currently the main drivers for the industry.

Civitas estimated the annual turnover of the 'US homeland security market' to be €24.7 billion ($31 billion) in 2006, with remarkable increases from the previous years (a 29% increase from 2004)[43]. However, more recent figures from HSRC (2008)[44], the US Security Industry Association (2007 and 2008)[45] and ECORYS estimates allow setting the US security industry at around **€42bn**, with a US global market share of around 41%. In addition, Papaioannou et al. (2006) assess that the US cover 45% of the global export in safety and security equipment[46].

Main fields of activity

Table 2.9 shows an overview of the weighted value of addressable spending for the different security industry sectors. Physical security protection and counter-terror intelligence are the main fields of activity in the US, accounting for around €12.5bn and €8bn respectively. Other sectors such as protective clothing for first responders (€6.5bn) or critical infrastructure protection (€5bn) follow. Equipment for the protection of US borders (with a market around €4.5bn), maritime security (€3bn) and aviation security (€2.5bn) configure the other relevant security market sectors.

Table 2.9 Breakdown US security industry market

US SECURITY INDUSTRY – Sectors	
Sectors	*Market value estimate*
Aviation security	€ 2.5 bn
Maritime security	€ 3 bn
Border security	€ 4.5 bn
Critical infrastructure protection	€ 5 bn
Counter-terror intelligence	€ 8 bn
Physical security protection*	€ 12.5 bn
Protective clothing (first responders)	€ 6.5 bn
TOTAL MARKET SIZE	**€ 42 bn**
** It includes CCTV, access control equipment, intrusion and detection systems, etc.*	

Source: SIA (2007), HSRC (2008) and ECORYS

[43] Civitas, 'The Homeland Security Market- essential dynamics and trends', November 2006.
[44] Homeland Security Research Corporation (HSRC), *Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018*. Published in 2008.
[45] The US Security Industry Association, 'US Security market report and economic impacts study 2008', January 2009.
[46] Papaioannou, 'Market overview of Safety and Security', 2006.

Public and private sector involvement

Considering the involvement of the public and private sector as purchasers of equipment, the US Federal government is responsible for around 60% of all the security equipment purchased in the US. The private sector (also including quasi-governmental bodies) represents around 30% of the spending on equipment. US States and local authorities are also purchasers of equipment, but at a smaller scale, being responsible for 10% of all US security equipment market purchasers.

Table 2.10 Breakdown US security industry market (public and private involvement)

Category	*% total spending on security equipment*	*Remarks*
US Federal	60%	Intelligence is the main sub-category of federal spending (50%); the main federal departments are: Defense, Justice, Health and Human Services, State, Agriculture and Energy.
US States and local authorities	10%	Approximately ±€3 billion is funded from federal programmes, often related to the Department of Home Security (DHS).
US private sector & quasi-governmental	30%	The protection of critical infrastructure -often owned by the private sector (70-80%) - is the main component within this category (energy utility, airports, harbours). Spending is mainly related to the type of industry and regulation.
TOTAL spending on equipment	**100%**	

Source: ECORYS based on Civitas (2006)

Key players

Given the broad and diverse scope of the security equipment market it is not easy to identify the key players in the market because their position differs per sub-segment. The table below presents the top-10 of companies active in the 'homeland security market', which is based on the total amount of awarded contracts by government agencies (2008).[47]

[47] Government Executive, Top 25 Homeland Security Contractors 2008 and 2009, see < http://www.govexec.com/features/0808-15/0808-15s11s1.htm >.

Table 2.11 Overview top 10 US security companies (2008)

(Parent) company	*Contracts value in 2008 (and 2007)*	*Remarks*
Boeing Co.	€ 402 m (€ 193 m)	Boeing is active in the commercial airplanes market, but Boeing Integrated Defence Systems (with 70,000 employees) also provides high-tech security solutions (like military aircrafts and sophisticated IT solutions). In 2008 they won a $2 bn contract regarding border protection.
Lockheed Martin Corp.	€ 331 m (€ 345 m)	A 'security and information technology company', although 58% of their turnover is related to the US defence market. In relation to homeland security they develop and produce equipment for border security, critical infrastructure protection, emergency management & response, information and transportation security. Their workforce reaches 146,000 employees.
IBM Corp.	€ 330 m (€ 322 m)	Provides (among others) IT-infrastructure (security) solutions.
Accenture	€ 267 m (€ 140 m)	Provides (among others) IT-infrastructure (security) solutions.
General Dynamics Corp.	€ 266 m (€ 136 m)	GD (92,000 employees) is active in aerospace, combat & marine systems and 'information systems and technology' (e.g. tactical and strategic mission systems).
SAIC	€ 247 m (€ 215 m)	Provides mainly technical services and products related to security (defence, homeland security, energy, etc.). They employ 45,000 people.
Unisys Corp.	€ 233 m (€ 230 m)	Provides IT-solutions for 'mission-critical environments'.
L3-Communications Holdings	€ 221 m (€ 255 m)	Originally a defence company; in relation to homeland security they offer aviation, port, maritime and cargo security solutions as well as security products for mass transportation and intrusion detection. It also offers services for crisis management and law enforcement and provides vehicles for first responders; 66,000 employees.
Northrop Grumman Corp.	€ 213 m (€ 326 m)	A 'security company' (120,000 employees) which is active in aerospace, electronics, information systems, shipbuilding and technical services.
Computer Sciences Corp.	€ 143 m (€ 93 m)	A 'consulting, systems integration and outsourcing company', which offer IT related security solutions.
TOTAL top 10	**€ 2,652 m** **(€ 2,257m)**	

Source: Government Executive, Top 25 Homeland Security Contractors 2008 and 2009; company websites.

According to Civitas many of the new entrants to the 'homeland security' market were previously active in the defence market (mainly related to the US Department of Defence) or the market for more traditional commercial security products[48].

Main geographical markets

US companies are active around the globe, but given the fact that the US market represents approximately 40-45% of the global spending on security equipment their domestic market is a very important one. Furthermore, they are active in Europe, Russia, Asia and the Middle-East (especially Israel), but specific information is lacking. In Israel

[48] Civitas, 'The Homeland Security Market- essential dynamics and trends', November 2006.

for example, US companies represent 70% of the total import value ($600 million). In Vietnam, 25% of the security equipment imports are coming from the United States[49].

Key strength

In general, US companies dealing with security equipment are often frontrunners in the technical development of products and manufacture sophisticated high-end quality equipment. Besides the 'traditional' good performance of US companies in technical development of products, this is triggered by significant spending by the US (federal) government on security equipment and R&D. Civitas stresses that the US companies (as first movers) often establish the standards for next generation (security) solutions, which gives them a good competitive position for the future[50].

Relevant public policies supporting the sector

A crucial factor in relation to the competitive position of US companies is the US government itself. As mentioned previously, security is a high priority for the US Federal Government and their demand is a dominant driver for (high-tech) security solutions. The Homeland Security Act of 2002 institutionalised the Department of Homeland Security with substantial budgets for security (DHS, with a requested budget for 2009 of $50 billion). Besides the DHS, the Administration and Congress also support other government agencies for their security spending. Civitas estimated the 'governmental demand' at € 17.3 billion in 2006, while also observing that "government spending is supporting an aggressive R&D infrastructure that is driving innovation across the security sector, improving capabilities, and building core technologies that will be applicable in adjacent markets as well" [51].

Another relevant factor is the US Safety Act. The US Safety Act is designed to promote the creation, deployment and use of anti-terrorism technologies by lowering the liability risk of companies that develop products and services used in combating terrorism. Carafano (2008) reports that in the period 2002-2008 approximately 200 companies have obtained certification.[52]

2.6.2 China

General overview

The US Commercial Service estimated that the Chinese safety and security market generated a turnover of **€13.5 billion** ($17 billion) in 2006.[53] Another source estimated the turnover of the security market (without surveillance) to be €27 billion ($34 billion) in 2006[54]. Given the relatively high growth rates of the Chinese economy (despite the 2008/2009 economic crisis) the growth expectations for the safety and security market are high. The US Commercial Service expected (in 2008) a turnover of €22.7 billion ($28.5 billion) in 2010[55].

[49] US Commerical Service, country fiches Israel and Vietnam.
[50] Civitas, 'The Homeland Security Market- essential dynamics and trends', November 2006.
[51] Civitas, 'The Homeland Security Market- essential dynamics and trends', November 2006.
[52] Carafano, J.J., 'Fighting terrorism, addressing liability: a global proposal', in: Backgrounder, no. 2138, May 2008.
[53] US Commercial Service, 'China: safety and security market', May 2008.
[54] China Security & Surveillance Technology (CSST), based on the 'China Public Security Guide'. See < http://sec.edgar-online.com/china-security--surveillance-technology-inc/6-k-report-of-foreign-issuer/2006/09/06/Section3.aspx >.
[55] US Commercial Service, 'China: safety and security market', May 2008.

The main drivers for demand are China's growing economy and massive construction projects (especially in the Eastern coastal area), as well as demand from the public authorities. The US Commercial Service reports that sophisticated surveillance equipment (mainly for monitoring and controlling access) is widely used in high-end residential areas and commercial office buildings. The 9/11 attacks lead to a stronger awareness for security protection. The government strengthened their anti-terrorism measures (especially in relation to air security) and surveillance and monitoring equipment is widely used in seaports, railways and airports (protecting cross-border shipments of goods and passengers) [56].

Other large government initiatives which drive the demand for security equipment are the 'State Emergency Response Systems', the 'City Emergency Forecast and Alarm Systems', and 'Safe City Construction', but also events like the 2008 Olympic Games, the 2010 World Expo in Shanghai, and the 2010 Asian Games in Guangzhou[57].

Main fields of activity

Three main fields of activity can be identified within the Chinese safety and security market, which are video surveillance, door access, and burglar-proof alarm equipment (see table below).

Table 2.12 Breakdown safety and security equipment market

Company	*2005*	*2006*	*Remarks*
Video surveillance	€ 769 m	€ 1,115 m	80% of the equipment is sold for commercial offices (financial institutions, shopping malls, and transportation facilities). Public demand is mainly related to infrastructure projects, such as airports, correction facilities and safety city initiatives.
Door access	€ 214 m	€ 261 m	Demand is mainly related to city construction projects, transportation systems, tourism sites and sports stadiums.
Burglar-proof alarm	N/A	N/A	The integration of web-based video surveillance with burglar-proof alarm is a future trend
Total	**> € 983 m**	**> € 1,376 m**	

Source: US Commercial Service, 'China: safety and security market', May 2008.

The (members of the) China Security and Protection Industry Association (CSPIA) covers also other types of security equipment, like biometrics, IT security, cash in transit, critical infrastructure protection, physical/barrier protection and transport and aviation security[58].

[56] US Commercial Service, 'China: safety and security market', May 2008.
[57] US Commercial Service, 'China: safety and security market', May 2008.
[58] CSPIA, see < http://english.21csp.com.cn/ >.

Key players

A division must be made between security equipment with high and low-end quality. Chinese security equipment companies mainly produce low-end quality products, while the US companies and (to a lesser extent also) European companies mainly produce for the high-end market.

The high-end market is more concentrated with the presence of US companies like 3M, General Electric (GE), Honeywell, Ingersoll Rand, Motorola, Pelco, Tyco and UTC, but also European companies (i.e. Legrand Group). The (low-end) security equipment market is very fragmented, as the US Commercial Service estimates that over 15,000 small-sized (private) enterprises are active on the market[59]. This group includes companies like Tiandy (CCTV, video surveillance, 120 employees), Anjubao (Guangzhou Anjubao Sci-tech Co, video surveillance) and Hikvision (video surveillance, 1,700 employees).

Main geographical markets

The Chinese security equipment companies are mainly active in the Chinese domestic market, but they also export products, for example to Russia[60]. Companies like Hikvision and Tiandy are also active on the US and European market. In this respect, the US Commercial Service observes that China is lacking in high-end and high-value-added domestic products[61].

Key strength

The competitive strength of Chinese security equipment companies seems to be relatively limited, which is related to the low-end production quality of Chinese security equipment and their fragmented market structure. For high-end quality products China is mainly depending on technical solutions from the US and Europe.

Relevant public policies supporting the sector

The safety and security segment is heavily regulated by the Security Ministry (including the Public Security Department and Public Security Bureaus). The main threshold for foreign companies is the China Compulsory Certification mark (CCC-mark) which is obliged for all safety and security products sold in China. Furthermore, the US Commercial Service stresses that local Chinese companies often have strong ties with the (local) Chinese government and are often better positioned to obtain all required certifications[62].

[59] China Security & Surveillance Technology (CSST), based on the 'China Public Security Guide'. See < http://sec.edgar-online.com/china-security--surveillance-technology-inc/6-k-report-of-foreign-issuer/2006/09/06/Section3.aspx >.

[60] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.

[61] Ibid, see footnote 34.

[62] China Security & Surveillance Technology (CSST), based on the 'China Public Security Guide'. See < http://sec.edgar-online.com/china-security--surveillance-technology-inc/6-k-report-of-foreign-issuer/2006/09/06/Section3.aspx >.

2.6.3 Japan

General overview

Currently, security is an important public concern in Japan and the size of the security industry is growing fast. In its analysis of the Japanese security industry, the US Commercial Service indicates that this public concern is related to very high crime rates (mainly related to burglary), but also credit card and e-mail scams and identity theft[63].

The size of the total Japanese security industry (including both the sales and installation of security equipment and security services) is estimated at €8.3 billion ($10.3 billion) in 2005 and shows an upward trend. The estimated market size for the security equipment industry in 2005 was €2.9 billion ($3.6 billion), while the projected market size by 2008 is **€3.8 billion** ($4.8 billion) and €4.6 billion ($5.7 billion) by 2010.[64]

Main fields of activities

Five main segments can be identified within the security equipment market (see Table 2.13). Image/monitoring and access control were the leading markets in 2005 while image/monitoring equipment as well as sensors are the main expected growth segments.

Table 2.13 Breakdown security equipment market

Field of activity	*2005*	*2008 (estimate)*
Image/monitoring market	€ 714.5 m	€ 964.6 m
Sensor	€ 639.3 m	€ 1,093.2 m
Home security (equipment & service)	€ 518.7 m	€ 606.9 m
Access control	€ 666.2 m	€ 739.5 m
Residential security service	€ 313.4 m	€ 373.0 m
Total	**€ 2,852 m**	**€ 3,777 m**

Source: US Commercial Service, 'Japan Market Brief', April 2007, based on a Fuji Keizai Ltd report.

The US Commercial Service observes that school and town security (emergency alert systems) and also regional safety (mass notification systems) are emerging sub-segments (with a projected size in 2008 of €78 million).

Key players

Due to historical reasons, the spin-off from the military and defence industry towards the security industry seems to be rather limited in Japan. However, some companies such as Mitsubishi Heavy Industries, Toshiba Corporation, Mitsubishi Electric Corporation,

[63] US Commercial Service, 'Japan Market Brief', April 2007, based on a Fuji Keizai Ltd report. The 2005 exchange rate from Eurostat is used. See: < http://www.authorstream.com/Presentation/Moorehead-58878-Japan-Market-Brief-MarchApril-2007-Whats-Different-Domestic-as-Education-ppt-powerpoint/ >.

[64] US Commercial Service, 'Japan Market Brief', April 2007, based on a Fuji Keizai Ltd report. The 2005 exchange rate from Eurostat is used. See: < http://www.authorstream.com/Presentation/Moorehead-58878-Japan-Market-Brief-MarchApril-2007-Whats-Different-Domestic-as-Education-ppt-powerpoint/

Kawasaki or Ishikawajima-Harima are defence-related companies also providing security equipment.

Related to IT security, the main players concerning mainly software solutions are Fujitsu, Hitachi, Mitsubishi, NEC or Toshiba, jointly with other global players like IBM, Nokia or Unisys, also present in the Japanese Market.

Main geographical markets

The Japanese security equipment companies are normally active in the Japanese domestic market, but they also export products to neighbouring countries such as China and Russia. Companies with global presence such as Mitsubishi, NEC or Toshiba have also remarkable export activities to the US and Western Europe.

Key strength

Due to the development and improvement of communications infrastructure and the advanced role of the Japanese market in providing high-tech IT solutions, the Japanese security market has a strength in the provision of both security hardware (security appliances and authentication devices) but also mainly in software applications (identity management, secure content management, etc.). Therefore, the country is in a competitive advantage in front of other suppliers in the IT security field.

Relevant public policies supporting the sector

Although some specific public policies already supported by the government could not be identified, Nihon Homeland Security K.K. states that there is a need for public policies supporting the sector to counteract a general passive approach to security. Moreover, a comprehensive access control is uncommon outside of financial and data centre industries, which implies that some public action should be taken to improve access control measures in other areas[65].

2.6.4 Israel

General overview

Given the unstable political situation in the Middle-East and direct terrorist threats, security is a top priority in Israel. Both the defence and homeland security (HLS) industry are seen as a fundamental part of the national security of Israel. At the same time, HLS-knowledge and experience is more and more seen as an interesting export product. Several (government related) websites promote the Israeli HLS sector as an important trade and investment opportunity for foreign countries[66]. The Investment Promotion Center (IPC, part of the Ministry of Industry, Trade and Labor), for example, identifies HLS & Public Safety as one of the main business sectors for investment, stating that 'Israel has earned a worldwide reputation for providing leading security solutions'[67].

[65] See http://www.nihon-homelandsecurity.com/documents/NHS-AFCEA_Presentation-08-05-21.pdf

[66] See for example: < http://www.israexport.co.il/about.asp >, < http://www.export.gov.il/eng/ > and < http://www.investinisrael.gov.il >.

[67] Investment Promotion Centre (http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm).

The annual HLS industry turnover (2008) is approximately **€2.7 billion** ($4 billion). Approximately 25% of that turnover is related to export of security products. Forecasted market growth (until 2010) is 10-15% per annum[68]. Gordon (2009) states that it is tenable to assume that the HLS (including surveillance, see below) is comparable to the turnover of the Israeli military and defence industry (€4 billion / $5 billion in 2006)[69]. Employment within the HLS industry is estimated at 25,000 people, being therefore slightly smaller than the military and defence industry (35,000 employees).

Main fields of activity

The HLS industry covers a whole range of security areas. The Israel Export & International Cooperation Institute (IEICE) identifies twelve main areas such as access control, commodity protection, identification / authentication, IT security & software, perimeter protection and tracking and motion detection; while the IPC also stresses aviation, maritime & transportation security, counter terrorism, CBRN and critical infrastructure protection.[70]

Key players

The HLS industry is seen as an important (and profitable) 'spin off' from the military and defence industry[71]. The Israeli defence industry is dominated by five players. Four of these companies are state-owned and sell 75% of the total arms, namely, Israel Military Industries (IMI), Israel Aircraft Industries (IAI, also including the sub-company ELTA) and Rafael. Private companies like Elbit and Elisra (part of Elbit and IAI) are responsible for another 20%.

[68] Investment Promotion Centre (http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm).
[69] Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009. Neve Gordon works for the Ben-Gurion University.
[70] IEICE, < http://www.export.gov.il/Eng/_Articles/Article.asp?CategoryID=1009&ArticleID=10141 >.
[71] Investment Promotion Centre (http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm).

Table 2.14 Overview of Israeli defence companies

Company	Employees	Turnover	Remarks
IMI	3,200	€ 377 m (in 2007)	Especially defence products, but also HLS activities (security & anti-terror training, public transportation security, aviation and airport security, strategic infrastructure protection, hazard detection systems, roof protection, fire extinguishing).
IAI	16,500	€ 2,200 m (in 2008)	Especially defence products, but also HLS activities (advanced sensing systems, communications, data processing, command and control, assisted decision making and support).
Rafael	5,000	€ 938 m (in 2007)	Especially defence products, but also HLS activities (border security and control, surveillance, maintaining security systems based on advanced biometric systems, development of protection systems and remotely controlled weapon platforms). 35% are Israeli orders, 21% from Europe and 6.5% from North America.
Elbit	10,876 (1,826 in the US)	€ 1,109 m (in 2007)	Especially defence products, but also HLS activities (integrated land, maritime and coastal control and surveillance systems, airport and seaport security systems, border control systems, "safe city" systems, access and border registration control systems, pilot identification systems, transportation security systems, C4I homeland security applications, etc.).
Elisra	1,310	€ 171 m	Mainly defence products, HLS activities are unclear.

Source: Company websites and Israel Defence & Security Report (Business Monitor International, 2009).

The HLS industry itself includes over 600 companies, of which 35% are active with security technology, 35% with security products, 20% are dealing with security IT and software and another 10% are related to security services. 350 of these companies contribute to the total Israeli export of security products[72]. The HLS industry is characterised by a decentralised and diffused production process[73].

Gordon (2009) also states that the activities of the HLS industry are mainly related to surveillance[74]. This is illustrated by the fact that 237 of the 312 (exporting) companies in the IEICE database are related to surveillance[75].

Main geographical markets

The main geographical areas where the Israeli companies are active differ per business line. However, it is clear that the domestic market is the largest market for Israeli companies. Concerning the HLS industry, the Israeli market covers 75% of the annual turnover. The overview of Rafael's market distribution (which also includes defence

[72] Investment Promotion Centre (http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm).

[73] Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009. Neve Gordon works for the Ben-Gurion University.

[74] Surveillance is defined by Gordon as "the production of goods, services, technologies and mechanisms that facilitate the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". The surveillance industry "manufactures products, provides services, and carries out R&D directly related to the surveillance of behavior of individual subjects, social trends and classifications, as well as biological, ecological and environmental processes".

[75] Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009. Neve Gordon works for the Ben-Gurion University.

related activities) illustrates that Western-Europe (33%) is one of the biggest export markets, followed by Central Europe (11%) and North-America (10%)[76].

Key strength

The constant security threat requires a strong military and defence industry which is directly linked to the national security (several state owned companies) and state budgets. Key strength for the defence industry and (as a spin off) for the HLS industry are the high tech IT, telecommunication and software technology. Often, entrepreneurs who start a new company have R&D experience in the army[77]. Gordon stresses that the Israeli army and defence industry is not only supplying specific technological knowledge, but also enables private entrepreneurs to manufacture spin-offs[78].

Relevant public policies supporting the sector

The huge government budgets for the Israeli defence industry are an important driver for R&D in the defence and HLS sector. Also the military training is an important factor in relation to the competitive position of the defence and HLS industry. Further, there are some policy related issues which should be mentioned here:

- Foreign competition within Israeli public tenders is allowed, but the regulatory framework requires that foreign companies use local components and services up to 35% of the costs of the awarded contract[79];
- The regulatory framework sets certain limitations to the acquisition of Israeli companies (related to defence and HLS) by foreign companies;
- Israel is the largest recipient of US military aid and arms exports (Foreign Military Financing) with billions of dollars of defence goods and services payments each year. Therefore, close relationships exist between the US and Israel. The impact on the Israeli defence and HLS industry is uncertain, but might strengthen their position[80].

2.6.5 Russia

General overview

The estimated value of the total Russian security market (including security services and equipment) was approximately €4.5 billion ($5.6 billion) in 2006. It is expected that the market will grow to €5 billion ($6.8 billion) in 2007. Approximately 20% of this total relates to the security equipment market (**€1.1 billion** in 2006) and this might grow to €1.2 billion in 2007. The rest of the security market is mainly related to security services (guarding services and physical protection)[81]. The Russian market shows high annual growth rates (see Table 2.15).

[76] See http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/6/766.pdf.
[77] Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009. Neve Gordon works for the Ben-Gurion University.
[78] Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009. Neve Gordon works for the Ben-Gurion University.
[79] Business Monitor International, 'Israel Defence & Security Report Q3 2009', p. 39.
[80] Business Monitor International, 'Israel Defence & Security Report Q3 2009', p. 39.
[81] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.

Main fields of activity

Within the safety and security equipment market, four key segments can be identified, namely CCTV & video surveillance, security & fire alarm, intruder alarm & perimeter protection, and access control (see Table 2.15). The CCTV segment is seen as the most developed and competitive sector. For the coming years, the CCTV and access control systems are the most promising segments in terms of growth expectations[82].

Table 2.15 Overview Russian security equipment market

Sector	*Turnover '06*	*% Market share*	*Annual growth rate (%)*
CCTV & video surveillance	€ 334,5 m	30	30
Security & fire alarms	€ 256,5 m	23	12-15
Intruder alarms & perimeter	€ 256,5 m	23	12-15
Access control	€ 178,4 m	16	15-16
Other	€ 89,2 m	8	N/A
Total	**€ 1.115 m**	**100**	**12-30**

Source: US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.

Key players

Due to lack of information, the relevant key players in the security equipment market are difficult to identify. One source indicates that approximately 20 companies cover 50-90% (in volume) of the 'market for electronic physical security equipment' (including CCTV)[83]. There are approximately 300 distribution companies active in the market, with Satro-Palladin, Luis+ and Ultra Star being the largest players[84].

The spin-off from the military and defence industry towards the security industry seems to be rather limited in Russia. The Russian defence industry mainly focuses on defence related equipment. Big defence companies are, for example, the United Aircraft Corporation[85] and Irkut (both related to aviation equipment), Almaz-Antey (dealing with land forces equipment and air-defense) as well as Sevmash and Admiralteyskie Verfi (both supplying naval equipment). In 2005 the aggregate sales of the 20 biggest defence companies was approximately €7.6 billion ($9.5 billion) [86].

Main geographical markets

The Russian home market is mainly concentrated in two city regions, namely Moscow and St. Petersburg, where 60% of the turnover in the security equipment market is generated. 23% is also produced in the Urals federal district, 11% in the Siberian federal district, and 6% in the Northwest federal district[87].

[82] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.
[83] See: < http://www.indiasafe.com/image/pdf-dec08/russia.pdf >.
[84] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.
[85] In UAC the Russian state consolidated their shareholdings in the (civil and military) aviation industry (since 2006).
[86] Moscow Defence Brief, see < http://mdb.cast.ru/mdb/2-2006/item2/item2/ >.
[87] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.

Key strength

Particular strengths of the Russian security equipment industry could not be identified. Russian companies appear to produce mainly (more low-end) physical security equipment. The size of the security equipment Russian export market seems to be very small due to (relatively) low quality standards. Low-cost security systems are mainly imported from China, Taiwan and Korea, while high-end equipment (like premium access control systems and security devices) are imported form the US, Europe and Japan[88].

However, their domestic market shows rapid developments in terms of value. The US Commercial service points out the constant innovation and price competitiveness within the Russian market.

Relevant public policies supporting the sector

Existing public policies supporting the Russian security equipment industry could not be identified. The US Commercial service states that the Russian regulatory environment for security products is very complex (e.g. mandatory certification by government agencies) and related to bureaucracy and lengthy decision-making processes.

[88] US Commercial Service, 'Russia: The Safety and Security Equipment Market'. January 2008.

3 Policy rationale and recommendations

3.1 Rationale for an industrial policy for the security industry

3.1.1 Security as a "public good"

Maintaining an adequate level of security within any society can be considered as a basic (pre-)requisite for establishing an environment in which individuals and companies are able and motivated to engage in economic activities and, hence, for growth and social welfare. In this sense, security is a basic public good which generates positive social externalities and, equally, inadequate provision is associated with negative externalities.

In the context of globalisation, where economic policy (and social policy, also) is frequently directed towards facilitating the movement of goods and services, finance and people, the economic opportunities created through such liberalisation can be associated with negative risks from corresponding easing of controls on 'bad' flows (e.g. terrorism, counterfeit goods, drugs, illegal immigration etc.) Thus, increasing need for security provision can be viewed as a negative outcome of economic growth and global integration. Equally, increased economic and social integration can be seen to raise the level and extent to which security issues can spill over from one area to another; for example between different economic activities or between different countries and regions. Arguably, this raises the need for the greater adoption of common approaches and standards in security provision, for example in terms of greater EU-wide commonality in security policies and at a wider global level also.

If security is a public good, the question that arises is: who should be responsible for ensuring that adequate security is provided for society as a whole, for economic agents, and for individual citizens? At a public policy level, a strong level of debate exists over expectations regarding the level of security that should be provided and, at the same time, over the appropriate allocation between public and private responsibility for providing – and paying for – security. Clearly, there are areas where public authorities take upon themselves the responsibility for security provision and in turn for public expenditures and investments for security purposes. At the same time, many areas of security remain a private responsibility. In between, are those areas of security where responsibility is imposed on private agents through legislation and regulations; *de facto* an indicator that public authorities consider that private agents - left to make their own decisions - do not maintain security levels corresponding to the optimum for society as a whole. Similarly, insufficient private investment in security-related research relative to the social optimum is a justification for public support for security research.

3.1.2 Complexity of measuring the value of security investments

A difficulty for both public and private actors is that, while the costs of investments in security can be measured, it is extremely difficult to evaluate the corresponding value that results from these investments (i.e. the return on investment). This is particular the case, given the uncertainty and unpredictability associated with many security threats. Though it can be obvious when security investments 'fail' to prevent a security threat occurring, it can be far more difficult to ascertain when a security investment has succeeded (e.g. by deterring a threat). At the end of the day, it is the terrorist or the criminal that knows if an investment in security has 'provided value', but not the person making the investment. In other words, while it is possible to measure the efficiency of security (i.e. the resources put into security) it is much more difficult to estimate the effectiveness of security (i.e. how well the resource performed).

The fact that the costs of investments of security are apparent, whereas the value is not, is one reason why it is argued that businesses do not sufficiently invest - from either a private perspective or from a public perspective - in security. Moreover, as security does not usually deliver a benefit to the financial 'bottom line' it is an easy item to identify when companies seek to cut costs, specifically in the currently difficult economic times.

3.1.3 Market conduct failures (market power and competition)

Barriers to market entry

An important feature of many of the security segments analysed is that they are characterised by a fairly concentrated industry structure with a limited number of key players in the sector. This is particularly the case both at the top or high-end of the security market (i.e. for highly specialised/complex and/or large equipment and systems) and also for low-end, mass-market security equipment and systems. In the case of the latter, this appears to reflect the combination of a market that is cost/price driven and economies of scale in production of security equipment and systems. For the former, a variety of factors can be identified that contribute to this situation, such as the very large investments that are often required in technological development (combined with proprietary rights over technology) and the relatively high concentration of demand (both in terms of share of demand and limited number of customers). Overall, there appear to be very important barriers to entry to many segments of the security industry.

It is not the purpose of this report to identify whether there are specific competition issues related to the structure or the security industry. However, with respect to the top or high-end of the security market, market entry barriers appear to exist at two levels:

- First, the sector is characterised by specialised SMEs that are often technology developers (or set-up to commercialise specific technologies) and/or serve specific niche markets. Such companies often have limited access to the market for larger scale public (and quasi-public) and major private security equipment and systems contracts. Accordingly, as noted in Section 2.2.4, they may well either licence there technologies to – or be acquired by - larger market players (e.g. dedicated equipment integrators[89]);

[89] See Section 2.1.5 for a definition/description of 'dedicated equipment integrators'

- Secondly, as noted in Section 2.2.2, there are a number of trends shaping and structuring demand that are leading to larger and more integrated security contracts/projects. Such developments would appear to strengthen the position of the major systems integrators vis-à-vis dedicated equipment integrators. A possible consequence in the longer run could be further consolidation in the future among dedicated security equipment and sub-systems providers.

Overall, it appears extremely difficult for SMEs to grow significantly, which is reflected in a general absence of medium-to-large companies in the security equipment sector. Moreover, even major dedicated equipment integrators may face increased difficulties to supply directly to procurers of major systems if, as expected, the trend towards more integrated security systems persists.

Intellectual Property Rights

Weaknesses in international IPR systems have been pointed to as an issue of concern, specifically in relation to China where it is claimed that it has utilised 'backward engineering' to develop security equipment. Given the high investment costs involved in the development of security equipment, this type of activity can clearly undermine the competitive position of those companies that invest heavily in security technology development.

There is perhaps, also, a broader issue that arises if 'security' concerns – which is by and large considered as a 'rich country' issue – becomes a more generalised phenomenon; certainly, there is some suggestion that future long-term growth markets may increasingly be found outside today's traditional major markets. This is likely to increase demand for 'low cost' security solutions that are available at prices that are affordable in countries and regions with lower income levels. Although it might be stretching the analogy too far, in the same way that 'health' is considered a public good and where there are strong arguments that 'rich countries' benefit from health improvements in poorer countries, the same can be said for security, also. Thus, in the same way as there is considerable public debate over the correct system for protection of IPR for pharmaceuticals while also enabling poorer countries to have access to the drugs and medicines they need, perhaps a similar debate is required in the field of security. At least such a debate may come up with solutions that prevent the potential large-scale undermining of IPR, and the loss of potential markets to 'low cost' generic providers.

Public procurement

Either as a direct purchaser of security equipment or, indirectly, through their role in setting or implementing regulations that determine private procurement decisions, national governments play an important role in shaping the market for security equipment. Within the EU, differences in national procurement rules are seen as a contributing factor to fragmentation of the European market for security equipment, in particular where such public procurement behaviour appears to favour national providers. Similarly, US procurement procedures are pointed to as a means by which US companies are favoured over potential competitors, thus restricting access or placing at a disadvantage EU companies. Though there may be legitimate reasons why a country might favour a national supplier over a foreign competitor, both the fragmentation of European markets and a separation of US and European markets, is economically inefficient and restricts competition.

3.2 Possible policy responses

From the insights provided by the analysis of the six segments covered by the report and the general assessment of the industry as well as from discussions with stakeholders, we can tentatively put forward some possible policy responses.

3.2.1 A European 'vision' for security through enhanced public-private dialogue

It appears that there is a lack of mutual understanding between policy makers and the security industry sector. On the one hand, security industry representatives point to the lack of clarity on European security policy and requirements. On the other, it appears that on the demand side (i.e. security equipment procurers and users), particularly in the public sector, need to be better informed (educated) about security technologies and capabilities[90]. In this respect, it appears that greater dialogue is called for to match the ambition of public policy makers with the potential and possibilities of the private sector (security industry and service providers). Such public-private cooperation could serve to map out a European 'vision' for security that would support the (EU) security industry and relevant stakeholders to more effectively (and efficiently) contribute to meeting the EU's security priorities.

➔ **European Security Congress** organised as an annual or bi-annual event to bring together leading policy makers, industrialists and other relevant stakeholders to discuss security priorities and future security agendas[91]. The purpose would be not only to promote dialogue, debate and discussion among participants but also, more broadly, to raise the awareness of security issues, and factors shaping the security market and industry.

➔ **Security Policy Forum** would establish a permanent platform for dialogue and exchange between policy-makers and regulators, industry and service providers, etc. to bring together industry and user demands with the aim of building a coherent public policy framework. Therefore, the Security Policy Forum would be established as a continuous platform to promote public-private dialogue on security issues and ongoing development of a European 'vision' for on security issues and policy.

The two above mentioned initiatives could contribute to setting out a European 'vision' for security. At the same, they could provide the context (e.g. in terms of setting policy priority benchmarks) and institutional setting for monitoring and updating of a European 'roadmap' for future security capability requirements and technologies, which could contribute to reducing uncertainties over future policy and market developments while supporting the development of more consistent and national level security policies. In this respect, an initial 'roadmap' has been developed by ESRIF in the form of the European

[90] Here a comparison can be made between defence/military users that are experienced in defining future technology/capability requirements and civil security users that are less experienced in identifying and defining their technology/capability requirements. This shortcoming could be addressed through specific training initiatives (see Section 3.2.10) and could also be aided through the development of enhanced procurement procedures, including 'best practice' guidelines (see Section 3.2.6). At the same time, enhanced opportunities for dialogue with industry itself could promote greater awareness among procurers/users of security products and services.

[91] This could be based on the format used for the World Economic Forum's Annual Meetings ("Davos" Meeting)

Security Research and Innovation Agenda (ESRIA) which, as they note, will require regular evaluation and revision in response to changing circumstances.

➔ **Strengthened representation of the security industry.** The security industry in its modern form has largely developed over the past two decades and, as such, it is relatively immature and without a well-established industry structures. One consequence is the need to strengthen the representation of the security industry, particularly at a European level, in order to enhance public-private dialogue[92]. In this respect, it seems necessary to reinforce representation of the security industry in a way that accommodates the wide range and diversity of industry players. Thus, it is not only the major players coming from the defence sector that are of relevance but also players coming from other fields of activity (e.g. more traditional security industry segments and 'new' fields such as ICT) including SMEs. Moreover, the role carried out by national security associations could also be taken into account and, as representatives of the security industry in the respective Member States, they could also contribute to establishing a new representative framework.

3.2.2 An industrial policy for the security sector

Although the EU has an active role in shaping security policy in specific domains (e.g. aviation security) it remains the case that there is an absence of a comprehensive policy framework for security and, as a consequence, a more coherent outline of the direction of European security industrial policy is needed. Both the European 'vision' for security and the monitoring and updating of a European 'roadmap' for future security capability requirements and technologies emerging from the European Security Congress and the Security Policy Forum would provide underpinning elements for the development of a more 'holistic' approach to industrial policy directed towards the security industry[93].

An industrial policy for the security industry should reflect the balance between industry capabilities (e.g. product portfolios, technologies, etc.) and requirements (technical standards, IPR, etc.), policy priorities and market demands (e.g. security missions, performance standards, competitive prices, etc.), and the underlying rationale of creating conditions that are supportive of the competitive development of the security industry and its ability to respond to global challenges now and in the future.

An assessment of European supply and demand conditions for security is already among the outcomes of the work of ESRIF and its European Security Research and Innovation Agenda, which is meant to link security research with security policy-making, creating opportunities for a more coherent research programming and funding, leading to better

[92] it can be noted that the European Organisation for Security (EOS) was created in 2007. EOS is an umbrella organisation for stakeholders, bringing together security industry players for them to address the opportunities and weaknesses of the EU security market together with the EU institutions, Member States, users and operators. However, EOS is a relatively new organisation and its current membership consists predominantly of the main larger actors in the defence sector that are also involved in the security field.

[93] Despite the common elements they share, a potential Security industrial policy would differ from a Defence industrial policy, as the two sectors are characterised by differing structures and dynamics, unequal market maturity, more customer fragmentation in case of the security industry, etc. Moreover, actors in the security market are not only defence-related players but include also ones coming from more 'traditional' security backgrounds (e.g. CCTV, fire and burglar alarms, perimeter protection, etc.) as well as more recent entrants from outside the defence-security domain (e.g. information and communication technologies, etc.).

innovation and to the strengthening of the industry, its competitiveness and the role of providers of security technologies and solutions[94]. Moreover, it is our understanding that ESRIF has not only examined the situation of the security sector from a research and technology perspective but also has put some initial attention to possible industrial policy and innovation instruments, including potential operational mechanisms for budgetary support.

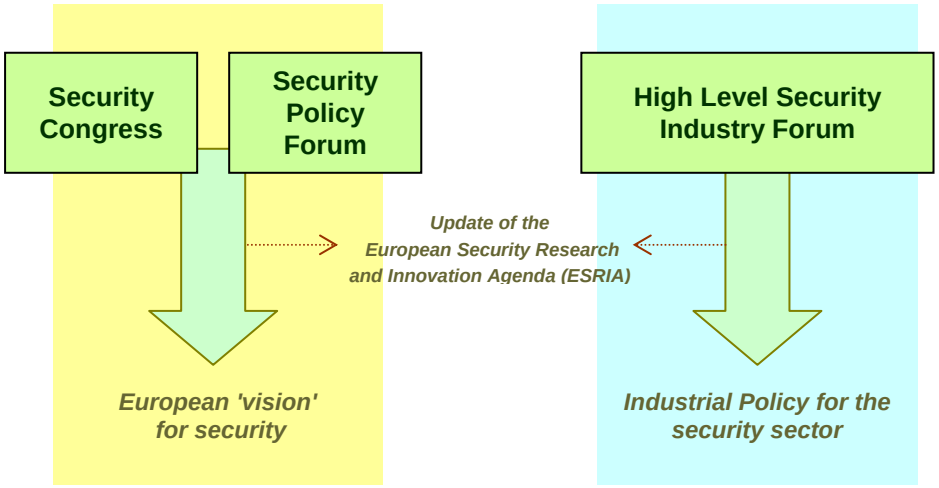
Notwithstanding the recommendations put forward by ESRIF, in order to further address the lack of a comprehensive security framework, the following initiatives may be proposed:

- **High-Level Security Industry Forum**, to develop the basic principles and objectives of a comprehensive industrial policy for security. The Forum would bring together high level representatives from the security industry, EU institutions, governments, social partners, experts, etc. with the objective of developing a European policy framework and policy initiatives directed towards enhancing conditions within the security market and strengthening the capabilities of the security industry to effectively respond to EU (and global) security requirements and needs. The implementation of the Forum as a platform for discussion could draw on experience from similar initiatives in other sectors, for example the pharmaceutical sector (Pharmaceutical Forum[95]) or the defence sector (Defence Industry Forum).The Forum could address relevant topics for the industry.

- **Identification of the European Security and Technological Industrial Base (ESTIB).** Although the STACCATO Project[96] was supposed to undertake a mapping exercise of the industry, it is acknowledged that the 'picture' is not yet clear. Therefore, work is still necessary if future policy is to be based on a well-founded understanding of the security industry. The identification of the European Security and Technological Industrial Base (STIB) and the mapping of its competences is, therefore, required. This would aim to provide not only an assessment of the security industry *per se* but would acknowledge, also, that the industry is based upon and supported by a much broader technological and industrial base.
  Such a mapping could also form the point of departure for a comprehensive assessment of the industry (e.g. an in-depth SWOT type analysis), helping policy makers to define the research, technology and development priorities at EU level. Accordingly, this exercise should cover all relevant technology, system and service areas as well as all involved industrial players in a cross-border analysis covering all EU-27 Member States.

[94] Source: ESRIF website (http://www.esrif.eu/objectives.html)
[95] See http://ec.europa.eu/pharmaforum/docs/final_conclusions_en.pdf
[96] Stakeholders Platform for Supply chain Mapping, Market Condition Analysis and Technologies Opportunities (PASR 2006). See: http://www.asd-europe.org/content/default.asp?PageID=34

Figure 3.1 Suggested European framework for security policy formulation



3.2.3 Standards and certification

Industry analysis and stakeholder consultation have made clear that one of the most significant problems the industry is facing is the absence of European and common international standards for security. The following policy recommendations aim at providing a framework for performance standards that are aligned to security policy, and for technical standards that promote greater consolidation of currently fragmented markets. Moreover, possible European leadership in the international (global) development and adoption of standards in the area of security could be potentially advantageous for the European industry and contribute to enhancing the its global competitiveness.

For the purpose of developing widely recognised and adhered to standards, the involvement of all relevant stakeholders for the setting up of standards is crucial, including not only major players from the public and private sector but also SMEs and the research community. Moreover, technological change and the reactive nature of the industry require European standards organisations to adapt quickly to market demands while, at the same time, promoting cooperation in the setting up of international standards, particularly with US organisations.

Standards are facilitators to market access for innovative products, services and processes but they are also diffusion mechanisms for R&D knowledge. Moreover, while technical standards ensure consistency in the quality and safety of security products, performance standards improve effective utilisation and confidence in users[97]. Therefore, taking account of the characteristics of the security industry and technologies, and the nature of perceived shortcomings in the functioning of the security market, it appears convenient to suggest a differentiated approach for both technical and performance standards.

[97] Commission Communication COM(2007)374 of 4.7.2007, *Mid-term review of industrial policy*, available at:: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/mtr_in_pol_en.pdf

Technical standards

Formal procedures for the creation of technical standards already exist, for instance, the requests by the European Commission for the development of standards to support a particular industry sector through specific legislation. However, these procedures often require significant amounts of time and may be inappropriate for the security sector for two reasons:

a) The underlying speed of technology development (too slow in a rapidly evolving sector, both from a supply perspective and a demand perspective);
b) The need to respond quickly to market demands, particularly when new security threats arise.

With the above-mentioned context, there is a risk that too formal and rigid structures for setting up technical standards may impede meeting security requirements and innovation. Moreover, such a rigid structure could be an extra barrier for new market entrants. Therefore, an industry-based solution for the development of technical standards may be more appropriate. In this respect, the following initiatives should be taken into account:

➔ **Strengthening of European Standardisation Organisations' work, with clear mandates from public authorities in the security field.** As security standards cover more than a single strategic area, public authorities could initiate and call for the development of new standards in the sector, providing clear mandates to European Standardisation Organisations (ESOs) based on priorities set out in the European 'vision' for security.

Of the main ESOs, CEN[98] has recently created a new Technical Committee on 'Societal and citizen security' (CEN/TC 391)[99]. The Committee is at an early stage of its work, setting the necessary scope and business plans. In this respect, the European Commission (through DG Justice, Freedom and Security) is pushing for and financing work in the fields of supply chain and water security, defence against terrorism and border management. Similar initiatives could support the different strategic areas identified by the Security Congress or the Security Policy Forum. ETSI[100] currently produces internationally-applicable standards for Information and Communication Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. The main area of work related to security undertaken by ETSI cover mobile/wireless communications, emergency telecommunications, information technology infrastructure, smart cards, fixed communications and security algorithms[101].

➔ **European Security Standards Institute:** Notwithstanding ongoing activities, such as those of CEN and ETSI noted above, some consideration may be given to whether or not there is a need to establish a means for actively promoting the development and adoption of European security standards. Based on the assessment in the report, if

[98] CEN (European Committee for Standardisation): www.cen.eu
[99] This has been created to take over the duties previously carried out in CEN's working group BT/WG 161 'Protection and security of the citizen'.
[100] ETSI (European Telecommunications Standards Institute): www.etsi.org
[101] ETSI White Paper No. 1 "Security for ICT - the Work of ETSI" available at: http://www.etsi.org/WebSite/document/Technologies/ETSI-WP1_Security_Edition2.pdf

such an initiative is taken it should be an industry-based organisation oriented towards self-development of technical standards. The ETSI (European Telecommunications Standards Institute), and its framework for development of standards, could provide a pertinent example of this type of approach. One possibility could, therefore, be for ETSI to play a stronger and broader role with respect to security standards.

➔ **New Approach legislation for security:** This legislative technique, already used regarding the Single Market for goods, puts in place an innovation-friendly regulatory framework where technical standards and specifications are developed by the companies or the respective interested parties themselves and updated accordingly when new technological developments occur. The reliance on voluntary standards may also help the security industry to remove further regulatory barriers to innovation[102].

Performance standards

In relation to performance standards[103], a formal approach to the establishment of a standardisation framework could be based on the following initiatives:

➔ **Development of a European Security Standardisation Handbook**: Based on the initiative already in place in the defence sector (with the existence of a European Handbook for Defence Procurement[104], produced in the framework of CEN and sponsored by the European Commission), the Security Handbook would contain a selection of performance standards and standard-like specifications in order to improve effectiveness, efficiency and interoperability at EU level. As with the Defence Handbook, the future European Security Standardisation Handbook would go through the subsequent phases:

- *Stage 1* – Initial handbook to identify international and national policies and procedures in the security field and to create a database with a list of the current standards in place;
- *Stage 2* – Selection of standards by identifying the relevant processes and technologies widely used in the security field;
- *Stage 3* – Recommendations, list of best practices guidelines and final completion of the handbook.

➔ **The creation of a European Security Label** would increase confidence and act as a catalyst for investment by attracting new investors to the security industry. As described by ESRIF, an EU security label should "stimulate innovative technologies that provide the best value for money in the long term, while ensuring interoperability. … It could become a common reference point for security providers,

[102] Commission Communication COM(2008) 133 final of 11.3.2008, *Towards and increased contribution from standardisation to innovation in Europe*.

[103] As an example of performance standard, the ASTM E2520 - 07 Standard Practice for Verifying Minimum Acceptable Performance of Trace Explosive Detectors (see http://www.astm.org/Standards/E2520.htm); as well as those performance standards set out in EC Regulation 1448/2006. See, for example, the requirements in regards detection rates or image quality as explained in the following Euromed's aviation security seminar presentation: http://www.euromedtransport.org/fileadmin/download/Aviation/Workshops/Paris-ECAC/Presentations/11-Presentation_Banitz.pdf.

[104] See http://www.defense-handbook.org/

end-users and legislators by creating a coordinated accreditation process for test facilities and auditors, while encouraging appropriate organisations to apply."[105]

➔ **A flexible system for performance standards in a dynamic context**. This would imply a system for the creation of performance standards based on on-going dialogue within the proposed Security Forums (see above) in order to adapt, change and update standards according to new industry demands and requirements.

Standardisation practices and testing infrastructures

The setting-up of standards at EU level should be accompanied by improved and more standardised approval and certification procedures based on a uniform technical level of testing in the security field (involving, for instance, technical harmonisation and quality assurance, as a set of minimum requirements for testing). An approval and certification scheme should aim to ensure that adequate capacity is available to meet EU requirements so that significant delays are not incurred. Moving to greater mutual recognition between countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and certification bodies (e.g. testing laboratories) could raise the efficiency of the system and support EU security technology development.

➔ **EU level testing and certification scheme and improved approvals and certification infrastructure**, with the aim of creating a testing protocol and the necessary infrastructure (dedicated labs or testing facilities) to carry out testing practices of security products. This will have the general objective of either generating new certification strategies or harmonising the existing ones.

➔ **Exchange of formal and informal information on testing facilities** and their portfolio of expertise, as well as the exchange of best practices with the objective of increasing transparency and cooperation. To this aim, initiatives such as the newly created CREATIF Network (Network of Testing Facilities for CBRNE detection equipment) should be enhanced and promoted.

➔ **Fast-track system for approval of priority technologies and equipment.** Due to the need to react rapidly to changing demands of the market (and society in general) when new security threats are identified, a fast track system for approval of technologies and security equipment and systems could be implemented. When a new security threat is identified, such an approval system could assist in identifying which existing technologies and types of equipment and systems are appropriate and to quickly evaluate and approve new and innovate approaches as they are developed. This fast-track approval procedure could be based on the notion of 'fit-for-use' rather than on a complex formal approval system.

3.2.4 Liability protection

The US SAFETY Act allows security equipment providers – particularly those supplying high-end security solutions – to benefit from a dedicated liability regime. It is argued that this has the effect of limiting investment risks for the industry, hence promoting

[105] ESRIF Intermediate Report, September 2008. Available at: http://www.esrif.eu/documents/intermediate_report.pdf

innovation and technology development. At the same time, the associated US certification regime provides a widely recognised 'seal of approval' for equipment and systems (see previous point).

Currently there is no equivalent system in Europe to that provided under the SAFETY Act, and representatives from the EU security sector (both equipment suppliers and users) argue that this creates considerable uncertainty as to the potential liability of security equipment users and suppliers in the event of breach/failure of security and has a negative impact on investment in the European security sector[106]. Moreover, proponents of a dedicated liability programme suggest that legislation and supporting mechanisms dealing with the proportionality of risk allocation would help to create a more robust strategic partnership between governments and the industry. Therefore, closer public-private cooperation would be able to encourage security innovation while mitigating potential terrorist threats.

In the absence of an EU-wide initiative on liability protection, there is potential for Member States to develop their own national liability protection programmes; for example the Society of British Aerospace Companies (SBAC) is promoting the establishment of a UK Liability Protection Programme which appears to be based on the US liability regime[107]. However, there is an inherent problem with the pursuit of national (Member State) level approaches to liability protection as there is the risk that such an approach would potentially contribute to further reinforcement of existing market fragmentation. Specifically, dissimilar national programmes would result in different market conditions (i.e. associated commercial risks), further inhibiting the creation of a single European security market.

From the above, it would appear that the development of an EU-wide approach to liability protection aimed at a more uniform system would seem appropriate. However, without further analysis of the legal situation –which is beyond the scope of this study– it remains unclear as to whether such a programme is warranted, or is feasible from a legal perspective, given the European context. Accordingly further analysis is warranted on this issue, together with an assessment of both the advantages and disadvantages of introducing such a programme in the EU.

➔ **Liability support for new security technologies:** legal liability protection could be provided to technology developers under a regime protecting those sellers of 'qualified anti-terrorist technologies'. Such a regime could grant liability support on a temporary basis depending on the effectiveness of the technology in place. In this respect, legislation could be also based on the US Support Anti-terrorism by Fostering Effective Technologies Act – Safety Act.

[106] For an assessment of the European liability situation with respect to terrorism, see the Report of the 11th International Liability Forum; available at http://www.munichre.com/publications/302-05501_en.pdf

[107] See http://www.sbac.co.uk/community/dms/download.asp?txtPageLinkDocPK=18515

3.2.5 Protection of IPR

To meet evolving security requirements and to remain competitive the security industry is required to invest heavily in technology development and innovation and, accordingly, protecting the return on this investment through protection of intellectual property rights (IPR) is an important concern. In this respect the security industry is in the same situation as many other sectors that invest heavily in research and technology development as a basis for enhancing their competitiveness. A partial differentiation does arise, however, if inadequate IPR protection is translated into lower investment and, in turn, lower levels of security for society as a whole. In this context, there is perhaps some additional justification for support for the security industry for international (global) protection of Intellectual Property Rights.

➔ **The creation of a European fund to support protection of IPR**. In common with many other sectors, some security companies – particularly SMEs – argue that they are simply unable to enforce IPR (e.g. patents) at an international level, and that they require additional support in order to be able to do so.

➔ **Better IPR enforcement** based on the recommendations of the IPR Enforcement – Expert Group[108] that could be implemented at EU level include:

- Zero tolerance policy in IPR enforcement regarding security equipment and technologies, sending a clear message that any abuse would be prosecuted by EU and national authorities;
- Security research and innovation support programmes should include effective provisions for IPR enforcement and promote Intellectual Asset Management (IAM)[109] in their guidelines;
- Training (for SMEs, enforcement authorities, for business support organisation staff, etc) regarding management and implementation of IPR;
- Coordination measures such as the establishment of co-ordination offices for IPR enforcement issues, both at a European and at national levels;
- Funding of IPR enforcement and Evaluation in the security field;
- Promoting the IPeuropAware initiative[110] (established in 2007) with a specific support service for security equipment manufacturers – the initiative has already created the www.InnovAccess.eu website to give support to SMEs in IPR matters;
- Promotion of specific IPR enforcement measures at Member State level[111].

[108] IPR Enforcement – Expert Group Report: *Making IPR work for SMEs*: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/ipr_conference_27_04_2009/report_making_ipr_work_for_sme.pdf

[109] Intellectual Assets include the legally recognised forms of intellectual property (patents, trademarks, copyrights, etc.) as well as a wider group of intangible assets owned by and enterprise (brands, goodwill, know-how, trade secrets, technical information, etc.). IAM fosters the management and exploitation of these issues as an strategic component of innovation policy and as a major source of competitive advantage.

[110] The initiative is a FP7 funded project which has developed the www.InnovAccess.eu website to give support to SMEs and other stakeholders in IP matters.

[111] In this respect, and although not tailored to security, the document *Making IPR work for SMEs* prepared by DG ENTR contains a list of best practice initiatives that could be considered. The document can be accessible at: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/ipr_conference_27_04_2009/annex_b.pdf

➔ The already existing **EU-US Action Strategy for the Enforcement of Intellectual Property Rights** could be tailored to security. Since 2006, the European Commission is fostering improved cooperation between customs authorities through the exchange of information and personnel, stronger joint action vis-à-vis problem countries and greater cooperation with the private sector. The implementation of the aforesaid Strategy in the security field would aim at reducing technology-related piracy, promoting the use of properly licensed technology and respect for patents.

➔ **Development of policy towards 'generic' security requirements** for lower income regions could also be considered. Taking into account that future long-term growth markets may be found outside today's traditional major markets, demand for 'low cost' security solutions may increase. If security is considered to be a public good, a debate over the correct system for protection of IPR for security (enabling poorer countries to have access to those security solutions they need) could be required. Such a debate may propose solutions preventing a potential undermining of IPR and the loss of potential markets to 'low cost' generic providers.

3.2.6 Market access and procurement systems

The public sector is a major purchaser of security solutions and often has a strong influence on purchases in other key segments (e.g. aviation, maritime, critical infrastructure, etc.). However, there is concern that public procurement systems for security equipment and systems are insufficiently transparent and that countries may explicitly (e.g. US exclusion of contracts with foreign entities) or implicitly limit market access to 'local' suppliers. In addition, public authorities can influence market access through other mechanisms; for example, constraints can be placed on exports of security equipment where they incorporate dual-use technologies that are classified as "sensitive". A related issue is differences in the approach adopted by authorities when distinguishing 'defence' from 'security' for procurement purposes, since different regimes and rules can apply depending on the distinction made.

More broadly, as noted in Section 3.2.1, there appears to be a need for public sector purchasers and users of security equipment to be better informed (educated) about security technologies and capabilities.

➔ **Clarification of 'defence' versus 'security'** procurement procedures and responsibilities. The objectives here would be twofold: first to clarify the extent to which common or differentiated procurement procedures should apply for defence as opposed to security equipment, systems and services (and the scope of procurement covered by each of these categories); secondly, to clarify the procurement responsibilities of different administrative bodies with respect to each category. This should enable suppliers to have a clearer understanding of the organisation and relevant procurement systems for security equipment, systems and services.

➔ **European Security Equipment Market Initiative.** This would aim to provide increased transparency of (public) procurement procedures and could, for example be based on the already existing initiatives related to the European Defence Equipment

Market[112]. Such an initiative could enhance clarity and comprehensibility of procurement procedures while fostering competition in the security equipment market, with European countries committing themselves to procure security equipment from each other if the offer is the best available, instead of contracting with a national supplier.

In contrast to procurement for defence markets (almost exclusively in the public sector domain) and the European Defence Equipment Market initiative, a procurement initiative covering security markets should also take into account those (private) markets highly influenced by public policy and regulations and/or in priority security areas.

In this context, greater transparency could be achieved through the establishment of a **European Handbook for Security Procurement**, that could be used as a reference for a more harmonised EU-wide public procurement schemes and which could include:

- A **'Code of conduct for security procurement'**, committing the subscribing Member States to maximise equal opportunities for all suppliers through the setting of specific and objective criteria for the selection of bidders and the awarding of contracts;
- A **'Code of best practice in the security supply chain'**, which could, for example, encourage the use of small and medium-size companies as subcontractors for the bidding of contracts, increasing competition in the market. This may contribute to offset the current market situation by which SMEs are often excluded from the market for many major security projects/contracts (a consequence of current systems that tend to foster close links between large system integrators and procurement agents);
- A **'List of best public procurement practices'** in the security field, serving as an example for future procurement activities.

➔ **Lead Market Procurement Network for Security**. This could be an element of a broader Lead Market Initiative for Security (see Section 3.2.7). The aim of existing lead market public procurement networks is "to enable public procurers (national, regional and local authorities and bodies governed by public law) to improve their knowledge about innovative solutions that are available or being developed by suppliers, to allow a better coordinated and articulated dialogue with suppliers about the future needs of contracting authorities, and to realise the benefits of European cooperation in exchanging experience in procurement practices and in undertaking joint or coordinated actions." [113] In the context of security, the scope of entities covered by such an initiative could be extended to also include 'mixed' public-private sectors (e.g. utilities, critical infrastructure, etc.).

[112] For more information, please see European Defence Agency document at: http://www.eda.europa.eu/WebUtils/downloadfile.aspx?fileid=43

[113] See http://ec.europa.eu/enterprise/policies/innovation/policy/lead-market-initiative/public-procurement-networks/index_en.htm.

3.2.7 Research and innovation

A new European focus of security research and innovation can lead to regional economic development, driving competitiveness of certain regions and countries, as well as of the European security industry. Moreover, it is worth noting that the security industry is experiencing a shift from manufacturing towards services and R&D, which requires a new research and innovation policy approach to deal with the changing demands of the industry.

Without seeking to undermine the current support for long-term fundamental research, there is concern that current research initiatives are insufficiently aligned to more immediate security capability requirements. Moreover, the slowness at which research programmes may be adapted means that it is difficult to rapidly mobilise public research funding in response to new security threats. With this scenario, it appears vital to stimulate and create a proper innovation framework in the security domain and establish fast-track development procedures for new market technology requirements. To this end, the following may be proposed:

- ➔ **An EU Security Programme**, bringing together and coordinating activities as an umbrella for ensuring synergies and coherence in research and innovation actions. The EU Security Programme would set guidelines for research priorities, reflecting those highlighted in the European 'vision' as well as the industrial policy for security. It will also be understood as a channelling platform for funding, hand in hand with RTD and innovation funding vehicles such as Framework Programmes[114].

- ➔ **Lead Market Initiative for Security**. Based on the existing European framework for Lead Market Initiatives (LMI), this would build around adoption of legislative measures designed to foster innovation and avoid imposing burdens on innovative business and other organisations; mobilising public authorities to act as 'launching customers' by promoting the use of Public-Private (PP) practices supportive for innovation (see Section 3.2.6 and Section 3.2.8); improving standardisation, labelling and certification (see Section 3.2.3); and other complementary measures[115].

- ➔ **European Security Technology Platform.** The creation of such a platform should be considered as an exchange platform to allow for the development of coherent solutions in specific and relevant knowledge domains in Europe. The platform would cover several technological domains (e.g. observation systems, physical protection, biological warning systems, information analysis, human performance, etc.), and could be based on the JTI (Joint Technology Initiative), put in place under the FP7, or

[114] A similar initiative has been proposed by EOS for the establishment of an EU Security Programme aiming to set up a coherent framework reflecting sectoral needs and diverse technological capabilities. This Programme would embrace different Sectoral Programmes or Development Platforms dedicated to specific areas (border control, critical infrastructure, security of transport, etc.) having their own agenda and constituency, adapting new technologies to security requirements and market needs. Through public and private participation, this umbrella programme could drive research and innovation in specific sectors and could act as a channelling way for EU funding, federating existing and future initiatives and coherently focussing resources and mechanisms. Source: EOS, *Priorities for a future European Security Framework*, August 2009.

[115] Commission President, José Manuel Barroso, proposes a lead market initiative for internal security. "Political guidelines for the next Commission" available at: http://ec.europa.eu/commission_barroso/president/pdf/press_20090903_EN.pdf

other similar initiatives in other fields, such as the European Space Technology Platform[116] or the European Robotics Technology Platform[117].

➔ **The setting-up of field-labs for the strengthening of innovative products and systems for security**. One key objective would be to have strong and better interaction between supply and demand structures, with an active engagement of security solutions end-users, the industry and R&D institutions required. Therefore, the proposed field-labs should be used as platforms for accelerating innovation in the security field, being environments for demonstration, validation and optimisation of innovative systems for security tasks as well as providing a bridge from R&D and innovation to market implementation. End-users of equipment should be the driving force of this innovation process, taking the lead by ensuring that new security solutions are adequately tailored to their specific needs. These labs should also function as exchange meeting points where all relevant stakeholders can take initiatives for joint implementation of improved solutions relevant for their daily work[118].

In addition, such field-labs are also a means to stimulate and encourage SMEs to enter the market, and for building a framework for cooperation and interaction between SMEs and larger players. This could serve to enable SMEs to build on their specific equipment and technical expertise so as to provide systems capabilities required by both small and large scale projects.

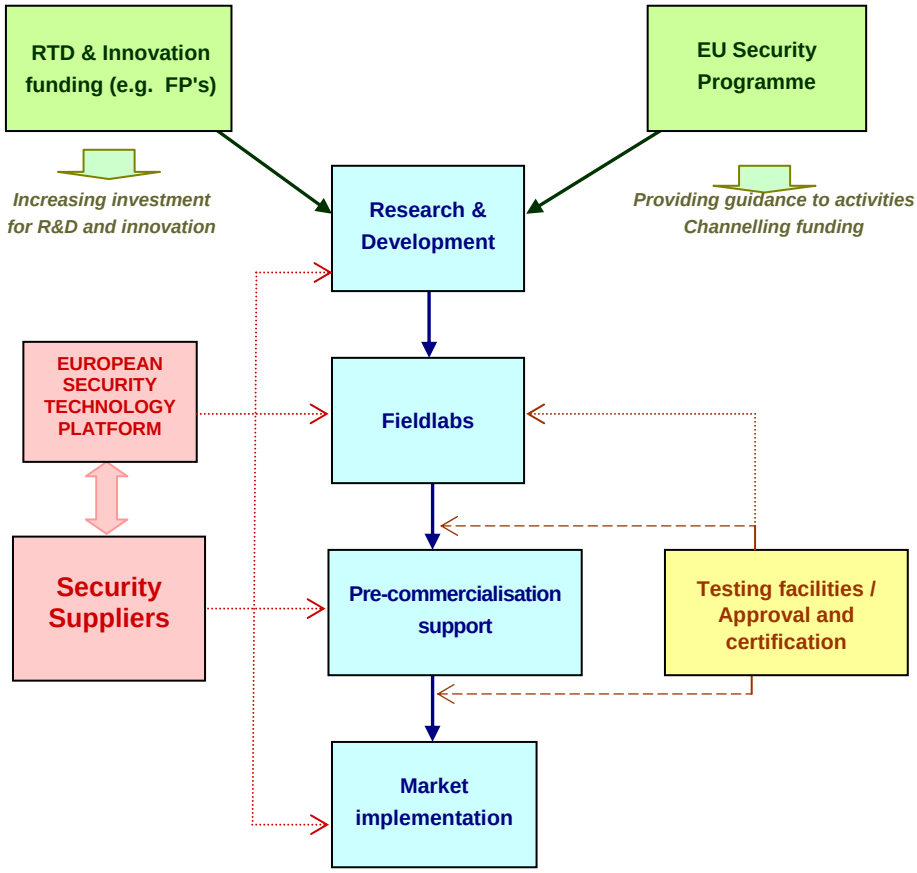
➔ **The creation of a specific Fund for EU Security & Resilience**, that could be used as a fast-track system to respond to the new security threats as they are perceived. This fund would provide public resources to research and innovation activities addressing new security threats that need a rapid mobilisation of research funding.

[116] See http://estp.esa.int/exp/E10430.php

[117] See http://www.robotics-platform.eu/cms/index.php

[118] An example of such an initiative is the "Pôle Pilote de Sécurité Locale" situated in Elancourt, France. It is created as a platform for research and experimentation of new security technologies for urban and local environments. See: http://www.ppsl.asso.fr/index.html

Figure 3.2 Suggested framework for security research, innovation and market implementation



3.2.8 Linking research to markets

Security equipment suppliers – notably smaller companies – have highlighted the difficulty of transitioning from technology development to full commercial development of products, with the outcome that companies will tend to licence technologies to larger players rather than enter into production themselves.

➔ **Revised public procurement rules and pre-commercialisation support.** Pre-commercial public procurement may provide a mechanism to bridge the gap from technology development to commercial production and initiatives already exist in this area[119]. The European Commission[120] has already emphasised the importance of public procurement in reinforcing the innovation capabilities of the EU whilst improving the quality and efficiency of public services. It also underlined the insufficiently exploited opportunities in Europe of pre-commercial procurement[121].

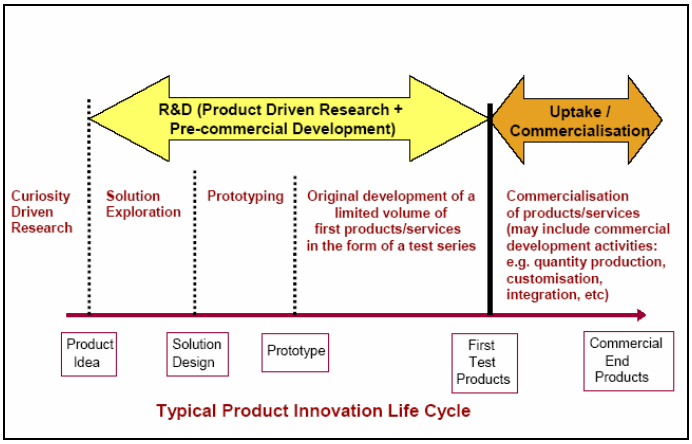
[119] See Commission Communication on *Pre-commercial procurement*, SEC (2007) 1668, and information available at http://ec.europa.eu/information_society/tl/research/priv_invest/pcp/index_en.htm

[120] COM (2006) 502 Final, Communication from the Commission, *Putting knowledge into practice: A broad-based innovation strategy for the EU*, dated 13 September 2006.

[121] Pre-commercial procurement is also seen as a way to bring supply and demand players closer to each other. If public procurers play their role as technologically demanding first buyers, they can drive innovation from the demand side while improving at the same time the quality and effectiveness of public services. Demand from the public sector can foster new and better innovative solutions to face new security challenges and threats. The key is the involvement of R&D procurement measures into 'traditional' public procurement strategies while reducing the risk involved and achieving better-value-for-money products.

The Commission Communication on Pre-Commercial Procurement[122] has further developed this concept and defines pre-commercial procurement to be the Research and Development (R&D) phase before commercialisation, as shown in Figure 3.3. In the context of security, however, consideration may be given to whether such a scheme should be limited to the public sector or could also be extended to those security priority areas in the private domain that are also highly influenced by public policy and regulation (e.g. critical infrastructure).

Figure 3.3 R&D versus commercialisation phase



Source: European Commission, COM (2007) 799 Final

➔ The **European Handbook for Security Procurement** (already mentioned) could also integrate pre-commercial procurement as a way of enabling European public authorities to innovate in the provision of public services faster and create opportunities for companies in Europe to take international leadership in new markets.

➔ **Field-labs**, already mentioned in the previous section, are also an instrument for bridging the gap between R&D (and related innovation activities) and market implementation.

3.2.9 Raising awareness and visibility of security issues and developments

Societal dimension of security

One aspect of security that is receiving increased attention is its societal dimension and the need for the inclusion of a 'human dimension' in security applications. From a product development perspective, this is reflected in the concept of 'privacy by design', by which any new solution must take into consideration aspects of privacy right from the beginning of the design of new security measures[123]. More broadly, however, a wider reaching assessment and dialogue on the implications of societal dimensions (and public acceptanc of security measures) for EU security policy, for the future development of security

[122] COM (2007) 799 Final, Communication from the Commission, *Pre-commercial Procurement: Driving Innovation to ensure sustainable high quality public services in Europe*, dated 14 December 2007.

[123] There exists also an analogous concept of 'security by design', which considers that security must be embedded in the technology and system development from the early stages of the conceptualisation and design.

applications, and for the competitiveness of the security industry is required. This could incorporate the following initiatives:

- ➔ **EU Platform for Societal Issues** linked to security could effectively support the integration of societal aspects (i.e. privacy, ethical, social and human issues) into the design of solutions and services. Such an initiative is proposed by EOS, which believes that such a body could assess and foresee future interactions of society (decision makers, security equipment operators, first responders, citizens…) with new security threats and the new technologies used to tackle them[124]. Such a platform could be integrated within the proposed Security Forum and its respective working groups.

- ➔ **European Security Label** (see above) being a reference point for suppliers, end-users and customers in general, should include a 'societal dimension' to security, incorporating the 'privacy by design' and the 'security by design' dimensions to security solutions designed and manufactured in Europe.

- ➔ **Assessment of the interaction between societal dimensions of security and development of the security sector**. One issue is the impact that the accommodation of societal concerns may have on the cost of developing and implementing security solutions. On the one hand, if as a result of societal concerns EU suppliers are obliged to provide more costly solutions then this may negatively impact on their cost competitiveness in third markets; though, alternatively, their may be competitive advantages stemming from the provision of more innovative solutions. From another perspective, societal concerns may have an impact on overall security levels if they mean that certain technologies are not permitted or where the volume of security equipment installed is reduced (e.g. where costs are higher and overall budgets are fixed). Although it is evident that fundamental human rights, for example, should not be set against cost and competitiveness criteria, the impact of societal dimensions on the development of security markets and the security sector appears to warrant analysis and debate.

Raising public awareness and understanding of EU security developments, policies, and solutions

Raising and maintaining awareness among private citizens, business and public authorities of security developments is seen as an important area for public policy intervention. As is the promotion of greater awareness and understanding of the potential of security equipment, systems and technologies to deliver necessary capabilities to meet requirements (missions) in a variety of security fields. Particularly for the private sector, there appears to be a need for efforts to maintain the concentration of businesses attention on security issues and developments in security solutions, while acknowledging the impact of security on 'bottom-line' performance. There is, therefore a role for public campaigns, programmes and projects to promote this awareness and understanding and, where necessary, to address misleading perceptions.

[124] EOS, *Priorities for a future European Security Framework*, August 2009.

➔ **Targeted awareness programmes** could be implemented to increase awareness of security threats and security solutions devoted to mitigating these threats. These programmes should reach out to the larger public, to not only raise awareness but also to make information available on security technologies and solutions, and on the processes and procedures put in place to respond to security threats, risks and vulnerabilities, and to encourage debate the acceptability of potential technological solutions, procedures etc. In this respect, similar initiatives to the CPSI project (Changing Perceptions of Security and Interventions, under FP7)[125] could be supported.

➔ **Citizens' communication and information service** to inform and prepare the public in case of a major emergency or security incident.

International promotion of EU approaches to security and enhancement of the visibility of the EU security industry

Being conscious of the international dimension of security issues, awareness raising initiatives could take on a broader international aspect that would promote greater understanding of EU security policy and approaches. At the same time, this would provide an opportunity to 'showcase' EU solutions and raise awareness of the technological expertise and strengths of the EU security industry in international markets.

➔ The development of an **International Security Programme**. This initiative would aim to increase international awareness of EU security approaches and initiatives (e.g. EU standardisation schemes, the European Security Procurement Handbook, and other initiatives such as the European Security Label) while also fostering joint or common approaches at an international level. Such initiative should be open to all countries sharing common security goals with the EU but could focus on countries and regions whose own security issues and concerns are seen as being particularly important in terms of their interrelationship with EU and global security priorities. The Programme could also serve to raise the visibility of the European security industry around the world.

3.2.10 Training and enhancement of skills

There are a number of areas in which training and skills initiatives could be directed. First, in terms of the supply-side of the sector, efforts could be made to address shortages of suitably skilled technical workers, in fields such as security equipment and systems design. Preparation of designers, users and other workers in the security field and their adaptability to change is essential for the industry to remain competitive in a rapidly changing environment. On the procurement side, efforts are required to better inform and educate procurement decision-makers on security issues and technologies, and to enable them to make better informed decisions regarding choices over security equipment and systems and their effective implementation. Further, with regard to users and operators of

[125] The CPSI project is developing a methodology to collect, quantify and monitor data on actual and perceived security issues. These data will be then available to end-users (such as governmental bodies at local, regional, national and international level; law enforcement agencies, organisations engaged in policy making…) for them to monitor security threats, formulate better policy and implement security interventions in a more focused (and cheaper) way.More information available at: http://ec.europa.eu/enterprise/security/doc/fp7_project_flyers/securityresearch-lowdef.pdf

security equipment, raising and maintaining (updating) of professional skills in response to changing security environments and technologies is an issue.

Strengthening EU security-related training infrastructure

In the area of security related education and training, the European market appears to be highly fragmented; for example current training initiatives for security functions and tasks are highly diversified, with a very large number of small public and private operational training centres (often) under direct control of local authorities or a specific public service. Accordingly, a first requirement is to establish the existing infrastructure in this field. A second step, drawing on an assessment of the existing infrastructure and market requirements could be to develop an EU initiative aimed at strengthening the provision of security related education and training.

➔ **Stocktaking and Assessment of the situation and role of the private (and public) sector training infrastructure in the security field**. This would allow the identification of training facilities and whether there are shortcomings in the current infrastructure or not. This assessment would provide a basis for a comprehensive support framework for the development and enhancement of training facilities and infrastructure, based on a mutually reinforcing principle among existing and 'to be created' new facilities.

➔ **European Security Training Initiative** devoted to training and education on security-related issues. This could incorporate the creation of a network of training centres at EU level. Such a network would provide a platform for *inter alia* exchange of best practice, cross-border training initiatives, etc. with the aim of overcoming the difficulties posed by the fragmentation in the security training domain

The e-skills initiative applied to security[126]

As is the case for many economic sectors, e-skills shortages, gaps and mismatches, as well as a persistent digital divide may negatively the competitiveness of the EU security industry. This is particularly the case given that the security industry is a technology-driven industry, with technology development and innovation in many segments either focused on or facilitated through software development and the implementation of information and communication technologies. Further, due to the reactive environment in which the security industry operates and the need to quickly adapt technological solutions to market demands, rapid and flexible access to required skills is of considerable importance. In this context, existing horizontal actions already in place in the European level could be extended and tailored to security requirements. In this respect, challenges and the action lines suggested in the Commission communication on "e-skills for the 21st century" [127] can be also applied to the security industry framework.

[126] See http://ec.europa.eu/enterprise/ict/policy/ict-skills/ict-skills_en.htm#latest_news

[127] Commission Communication COM(2007)496 final on e-skills for the 21st century: Fostering competitiveness, growth and jobs (published on 7.9.2007)

3.2.11 Areas for further research and analysis

The reactive and quickly evolving nature of the security industry implies new potential challenges for the sector. The preparedness and response of both society and the public and private domain is essential. A better understanding of some of the endogenous conditions of the industry is necessary to improve the competitiveness of the European security industry.

On the basis of the analysis undertaken in this study and taking into account the lack of both qualitative and quantitative research carried out in the security field, a number of areas can be identified where the European Commission could seek external advice through the potential provision of a series of studies in the security domain. Such studies would complement and consolidate the work undertaken under this assignment.

Some potential topics to be addressed in future research assignments may include:

- **Competitiveness of security services and interaction with industry:** The present study has focused primarily on an analysis of security equipment and systems. A complementary analysis is required of (both public and private) security services and their role, considering their relevance as a 'market' for the security industry as well as for the inter-linkages currently existing between the security industry and the security services. The overall delivery of security capabilities is strongly dependent on the performance (efficiency and effectiveness) of service providers.

- **Analysis of the security regulatory framework in Europe:** A proper description of the legal environment for security requirements and capabilities is needed in order to identify existing inconsistencies in the market environment and potential negative effects on the security sector as a whole. Among the possible topics to be covered are issues such as liability protection, the legal differentiation between defence and security, etc.

- **Mapping of the European Security and Technological Industrial Base (ESTIB) and its competences[128]:** A proper study is needed in order to have a clearer picture of the technological industrial base in Europe. This would provide foundations for a better understanding of the role played by different market actors (e.g. industry, public and private research, etc.) and the interactions between the security and other industry and technological domains.

- **Country-competitor analysis in the security field:** An in-depth examination of the strengths and weaknesses of Europe's main market competitors in different security domains would assist in a clearer assessment of the competitiveness position of the EU and potential opportunities and challenges for the future.

[128] Please note this is a specific topic underneath section 3.2.2 'An Industrial Policy for the security sector'.

Policy Recommendations – Summary Matrix

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
Lack of mutual understanding between policy-makers and industry	▪ Development of initiatives to promote analysis, debate and dialogue on security issues and to develop a European 'vision' for security. This would integrate proposals and initiatives that would contribute to matching the ambition of public policy makers with the potential and possibilities of the private sector.	▪ **European Security Congress** (similar in format to the WEF "Davos" meeting) promoting dialogue and debate and raising awareness of security issues. ▪ **Security Policy Forum** would establish a permanent platform for dialogue and exchange between policy-makers, private bodies and service providers; ▪ **Strengthening the European representation of the security industry**, including not only representation from defence orientated players but also other players coming from other fields of activity (e.g. ICT), as well as national associations, and including SMEs.
Lack of a comprehensive EU industrial policy for security	▪ Monitoring and updating of a 'roadmap' for future security capability requirements and technologies aimed at contributing to reducing uncertainty over future market developments; ▪ Development of an Industrial Policy for security, giving a global and coordinated view of EU security related activities, indicating what gaps (technology, operational, societal, legal) are to be filled and what policy initiatives may be taken to improve the position of the EU security industry and functioning of EU security markets.	▪ **High Level Security Industry Forum**, to develop the basic principles and objectives of an industrial policy for security. It is meant to be a platform for discussion, bringing together industry representatives, EU institutions, governments, social partners, academic experts, etc. who would create a framework (proposals and initiatives) for the security industry to effectively respond to EU (and global) security requirements and needs. ▪ **European Security Technological and Industrial Base (ESTIB) mapping**. The identification of a European Security Technological and Industrial Base (ESTIB) and the mapping of its competences is requires as a basis for policy development and for a comprehensive assessment of the industry.

Absence of European and common international standards for security	▪ Enhanced standardisation and certification at EU and international level. This should aim to provide a framework for performance standards that are aligned to security policy, and for technical standards that promote greater consolidation of currently fragmented markets.	▪ **Industry-based solution for the development of technical standards**:
		  ▪ **Strengthening of European Standardisation Organisations' work.** Public authorities could call for the development of new standards in the security field, providing clear mandates to ESOs based on priorities set out in the European 'vision' for security;
		  ▪ **European Security Standards Institute**. Either within existing ESO framework or as an oversight body for security standards. For example, following a similar approach as that adopted by ETSI (European Telecommunications Standards Institute) and aimed at facilitating the self-development of technical standards;
		  ▪ **New Approach legislation for security**: The possibility of establishing a system of voluntary standards in the security industry should be considered.

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives

		▪ **Formal approach for the development of performance standards:**
		  ▪ **European Security Standardisation Handbook**, based on the initiative already in place in the defence sector (i.e. European Handbook for Defence Procurement);
		  ▪ **European Security Label**, which would increase confidence and act as a catalyst for investment by attracting new investors to the security industry. As mentioned by ESRIF, this will act as a reference point for manufacturers, end-users and other relevant stakeholders and would provide the frame for a dynamic standardisation process.
		▪ **EU-level testing and certification scheme and improved approvals and certification infrastructure**, with the aim at creating a testing protocol and the necessary infrastructure (dedicated labs or testing facilities) to carry out testing practices of security products;
		▪ **Exchange of formal and informal information on testing facilities as well as best practices,** with the objective of increasing transparency and cooperation (e.g. following the example of the CREATIF Network initiative);
		▪ **Fast-track system for approval of priority technologies and equipment**, to enhance rapid responses to new security threats and challenges.

Lack of dedicated liability regime for the security industry	▪ Develop EU-level principles and systems for security equipment (and services) liability protection. [**NB**: this study – which is 'economic' in focus - has not analysed in detail the legal situation and arguments related liability. A further assessment of potential options is required]	▪ **Liability support for new security technologies:** legal liability protection could also be provided to security technology developers; for example under a specific liability regime for sellers of 'qualified anti-terrorist technologies'.
IPR concerns (e.g. undermining of investments when IPR protection is inadequate)	▪ Develop support to the security industry (in common with other sectors) for international protection of IPR.	▪ **The creation of a European Fund to support protection of IPR**, as an additional support for security companies to enforce IPR (e.g. patents) at international level. ▪ **Better IPR Enforcement** based on the recommendations of the IPR Enforcement – Expert Group that could be implemented at EU level, such as zero tolerance policy in IPR enforcement, promotion of Intellectual Asset Management, specific training, coordination measures, funding, etc.; ▪ **EU-US Action Strategy for the Enforcement of Intellectual Property Rights,** which is already in existence, could be tailored to security; ▪ **Development of policy towards 'generic' security requirements** for lower income regions could

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
		also be considered.
Public procurement systems for security equipment and systems are insufficiently transparent and may be used to limit markets access (i.e. preference for 'local' over 'foreign suppliers)	▪ Enhance the transparency of (public) procurement procedures and improve awareness among users/purchasers of security products and services.	▪ **Greater clarity of 'defence' versus 'security'** from a procurement perspective. ▪ **European Security Equipment Market Initiative** aimed at increased transparency of (public) procurement procedures for security. This initiative should include a **European Handbook for Security Procurement**, containing a 'Code of conduct on Security procurement', a 'Code of best practice in the supply chain', and a 'List of best public procurement practices' while, at the same time, fostering pre-commercial procurement practices; ▪ **Lead Market Procurement Network for Security**, enabling public procurers to improve their knowledge about innovative solutions and to enhance coordination.
Current security research being insufficient and not aligned to immediate security capability requirements	▪ Stimulate security research and innovation; ▪ Promote research that is more tailored to market requirements; ▪ Strengthened cooperation to support the security knowledge area to progressively structure itself, and provide an open platform used to share information and practices.	▪ **European Security Programme** as an overall umbrella ensuring synergies and coherence on research and innovation activities at EU level. It would be responsible for setting the guidelines for research priorities, which would be implemented through funding vehicles such as Framework Programmes. ▪ **Lead Market Initiative for Security**, based on the existing EU framework for LMI, built around the adoption of legislative measures designed to foster innovation, mobilising public authorities to act as 'launching customers', improving standardisation, etc. ▪ **European Security Technology Platform**, to facilitate exchange of information and the development of coherent solutions in specific and relevant knowledge domains in the EU. ▪ **Field-labs for testing innovative security products and systems.** These 'laboratories' should provide real life environments for developing and testing security products and systems. The should also function as meeting points where end-users, security authorities, industry and the research community can take initiatives for joint implementation of improved solutions relevant for their daily work. Such field-labs will can also serve to stimulate SME's in entering the market; ▪ **Fund for EU Security & Resilience**, that could be used as a fast tracking system to respond to the new security threats as they are perceived. This fund would provide public resources for research and innovation activities addressing new security threats that need a rapid mobilisation of research funding.

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
Difficulty of transitioning from technology development (research) to full commercial development of products, particularly for small and medium sized suppliers of security equipment and systems	▪ Pre-commercial public procurement may provide an alternative means to bridge the gap from technology development to commercial production.	▪ **Pre-commercialisation procurement support**. This would include the promotion of pre-commercialisation support programmes and the establishment of procurement procedures and rules to stimulate the market for innovate products both in the public and the private sector; ▪ **European Handbook for Security Procurement** (see above) should include pre-commercial procurement as a way of enabling European public authorities to innovate faster in the provision of public services and create opportunities for companies in Europe to take international leadership in new markets; ▪ **Field-labs** (see above) are also an instrument for bridging the gap between R&D (and related innovation activities) and market implementation as well as for stimulating and encouraging SMEs in entering the market.
Lack of knowledge and understanding of the societal dimension of security	▪ Enhance dialogue and understanding of societal issues and impacts aimed at increased incorporation of societal considerations in development of security solutions (e.g. 'privacy by design' and 'security by design').	▪ **EU Platform for Societal Issues** linked to security could effectively support the integration of societal aspects, privacy, ethical, social and human issues, into the design of solutions and services; ▪ **European Security Label** (see above), being a reference point for suppliers, end-users and customers in general, should include a 'societal dimension' to security, incorporating the 'privacy by design' dimensions to security solutions designed and manufactured in the EU; ▪ **Assessment of the impact of the societal dimension of security and competitiveness**. This should analyse the extent to which societal concerns have a positive or negative impact on the cost of security solutions, the competitiveness of the security industry and the effectiveness of security systems.
Absence of public awareness and understanding of security developments (threats), policies and solutions.	▪ Development of programmes and projects to inform and educate target groups and the general public.	▪ **Targeted awareness programmes** reaching out to specific target groups and the larger public, to raise awareness of threats, risks, vulnerabilities, to improve the understanding of the processes and procedures put in place to tackle the challenges that these threats, risks and vulnerabilities bring, to debate the acceptability of technological solutions, etc. An example could be the CPSI project (Changing Perceptions of Security and Interventions); ▪ **International Security Programme** aimed at increasing understanding of EU security policies, approaches and solutions (including themes such as standardisation, procurement, etc.) and fostering the adoption of joint or common approaches at an international level. The programme would also provide an opportunity to raise the visibility of the European security industry around the world. ,

Market failure / Problem	Policy solution / recommendation	Proposed concrete initiatives
Lack of training and skills of security equipment designers and users	▪ Assessment of the role of public and private training infrastructure in the security field; ▪ Development of international initiates to improve education and training in the field of security.	▪ **Assessment of the private and public sector training infrastructure in the security field**. This would allow the identification of training facilities and whether there are shortcomings in the current infrastructure or not. ▪ **Development of a European Training Initiative** with the creation of a network of training centres at EU level devoted to training and education on security issues. Such network would provide a platform for exchange and cross-border training, aiming to overcome fragmentation in the security training domain. ▪ **Security industry skills framework initiative,** based, for example on the challenges and action lines suggested in the *e-skills for the 21st century* Commission communication.
Lack of quantitative and qualitative research carried out in the security field	▪ A better understanding of the endogenous conditions of the industry is necessary to complement and consolidate the work undertaken under this assignment.	▪ **External advice through the potential provision of a series of studies in the security domain, which may include:** - Competitiveness of security services and interaction with industry; - Analysis of the security regulatory framework in Europe; - Mapping of the European Security and Technological Industrial Base (ESTIB); - Country-competitor analysis in the security field.

PART B - SPECIFIC ASSESSMENTS

4 Air transport of goods (cargo)

4.1 General description of the segment

4.1.1 Segment definition

The broad description of the segment covered under this chapter is the *detection, identification, tracking and tracing of goods for secure and safe air transport*. However, the main focus for the segment analysis will be on the first elements of this description, namely **detection and identification**[129]. In this context, we understand detection and identification[130] as relating primarily to the ability to detect and identify the presence of specific dangerous or hazardous goods and materials (e.g. weapons, explosives, viruses, and chemical, biological radiological and nuclear substances (CBRN)). More broadly, it concerns the detection and identification of illicit trafficking of goods, such as weapons and drugs and, also, other forms of smuggling of both 'genuine' and counterfeit goods[131].

With respect to the scope of the definition of the scope of 'goods' to be included within the segment, from the perspective of air transport the following main categories may be identified:

- Items carried on the person of air travellers, within their cabin (carry on) luggage or loaded as hold baggage;
- Items of mail (letters and small packages);
- Other items of cargo, transported either in passenger airplanes (i.e. cargo loaded alongside hold baggage) or in dedicated cargo airplanes.

The focus for the segment analysis will be on the final category, namely air cargo. Nonetheless, many underlying technologies for detection and identification are applicable across the different categories.

[129] Tracking and tracing of goods is covered in Chapter 5, which deals with marine cargo.

[130] The capability of detection and identification is often linked to the issue of authentication. In the context of 'goods' authentication, this is primarily concerned with the ability to determine whether a product is genuine or whether it is a counterfeit product. Thus authentication relates to the protection of trademarks and other intellectual property by their owners. In addition, in the context of overall supply chain security, authentication may relate to the shipping company (e.g. in the case of known shipper programmes), or to the authentication of documentation concerning the integrity of the 'chain of custody' of goods in transport.

[131] In addition, it may also concern the detection and identification of cargo shipments and/or cargo containers so that, if required, they may be traced and tracked.

4.1.2 Product overview

A variety of technologies exist for detecting dangerous or hazardous items (e.g. explosives, incendiary devices, chemical, biological or nuclear agents) or illicit goods. The development of these technologies has typically originated in the form of passenger applications. It should be noted, however, that many of the underlying technologies for screening passengers and luggage, though subject to refinements, have not substantially changed since the 1980s. Key technologies – see section 4.1.3 for a more detailed description – that are already being applied or tested for cargo screening, include:

- x-ray screening;
- x-ray based explosive detection systems (EDS);
- explosive and chemical trace detection systems (ETD); and
- technologies based on neutron beams.

In addition to these technologically 'sophisticated' approaches, a widely-used approach is the use of canine teams to screen cargo.

The main focus for the segment analysis contained in this chapter will be on **x-ray based detection systems**, while trace detection systems are covered in Chapter 5.1, which deals with Chemical, biological, radiological, nuclear or explosive (CBRNE) detection.

It is important to note that the physical size, diversity and sheer volume of cargo (pallets and containers) to be screened presents a considerable challenge for developing effective screening technologies with the capability to screen air cargo – and cargo more generally – in an efficient way (see Box **4.1**). Overall, although the various technologies differ in terms of their capabilities and performance, a major problem remains that of reconciling the effectiveness of the screening process with sufficient throughput of cargo to avoid significant delays in delivery schedules that could undermine the economic viability of cargo operations.

Box 4.1 Air Cargo Screening Challenges

The U.S. Department of Homeland Security notes the following challenges for developing systems to screen air cargo:

Commodities – The greatest challenge in screening air cargo is the tremendous range and - configuration of commodities. Many of the common cargo commodities (e.g., machine parts) are very dense and present significant challenges for inspection technologies. In addition, many commodities are exceptional, such as cargo that is live (e.g., tropical fish) or requires great care and sensitivity (e.g., human remains). The time-sensitive nature of air cargo requires fast screening and resolution. Further, there is wide seasonal, temporal, and geographic fluctuation in commodities shipped by air. Lastly, approximately fifteen percent of the cargo is unique or unusual (e.g., race cars, marble statues) and can present tremendous screening challenges.

Configurations and Packaging – Another challenge in screening air cargo is the wide range of packaging and configurations. Cargo can be presented in individual boxes, on pallets, and in a wide range of containers (i.e., Unit Load Devices or ULDs). In general, break bulk cargo is considered to be individual boxes less than one cubic meter (3ft X 3 ft X 3 ft). Containerized cargo includes shrink wrapped pallets, cookie sheets, and ULDs. These configurations are generally 4ft by 4ft by 8 ft, but can also be much larger. Currently, there is no inspection technology to inspect the larger cargo configurations automatically (i.e., without operator

intervention). In addition, cargo is packaged in a diverse range of material including cardboard, metal, wood, and plastics and a large range of weights that can exceed current equipment capabilities.

The Technology Base – The technologies that have been used, or proposed, to screen air cargo were developed for carry-on baggage. As a result, each technology and approach has limitations in terms of detection, throughput, sensitivity, automation, and operational costs. Several screening methods and technologies exist for the type of commodity and configuration that are acceptable for screening low density commodities in small configurations. Performance gets progressively worse as the density increases, the configuration gets larger, and the packaging becomes more complex.

Additional Security Challenges – Other challenges to screening air cargo include the need for operational speed and efficiency. This is particularly important given the corporate and national economic benefits of air cargo commerce. Furthermore, a very low nuisance alarm rate is required of any technology that will be operationally acceptable, especially given the high costs and difficulty in opening and resolving alarms in carefully packaged break bulk and containerized configurations. In addition, the open nature of the air cargo system has made it vulnerable to threats from insiders and to theft, which is estimated at 3 percent annually and is accepted by the industry as a "cost of doing business." Theft of cargo indicates that there are vulnerabilities in the system that could be exploited to insert a threat.

Source: Statement for Record, Mr. James Tuttle, Division Head, Explosives Division, Science and Technology Directorate U.S. Department of Homeland Security. Before the House Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection. July 15, 2008[132]

4.1.3 Overview of (air) cargo screening technologies[133]

X-ray screening

Systems utilising x-ray technology are the most common systems currently available for large-scale screening of cargo shipments. These systems rely on transmission and backscatter x-ray techniques to probe cargo pallets and containers.[134]

Commercial (single-energy) x-ray systems using high-energy beams can provide high resolution two dimensional density images of the contents of containers. They are suited to the detection of metallic objects with readily identifiable shapes (e.g. firearms) but are not well suited to the detection of illicit substances that have similar densities and shapes to common substances.

Dual-energy x-ray radiography is a common screening method in applications such as the non-intrusive inspection of passenger luggage. A colour coded two-dimensional image is created by comparing the relative transmissions of high and low-energy x-ray beams to

[132] Available at: http://homeland.house.gov/SiteDocuments/20080715141843-91466.pdf. Note, the Statement also refers to the operational constraints and environment, notably the numerous and diverse stakeholders are involved with air cargo. Key operational constraints to screening air cargo include: Diverse and Numerous Stakeholders; Regulatory Oversight / Approach from Government; Percentage of Cargo Screened; Operational Need for Speed and Efficiency; Economic Impact of Screening; Alarm Resolution is Critical; Insider Threats; Theft; Public Concern; Political Interest.

[133] For a non technical overview of air cargo technologies see: Congressional Research Centre "Aviation Security: Background and Policy Options for Screening and Securing Air Cargo" February 25, 2008, available at: http://www.fas.org/sgp/crs/homesec/RL34390.pdf
Note: Some passages of text are directly quoted from the aforementioned Reports

[134] Transmission X-ray techniques provide a negative image (i.e. from rays passing through the object), while backscatter techniques provide a positive images from rays reflected back of the object. The main problem associated with backscatter techniques for cargo screening is that - although offering clear images - backscatter x-rays have limited penetration. Thus, use of backscatter is generally accepted as complementary to transmission techniques rather than an alternative.

indicate metal and organic materials. However, the limited penetration of the low energy x-rays used to provide composition information prevents the method being used on consolidated air or sea freight. However composition information has been sought using dual-energy x-ray radiography at very high energies.[135]

Explosive detection systems (EDS)

Current explosive detection systems (EDS) are being used extensively in the aviation security environment for screening of checked passenger baggage.[136] These systems use x-ray computed tomography (CT) to scan objects, and computational algorithms that assess the probability of threat object detection based on object density characteristics. Using this type of technology to screen (air) cargo presents a number of challenges. In particular, current EDS machines are unable to screen objects of the size of pallets or containers; they also suffer from reported high false alarm rates, which means that significant secondary screening or inspection may be required; and, the processing/throughput rate of EDS equipment may be insufficient for commercial cargo operations.

Chemical trace detection systems / explosive trace detection (ETD)[137]

Chemical trace detection systems, referred to commonly as explosive trace detection (ETD) devices, are widely used for secondary screening of passenger carry-on and checked baggage[138]. These systems use a variety of technical principles to analyse the chemical composition of sample residue wiped from suspect articles. These systems compare the chemical composition of a sample to the signature of known explosive materials and signal an alarm to the operator if the probability of a match exceeds a specified threshold. However, screening procedures using these systems are very labour intensive and time consuming.

Biological, radioactive and nuclear detection system[139]

Both fixed and hand-held detectors for biological, radioactive and nuclear detection can be integrated into security systems. For example, fixed detectors placed at airports of entry/departure can help to detect radiological or nuclear materials or weapons. Hand-held devices can also be used at airports for detection or confirmation of the presence of RN materials.

---

[135] Eberhardt, J., Liu, Y., Rainey, S., Roach, G., Stevens, R., Sowerby, B. and Tickner, J. (2006) "Air cargo sceening using a fast neutron and gamma-ray radiography scanner", paper presented at the 15th Pacific Basin Nuclear Conference. Available at: http://www.pacificnuclear.org/pnc/2006-Proceedings/pdf/0610015final00111.pdf. See also: William Reed (2007), "Energy driven", Cargo Security International, June / July 2007; William Reed (2007) "X-ray cargo screening systems: the technology behind image quality", Port Technology International, September 2007.

[136] For example: *"The U.S. has implemented an automated check baggage screening regime based primarily on certified EDS Computed Tomography (CT) at level one. Over 1,500 certified CT-based EDS systems have been deployed at the largest airports. … At the smaller airports trace explosive detection is used to clear checked baggage. There are about 6,000 trace systems from two suppliers deployed as either primary screening or alarm resolution. The plan is to replace trace systems for primary checked baggage screening with CT-based EDS as the resources allow. Trace for checked baggage screening is labor intensive and insensitive to passenger privacy because it requires the opening, examination and handling of the contents of the bag."* Source: "Review of developments in testing, implementation and operational deployment of advanced security screening technologies". Information submitted by the United States to 28th APEC Transportation Working Group Meeting ,Vancouver, Canada, 5-8 September 2006. Available at: http://www.apec-tptwg.org.cn/new/Archives/tpt-wg28/Aviation/2006_TPT-WG-28_AEG-SEC_013.doc

[137] See Chapter 5.1, for more discussion of these systems.

[138] ETD may also be used for primary screening of oversize, fragile or other baggage that cannot be screened using EDS.

[139] See Chapter 5.1, for more discussion of these systems.

Neutron beam technologies (gamma sensors)

These systems use a pulsed neutron generator to probe an object, initiating several low energy nuclear reactions with the chemical elements comprising the object. Detectors can then measure the nuclear signature of the transmitted neutrons and/or the gamma-rays emitted from the reactions. As neutrons and gamma-rays have the ability to penetrate through various materials to large depths in a non-intrusive manner, neutron technologies may have advantages for cargo screening[140].

Millimetre Wave Imaging Systems

Millimetre wave screening technology refers to a wide array of screening devices capable of creating highly detailed images by measuring the reflections of ultra high frequency (i.e., in the 30-300 giga-Hertz frequency range) waves emitted by the system that are capable of passing through barriers that normally preclude visual inspection[141].

Millimetre wave (and x-ray imaging portals) can today generate images of weapons and explosive devices hidden under the clothing, even ceramic and plastic weapons[142,143]. Interest in the use of millimetre wave imaging systems for air cargo screening has, however, been limited to date. Nonetheless, commercial products using millimetre wave imaging are currently available for application in standoff scanning of a wide variety of objects, including cargo, from a distance of several meters.[144] While images from multiple angles are typically required to get a complete picture of a container's contents, currently available millimetre wave imaging systems are capable of generating relatively high detail images of items held inside a cargo container. However, like X-ray screening technologies, millimetre wave imaging systems are labour intensive, and can be expensive to operate, because they require trained operators to interpret the images generated by the system and identify potential threats for further examination.

Canine Screening

Canine teams are already used for explosives detection – and detection of other substances – as an alternative to physical or more technological solutions and may provide a relatively low cost solution to air cargo screening.

One specific technology is Remote Air Sampling for Canine Olfaction (RASCO), which has a long history of use, notably in Europe and South Africa; RASCO is approved for air cargo screening in France and the UK. Vapour samples are collected from air cargo or trucks into a sample tube or through a specially designed filter. Trained dogs – able to detect minute traces of explosive vapour - are then used to sniff the filters. The technique

---

[140] Gamma-ray technology requires less maintenance and lower cost of ownership than equivalent x-ray systems but provide lower definition images. Neutron technologies are, however, expensive and the GAO notes that currently available neutron-based technologies cost about $10 million per machine and require about one hour per container for screening thus making this option very expensive and time consuming. Source: Congressional Research Centre "Air Cargo Security" Updated July 30, 2007. Available at: http://www.fas.org/sgp/crs/homesec/RL32022.pdf

[141] Source: Congressional Research Centre "Aviation Security: Background and Policy Options for Screening and Securing Air Cargo" Updated February 25, 2008; page 35. Available at: http://fas.org/sgp/crs/homesec/RL34390.pdf

[142] Smiths Detection is developing a handheld wand that will detect not just metal but also ceramic weapons and even explosives. The technology uses terahertz waves, capable of analysing chemical compositions and identifying substances.

[143] It is worth noting that the use of millimetre wave technologies to scan persons - sometimes called an electronic strip search – has raised concerns about propriety. To eliminate the strip search problem, researchers are looking at ways to remove the body from the viewing image by transferring the metal, ceramic, and plastic items to a wire frame image resembling a generic body.

[144] Calvin Biesecker. "Rapiscan To Market Brijot's Stand-Off Millimeter Wave Body Scanner," Defense Daily, October 31, 2007.

has the advantages of a high detection rate and low false alarm rate, high throughput, use for all cargo types (including those difficult to screen using x-ray) without needing to break cargo.[145]

4.2 Market (demand side) overview

4.2.1 Overview of main market (customer) segments

The main market (demand) segments for security equipment dealing with detection and identification of goods in the air transport sector are the following:

- **Airports:** Airports, being the major responsible for passengers' security and also dealing with cargo operations, are some of the major purchasers of screening and scanning equipment. As stressed by the industry, their behaviour as purchasers of security equipment is technology neutral, not favouring any provider but the end mission of the equipment[146].
- **Airlines:** Air cargo security is primarily a responsibility of the airlines themselves, being the main responsible for cargo screening and security-control at airports. When the supply chain security cannot be guaranteed or is 'unknown', cargo is systematically screened. Some airline companies, however, still screen all cargos even if the supply chain is guaranteed to be 'secured'. In airlines' hubs (i.e. British Airways in Heathrow, Air France in Charles de Gaulle, KLM in Schipol etc.) there is a tendency for the airlines to manage their own security operations[147].
- **Freight forwarders:** They purchase a wide variety of equipment, from scanners, detection and recognition devices to CCTV systems, biometrics or bar code based tracking devices for their operations. The equipment they use depends mainly on the type of goods they transport or store, with high risk cargo needing a whole range of security equipment devices. Their role as customers may become more important depending on how the supply chain security is organised (i.e. existence of known-shipper programmes, their designation as 'regulated agents', etc).
- **Customs:** Customs services, found in all airports, normally have their own screening and scanning equipment. Their priorities for security screening relate to drugs, counterfeit goods, nuclear materials, weapons, etc. They do inspect cargo depending on the potential risk involved.
- **Security service providers:** Private security companies are the main end-users of screening and scanning equipment. In some cases, the service providers are also responsible for purchasing the equipment used to carry out their operations[148].

[145] Source: "RASCargO – Fast, Cost Effective Screening for Air-Cargo", Homeland Security Europe, available at: http://www.homelandsecurityeu.com/pastissue/article.asp?art=268388&issue=176

[146] Interview with Airport Council International-Europe (ACI-Europe). In 2007, ACI-Europe member airports (around 450 airports in Europe) welcomed 1.47 billion passengers and handled 17.4 million metric tonnes of cargo and 20.8 million aircraft movements.

[147] In this situation, the various categories of personnel engaged in security/cargo related activities (e.g. security screening, ground handlers, airline personnel) are part of the same company (i.e. one sole company can be responsible for all cargo operations). Source: Interview with Association of European Airlines (AEA).

[148] Information gathered from COESS (Confederation of European Security Services) and ASSA-I (Aviation Security Services Association – International) questionnaires sent to their members for the purpose of this study.

4.2.2 Cargo related security risks

In a general sense, demand for capabilities for the detection and identification (inspection and screening) of cargo, particularly with regard to cross border movements, relates to three main categories of risk[149]:

- **Terrorism**: i.e. either in the form of attacks on or attacks using aircraft, or as a mode of transport for goods or materials used for terrorism acts (e.g. weapons, explosives, etc.);
- **Illegal movement of goods**: i.e. criminal activities related to the movement of prohibited goods (e.g. drugs, weapons, alcohol etc.) or to other types of illegal activity (e.g. smuggling of persons, counterfeit goods, etc.);
- **Fraud and revenue avoidance**: i.e. the deliberate (or unintentional) mislabelling of goods so as to avoid customs and other import duties and taxes.

For obvious reasons, terrorism-related risks represent the main driver of demand for detection and identification equipment and systems in the aviation sector. The main focus of attention has been the direct threat posed by terrorist hijackings of passenger airplanes or by explosive devices concealed on persons or boarded as part of passenger luggage. However, as security measures in relation to passengers and their luggage have been stepped-up, there is increasing recognition that air cargo may become a potential target for terrorists[150]. This relates both to the hijacking of cargo airplanes (e.g. use of aircraft as a weapon of destruction) and to the introduction of explosive devices in cargo shipments, particularly where such shipments are transported in passenger aircraft[151]. The recognition of this potential threat has lead to the adoption of security measures to enhance air cargo security; notably in the US where a system to screen 100 percent of cargo transported on passenger aircraft should be implemented by 2010.

Although the focus is on terrorism-related risks, the other two risk categories mentioned above are important, particularly from the perspective of border policing and customs-related requirements for screening equipment and systems. At the same time, addressing cargo crime (e.g. theft, fraud, smuggling, etc.) and detection of undeclared hazardous materials may also contribute to improving overall cargo security and could deter terrorist threats to cargo shipments.

---

[149] A further risk relates to the shipment of undeclared or undetected hazardous materials aboard aircraft: "Although, most explosives and gases are prohibited aboard aircraft, many properly handled hazardous materials are permitted aboard passenger and all-cargo aircraft within specified quantity limitations. Risks are introduced when hazardous materials are not declared leading to the potential transport of prohibited materials by air or improper handling of hazardous goods during loading and while in transit. While safety concerns regarding hazardous cargo shipments aboard passenger aircraft are of particular concern, preventing unauthorized shipments of hazardous materials is a challenge for all-cargo aircraft operators as well. According to the U.S. General Accounting Office, about 75% of hazardous materials shipped by aircraft are carried aboard all-cargo aircraft, while the remaining 25% is shipped on passenger aircraft". Source: U.S. General Accounting Office "Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach". GAO-03-22, January 2003.

[150] See, for example: Congressional Research Centre "Air Cargo Security: CRS Report for Congress" (updated July 30, 2007), available at: http://www.fas.org/sgp/crs/homesec/RL32022.pdf; Congressional Research Centre "Aviation Security: Background and Policy Options for Screening and Securing Air Cargo" February 25, 2008, available at: http://www.fas.org/sgp/crs/homesec/RL34390.pdf
Note: Some passages of text are directly quoted from the aforementioned Reports

[151] This risk is somewhat mitigated, however, by the fact that – without assistances to access individual aircraft (e.g. cargo workers) – it would be extremely difficult to target specific flights. Moreover, there is usually the possibility that cargo may be transported by all-cargo aircraft, which are seen as less 'appealing' targets than a commercial passenger aircraft.

4.2.3 Aviation terrorism impact on security equipment requirements[152]

Prior to the 1970's the main security concerns in the area of aviation related to aircraft hijacking. The first effective aircraft hijacking counter-measures were introduced in 1970 but it was not until 1973 that airlines started to introduce 100% passenger and cabin baggage searches. The blowing-up of Pan Am flight 103 over Lockerbie in Scotland in 1988 was the catalyst for major change in national aviation security programmes with the phased introduction of 100% hold baggage screening in a number of European States and introduction of systems for positive baggage reconciliation.

The terrorist aviation threat is considered to have moved to a new dimension in December 1994, when Algerian terrorists hijacked Air France flight 8969, en route to Paris from Algiers. The French government refused the aircraft landing rights at Paris as they had received intelligence that the hijackers intended to blow up the aircraft over the city. The use of aircraft as a 'weapon of destruction' with the intention to inflict maximum collateral damage and loss of life became a reality with the events of 11 September 2001. These events resulted in significant policy decisions and the introduction of legislation; in particular Regulation (EC) No 2320 / 2002 in Europe and the Air Transportation Security Act (ATSA) in the US, both of which resulted in fundamental changes to the way aviation security is conducted and managed across the world.

In August 2006, a number of suspects were arrested on suspicion of plotting to detonate liquid explosives carried on board several airliners travelling from the United Kingdom to the United States and Canada. This resulted in the introduction of new measures limiting carry-on liquids and the size of cabin luggage.

As the responses to the events outlined above illustrate, security requirements (both mandatory and voluntary) and, in turn, the introduction of security systems and equipment has tended by and large to be a reactive process with developments reflecting changes in the *modus operandi* of terrorists. Briefly, these developments in security approaches, priorities and requirements can be summarised as follows:

- Prior to the 1970's, screening of passengers and their carry on luggage for weapons using metal detectors.
- 1970's, introduction of basic x-ray baggage screening - in response to a shift in tactics away from the gun and toward the bomb. Subsequently followed by introduction of smart x-ray and computed tomography (CT) baggage scanning in response to the increasingly sophisticated materials used to make the bombs.
- 1990's (post Lockerbie), additional screening of hold baggage and positive baggage reconciliation.
- 2000's (post 9/11), shift to mandatory systems including 100% screening of carry-on and hold luggage. Development of more sophisticated technologies for explosives detection[153].

[152] The assessment in this section (up to 2004) is based on: Irish Aviation Authority and Avia Solutions (2004) "Civil Aviation Security financing Study" Background Report, Chapters 1 and 2, prepared for DG Transport. Available at: http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_1.pdf and http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_2.pdf
Note: Some passages of text are directly quoted from the aforementioned Report

[153] It should be noted that use of canine detection (sniffer dogs) is a widely used solution.

4.2.4 Current approaches to air cargo supply chain security

Although the focus of this Chapter is on screening of air cargo, this attention should be placed in the broader context of air cargo supply chain. There is widespread consensus that the (increasing) size and complexity of international supply chains makes them particularly vulnerable not only to terrorism threats[154] but also to organised crime or to events (e.g. natural or man-made disasters) that break the chain. Specifically, the large number of linkages and parties involved in international supply chains means that custody of goods (or information) frequently pass from one party to another (with consequential loading, offloading, reloading and storage etc), thus opening it up to potential breaches and/or opportunities to be attacked.

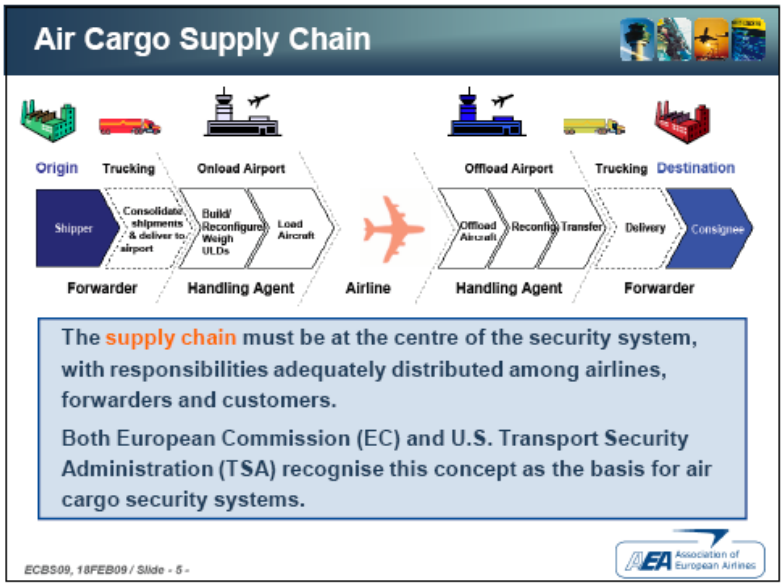
Consequently, air transport security relies not only upon security within the air transport sector *per se* but also on the maintenance of security at each stage (and by each operator) in the supply chain (see Figure 4.1). A supply chain based approach forms the basis for current initiatives to enhance security within the transport sector, particularly those initiatives taken after the events of 11 September 2001 that highlighted the vulnerability of the transport sector to terrorist attacks. Notwithstanding these initiatives, operators within the supply chain also need to address broader security issues, for example to prevent theft, as well as complying with working environment rules and other regulations and to protect their own personnel[155,156].

[154] This may relate to supply chains that are broken as a result of a terrorist attack, or through the use on transport modes to make an attack.

[155] National Board of Trade Sweden (2008) "Supply chain security initiatives: a trade facilitation perspective", Kommerskollegium 2008:1. Available at: http://www.kommers.se/upload/Analysarkiv/In%20English/Trade%20facilitation/Report%20Supply%20Chain%20Security%20Initiatives.pdf

[156] In addition, "incentives for companies to participate in the [security] initiatives can include the possibility of obtaining smoother customs treatment; requirements made by partners, and pure marketing considerations". Ibid. footnote 155.

Figure 4.1 Air cargo supply chain



Source: Alain Breuer (2009)[157]

In general, international and national approaches to supply chain security – particularly in the context of air cargo – are based on 'layered' approaches that include:

- **Known shipper programmes / Vetting of companies** and their security measures throughout the supply chain[158]:
  - **Shippers:** e.g. EU air security regulations allow for the designation of "known consignor" [159] and "account consignor"[160,161], and the US operates a "known shipper" program. If shippers meet the requirement for these designations then certain security controls may not be applied when there cargos are received by an air carrier or "regulated agent"[162].
  - **Freight forwarders:** for example EU air security regulations allow for the designation of "regulated agent"[163], and the US operates an Indirect Air Carrier (IAC) Programme. Again, if a freight forwarder (or other "regulated agent")

[157] Alain Breuer, Chair AEA Cargo Security Working Group, "The future EU and U.S. air cargo security requirements: What are the challenges for the industry?", Presentation at ECBS09 17-18 February 2009, Prague Aviation Master Class. Available at: http://files.aea.be/Speeches/ECBS09_18-02-09.pdf

[158] The stringency of requirements – and (mandatory) requirements for inspection - for security systems and procedures typically increases the further along the supply chain an 'agent' is located (in relation to the point at which cargo is actually transported in an aircraft) . Vetting procedures may relate to verification of the identity of companies (i.e. shippers), security checks on personnel, and actual physical and information security procedures, equipment and systems.

[159] "The originator of property for transportation by air for his own account and who has established business with a regulated agent or carrier". Regulation (EC) 2320/2002

[160] Regulation (EC) 831/2006

[161] Known consignor status requires shippers to fulfil certain security requirements (i.e. implement and maintain security systems); these will be subject to inspection before known consignor status is granted. An account consignor is a shipper whose cargo can be positively identified for carriage exclusively on all-cargo aircraft.; account Consignors can be designated directly by their Air Carrier or Regulated Agent.

[162] For example, air carriers or regulated agents are not obliged to screen cargo received from a known consignor. In the US, only cargo from a known shipper can be carried on a passenger airliner.

[163] "An agent, freight forwarder or other entity who conducts business with an operator and provided security controls that are accepted or required by the appropriate authority in respect of cargo, courier and express parcels or mail." Regulation (EC) 2320/2002

meets the requirements for these designations, then certain security controls may not need to be applied when their cargos are received by an air carrier.

- **Inspection and screening requirements** for cargo. For example EU and US regulations require screening of all cargo to be loaded onto an airplane that does not come from either a known consignor/shipper or from a regulated agent/IAC[164]. Cargo must also be screened if there is any indication of interference with the cargo since the point at which it was subject to security controls by the known consignor/shipper or from a regulated agent/IAC. Under current US legislation, the intention is to introduce 100 percent screening of all cargo transported on passenger aircraft by 2010.
- **Strengthened security of air cargo facilities**. For example strengthening of physical security measures (e.g. perimeter security and surveillance) and access systems for cargo areas. In addition, tightening of security/background checks on personnel with access to cargo facilities.

From the perspective of the structure of demand for equipment and systems for detection and identification (inspection and screening) of cargo, the adopted approach to supply chain security is important. For example, without the implementation of "known shipper" type programmes, the adoption of 100% screening requirements would imply that air cargo handler/carriers would need to screen all cargo they receive; demand (and associated cost of acquisition) for screening equipment would thus be concentrated at airport cargo facilities. The adoption of "known shipper" type programmes allows for the responsibility to be shifted back up the supply chain with the possibility to avoid bottlenecks and congestion where screening capacity at airports is insufficient to both maintain adequate throughput and meet security requirements.

4.2.5 International market profile and market size estimates

Different estimations concerning both the global aviation security market and the market for security equipment in the aviation sector do consider very dissimilar figures and estimates. Therefore, there is an enormous difficulty to calibrate the real size of the aviation security sector and its related equipment.

The difficulty to obtain estimates of the size of the market for air inspections and screening equipment and systems is mainly due to fairly obvious reasons: users of such equipment are reluctant to provide information on investments and expenditures as this could indicate the type and level of security equipment and systems utilised. Similarly, for suppliers, such information is commercially sensitive.

The global aviation security market

Estimates from Homeland Security Research Corporation (HSRC)[165] (see Table 4.1) value the global aviation security market at $7.6bn (€5.2bn) in 2008. The market is expected to grow to $14.2bn (€10.4bn) by 2018 with a forecasted CAGR (in case of no long term economic crisis) set at 6.5%. Although the market is substantially growing,

[164] In the EU case, cargo from an "account consignor" shipped on an all-cargo aircraft may not be screened, also.

[165] Homeland Security Research Corporation (HSRC), *Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018*. Published in 2008.

HSRC considers that the aviation security market will maintain a stable share of the total global homeland security market[166] (from 11.4% in 2008 to 11.9% in 2018).

Table 4.1 Global Aviation Security Market Outlook 2008-2018 (€ billion)

	2008	2009	2010	2012	2014	2016	2018	2008-2018	
								Total	CAGR
Global Aviation Security market	5.2	5.9	6.3	7.2	8.1	9.1	10.4	85	6.5%
Aviation Market as % of global Homeland Security Market	11.4%	11.5%	11.6%	11.7%	11.9%	11.9%	11.9%	N/A	N/A

Source: Homeland Security Research Corporation (HSRC)

Taking into account a 2008 regional breakdown, the European Union comes second with a 22% market share of the total global aviation security market. The EU share is valued at €1.2bn in 2008 and it is expected to grow to €2bn by 2018. North America is currently leading and taking the largest market share with 38.1% of the market (€2bn) with the US market value meant to double (and reach €4bn) by 2018. The East Asia region market (mainly China and India) is anticipated to experience the biggest growth in the coming years, gaining ground to the EU market share by 2018.

Table 4.2 Global Aviation Security Market: Regional breakdown (€ billion)

	Global market value (€bn)		Global market share (%)		2008-2018 CAGR
	2008	2018	2008	2018	
North America	2	4	38.1%	38.3%	6.5%
Latin America	0.2	0.4	4.4%	4.4%	6.4%
European Union	1.2	2	22%	18.9%	4.9%
Middle East	0.3	0.7	6%	6.5%	7.3%
East Asia (CN+IN)	0.7	1.8	13%	17.9%	9.9%
Pacific Region (JP+AU)	0.3	0.7	5.9%	6%	6.8%
Other countries	0.5	0.8	10.6%	7.9%	3.5%
Total	**5.2**	**10.4**	**100%**	**100%**	**6.5%**

Source: Homeland Security Research Corporation (HSRC)

The HSRC estimate for the EU aviation security market (€1.2bn in 2008) is countered by other estimates from ASSA-International[167] which valued the European airport and aviation security market at €2.7bn in 2006 and considered the market would reach €3bn in 2009. This is far ahead the HSRC approximation, which sets the 2008 EU market value at €1.2bn and the expected 2018 value at €2bn. However, both sources (HSRC and

[166] Please note this is a Homeland Security Research Corporation estimate not to be understood as an estimate made by the study team for the general assessment of the security industry. The 'homeland security market' is defined by HSRC as the national effort to prevent terrorist attacks within a territory and all activities involved in the prevention of such attacks (protection of critical infrastructure, support domestically-based systems and processes, screening of passengers and goods, etc).

[167] Source: "European Aviation Security Market Overview" Presentation by Marc Pissens, President of ASSA-I (Aviation Security Services Association – International) in May 2007 available at: http://www.easa-security.org/news.htm

ASSA-I) coincide in arguing that the market will grow at an average of around 5 or 6% per annum.

Airport screening markets for air passengers and cargo

Industry sources indicate that the current global market for x-ray equipment for airport screening of hand luggage probably represents demand of around 3,000 units per year, with a further 800 units per year for hold luggage. Purchase prices for this type of equipment vary depending on their technical characteristics and size (see Table 4.3). Nonetheless, these data suggest that the total global market for equipment purchases alone for x-ray based screening systems (EDS) for carry on and checked baggage has a value of around $2 to 3 billion (€1.5bn to €2.2bn). This does not include the associated costs for baggage handling systems, installation costs, maintenance, and refurbishment and upgrading, along with any modifications that may be necessary to buildings and other infrastructure. These costs can be considerable and imply an overall value (cost) of screening that may be a significant multiple of the basic purchase price for equipment[168].

Table 4.3 Purchase price of checked baggage screening equipment (indicative)

Vendor	Model	Purchase Price
Analogic	AN XLB	$1,100,000
Analogic	King Cobra	$350,000
GE	CTX 9400	$1,200,000
GE	CTX 9800	$1,200,000
L-3	3DX 6000	$880,000
L-3	3DX 6600 (formerly AN6400)	$1,100,000
GE	CTX-5500 w/ ViewLink	$880,000
GE	CTX-2500	$625,000
Reveal	CT-800	$350,000

Source: TSA (2009)[169]

With respect to the market for air cargo screening equipment, it is even more difficult to make an estimate of the market value. This is partly because current screening technologies are not fully adapted to the requirements for screening non-break bulk (e.g. pallets, ULDs, containers) cargo. Although EU regulations set a general framework for air cargo screening, specific requirements, accepted technologies and equipment standards are determined by EU Member States and are not harmonised across the EU. In the US, the TSA has not yet defined final standards and certification requirements for cargo screening. Moreover, it remains uncertain to what extent demand for cargo screening equipment will be concentrated mainly close to airports (i.e. air cargo handling

[168] ACI-Europe indicated to the study team that the purchase cost of equipment is a minor share of the total security cost; for which the largest share relates to labour costs of personnel utilising the equipment. The overall cost of security 'equipment' is determined by the cost of the equipment itself (a small share of the total cost); maintenance of the equipment; upgrading of the equipment (in case new technologies are developed or new threats arise); labour costs of personnel operating the equipment. In addition, changes to airport infrastructure may be needed to accommodate new equipment (normally more sophisticated but also longer, larger, heavier and producing more heat), and the budget for this type of large scale infrastructure projects is most usually included in an airports security budget.

[169] Transport Security Administration "Planning Guidelines and Design Standards for Checked Baggage Inspection Systems" January 30, 2009.

facilities and carriers) or will be spread backwards in the supply chain to freight-forwarders (e.g. regulated agents and IACs[170])..

There are about 450 airports in Europe[171], with around 200 warehouses for cargo shipments; therefore the market for screening and ETD equipment (and also canine screening) in European airports is rather limited. On the basis that each warehouse may use 2 to 3 screening machines on average, then the total EU market for cargo screening equipment is only around 500 machines. Given that only a proportion of these machines would be installed (or replaced) in any year, the underlying demand would probably be well under 100 units per year. Nonetheless, should policies be adopted that promote the use of screening more widely throughout the supply chain – as it is the case in the US (see below) – then this could have a significant impact on the overall value of the market.

Some indication of the potential size of the market is provided by estimates of the cost of implementing 100% screening of cargo carried on passenger aircraft, as required under US legislation. The Congressional Budget Office estimated a total cost of $3.5 billion over six years of implementation[172], while the TSA indicated a cost of $3.6 billion over ten years. At the same time, it should be noted that as the equipment necessary for meeting the full screening requirements does not exist, there is some uncertainty as to the actual cost. In this regard, it can be noted that the TSA provides a reimbursement of $375k per facility for Certified Cargo Screening Facilities (CCSF)[173] under its Certified Cargo Screening Program (CCSP)[174].

It is also worth taking into account the assessment by HSRC, which states that air cargo transport worldwide will triple over the next 20 years, with an increase from 131.1bn RTKs (Revenue Ton-Kilometres) in 2001 to 464.1bn by 2021. Therefore, the market for air cargo screening equipment is expected to grow substantially in the coming years.

Other estimates by Frost & Sullivan concerning specifically the US airport screening markets (for both passengers and cargo screening)[175], consider that the US market for airport screening equipment was valued at around $450m (€328.5m) in 2007. The market is meant to reach $550m (€402m) in 2012. From these figures, 42.9% in 2007 (€141m) was devoted to equipment procurement. The share for equipment procurement spending is meant to grow to 49.1% (€197.4m) by 2012. Frost & Sullivan does not include estimates for the airport screening market in the EU.

[170] See section 4.2.4.
[171] As represented by ACI – Europe
[172] Congressional Budget Office. H.R. 1 - Implementing the 9/11 Commission Recommendations Act of 2007, February 2, 2007.
[173] In addition to freight forwarders, third party logistics providers (3PLs), manufacturing facilities, warehouses, and distribution centres may apply to become CCSF if their facility directly tenders cargo to a freight forwarder (IAC) or air carrier.
[174] On this basis, given that there are some 12,000 freight forwarders in the US, then if half were to be certified as CCSFs and qualify for full reimbursement for security equipment, this would represent a total of $2.25 billion.
[175] Source: "Airport Security: Are advanced technology deployments enough to grow the market?" Presentation by David Fishering (Frost & Sullivan), 28 August 2008. available at: http://www.slideshare.net/FrostandSullivan/frost-sullivan-airport-security-analyst-briefing-presentation

4.3 Description of the supply (value) chain

Note: To illustrate the structure of supply chains for identification and detection equipment, this section will focus on the supply chain for x-ray (including EDS) based screening equipment.

4.3.1 General description and overview

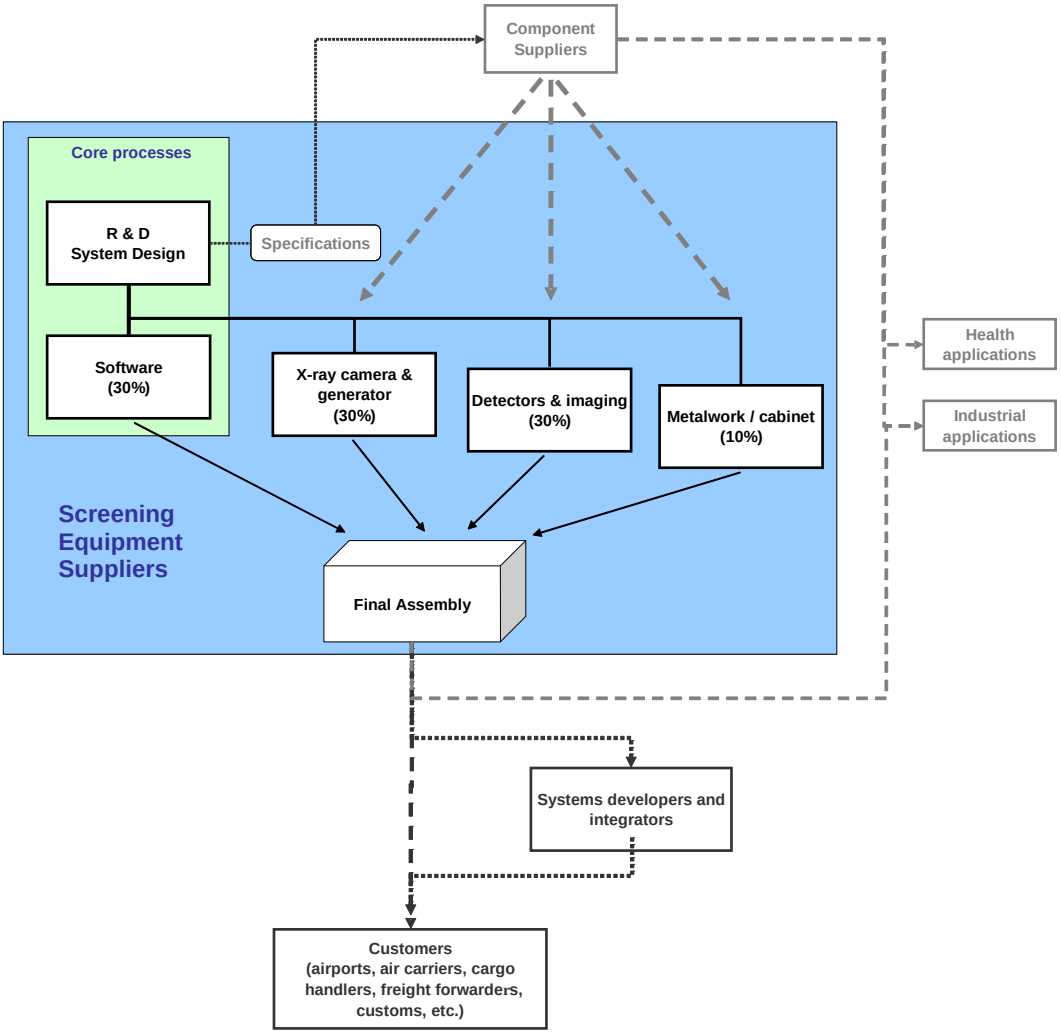
The supply chain for air cargo screening equipment is illustrated in Figure 4.2. It is characterised by the presence of a limited number of international players that develop and supply screening equipment for the aviation sector. These equipment suppliers (OEM) either supply downstream markets directly or will be linked to downstream markets via the major systems integrators (for example, where large integrated security systems are implemented for an new airport or terminal).

In terms of technology development and upstream linkages to component suppliers, the situation of individual equipment providers can differ depending on the technology expertise within the company (or other companies within the same group). Depending on this expertise, main components (e.g. x-ray cameras, generators, detectors, imaging systems etc.) may be either produced 'in-house' (or from within the group) or acquired from specialised external components and sub-system suppliers based on the OEMs specifications. However, for OEMs supplying the security market, the specific value-added derived from these components is typically low, and their main source of value-added comes from equipment/systems design, and technology and software development. Currently, in the absence of major changes in underlying technology, software development is an increasingly important driver value added for security screening equipment.

In light of the above, the trend appears to be for OEMs to move away from vertically integrated production towards the integration of sub-systems whose production is sub-contracted out to specialised providers. Thus, the focus of OEMs is increasingly on the core processes of R&D / technology development and software development[176].

[176] This conclusion is mitigated somewhat according to the extent to which the company (or company group) is engaged in supplying technologies/equipment to markets other than security (e.g. health, or industrial applications such as non-destructive testing). For companies that are part of a larger group, components and sub-systems may be supplied from within the group thus retaining a greater degree of vertical integration. For smaller companies, their core expertise may be in one of the main component/sub-systems fields, for which they supply equipment/applications to a wider market than just security.

Figure 4.2 Supply (value-added) chain for air cargo screening equipment[177]



4.3.2 Overview of main market players

The global supply of x-ray based and EDS screening equipment and systems in the air transport sector is dominated by a few major players (OEMs) that are the main equipment integrators[178,179]. This group consists of:

- Smiths Detection – see Table 4.4
- GE Homeland Protection (now part of Safran[180]) – see Table 4.5

[177] Number (percentage in parentheses) indicates approximate breakdown of cost elements in final equipment.

[178] Data published by IMS Research (The World Market for Explosives, Weapons & Contraband Detection Equipment 2007 Edition) shows that, in the combined Transportation, Critical infrastructure and Ports &Borders sectors, Smiths Detection has a 29% market share, with GE Security (15.5%), L3 Security & Detection Systems (12.5%), Rapiscan Systems (8.5%) and Nuctech (8%).

[179] Estimates by Frost & Sullivan of the market share of the US airport screening market for 2007 indicate: GE Homeland Protection (52.7%), L3 Security and Detection (22.9%), Smiths Detection (9.7%), Reveal Imaging (8.8%), Rapiscan (2.2%), Other (3.8%). Source: "Airport Security: Are advanced technology deployments enough to grow the market?" Presentation by David Fishering, 28 August 2008. available at: http://www.slideshare.net/FrostandSullivan/frost-sullivan-airport-security-analyst-briefing-presentation

- L3 Security & Detection Systems – see Table 4.6
- Rapiscan Systems (part of OSI Group) – see Table 4.7

Both Smiths and L3 are strongly connected to the defence sector, while the acquisition of GE security by Safran (Sagem Sécurité) will reinforce the interconnection between defence/aerospace and the security sector. The development of the activities of these companies in the air transport security sector has been the outcome of strong acquisition activity following the Lockerbie and 9/11 disasters (see Box **4.2**). Rapiscan is a wholly owned subsidiary of the OSI Group which also has activities in the field of health and optoelectronics[181]. The acquisition of the UK based Rapiscan Security Products Ltd by OSI followed from the rapid growth in demand for x-ray scanning equipment and detectors following the Lockerbie disaster in 1988.

Box 4.2 Examples of M&A activity by main air transport security equipment integrators following major terrorist attacks

OSI acquired the UK based Rapiscan Security Products Ltd (since renamed Rapiscan Systems Ltd.) in 1993 and commenced operations as a provider of security and inspection systems in the United States.

Smiths Group acquired Heimann Systems GmbH in 2002. Heimann was a recognised market leader in x-ray security products, primarily used in the transportation sector.

General Electric (GE) acquired Ion Track Inc (a leading provider of advanced trace detection systems) in 2002 and in 2004 acquired InVision Technologies Inc (a maker of bomb-detection equipment used in airports)

L3 Communications acquired PerkinElmer's Detection Systems business in 2002 (PerkinElmer had itself acquired Vivid Technologies – a manufacturer of x-ray explosive detection systems – in 1999). This acquisition brought with it an installed base of 18,000 x-ray screening units in airports and ports.

In addition to the above-mentioned companies, Nuctech from China is an increasingly important player. Nuctech is able to build on its direct linkage into the research capacity and network of the University of Tsinghua[182], while taking advantage of lower production costs than its main rivals. Nuctech has had some success in obtaining contracts in Europe and notably in geographical markets that are of strategic interest to the Chinese state.[183]

[180] In April 2009, Safran announced that it has acquired 81% of GE Homeland Protection, a wholly owned affiliate of the General Electric Company for $580 million. This acquisition will enable Safran to combine GE Homeland Protection's detection capabilities with Sagem Sécurité's (part of SAFRAN Group) identity solutions.

[181] OSI Optoelectronics is a producer of optoelectronic detectors which are a critical element in the detector hardware of x-ray systems.

[182] The extent to which Chinese technological development has been obtained through reverse engineering of rival products is an issue of contention. Certainly there is some concern about the level of respect for intellectual property rights and questions as to how technologies have been obtained.

[183] FISCAN (Beijing Zhongdun Anmin Analysis Technology Co. Ltd) is another Chinese company supplying x-ray and other security equipment. FISCAN is a subsidiary security division of First Research Institute of Ministry of Public Security.

Following this leading group are a number of medium-sized companies. Other US or EU based companies with a notable presence in aviation screening equipment market include:

- Reveal Imaging[184] - see Table 4.8
- American Science & Engineering[185] - see Table 4.9
- Gilardoni[186] - see Table 4.10

In addition, there are various smaller companies – for which it is extremely difficult to evaluate their number – that tend to be focussed on the development of specific technologies and/or offer specialised or niche products to the market; often these may be set up to commercialise academic research[187]. With high barriers to entry into the security market – particularly in relation to aviation security – it is often the case that smaller companies only access the market through licensing technologies /manufacturing to larger OEMs. Finally, some of the component and subsystem suppliers of OEMs may also provide products directly to the market.

[184] Reveal was founded in 2002 in direct response to the United States Government's post-9/11 mandate for vastly improved aviation security screening. Its co-founders included former senior executives from Perkins Elmer Detection Systems that was acquired by L3 in 2002.

[185] Formed in 1958, AS&E began as a developer of scientific instruments and applications for NASA, with a focus on x-ray technologies. It began producing x-ray scanning equipment for the aviation sector in the 1980s.

[186] With the exception of Smiths Detection – which itself has a major presence in the US and access to US project financing – Gilardoni is perhaps the only European owned and based company providing x-ray detection equipment to the aviation sector. The company employs around 250 persons with total turnover of around €50 million, of which €20 million relates to x-ray equipment, mainly for the aviation sector.

[187] See, for example:

- Kromek (www.kromek.com). Kromek, formerly Durham Scientific Crystals was incorporated in April 2003 to commercialise technology which had been developed in the Physics Department of Durham University. The Company has developed significant expertise and capabilities to combine its detector technology and the x-ray imaging technology. The result is a series of products that are being launched to deal with liquid based threats in aviation security and border control.
- 3DX-Ray Ltd (www.3dx-ray.com). 3DX-Ray Ltd was formed in 1996 to exploit original research undertaken at Nottingham Trent University on stereoscopic and multiple-view x-ray imaging technologies. The company has emphasised the development of innovative software and hardware (such examples as real-time stereo image processing and novel sensor geometries). Its 3D baggage screening "X-ray Vision Engine" is the only system in the marketplace offering genuine stereoscopic images and has been adopted by several baggage scanning equipment manufacturers.
- Optosecurity (www.optosecurity.com) Optosecurity is a technology spin-off from the Canadian National Optics Institute (INO), a world-class centre of expertise in business applications for optics and photonics. The company describes its OptoScreener as the world's first x-ray checkpoint upgrade that automatically detects potential threats, such as weapons and weapon parts, and also identifies dangerous liquids and gels. The company is partnering with market leading security X-ray system manufacturers for product integration and deployment in the transportation and critical infrastructure markets.

Table 4.4 Smiths Detection: Basic company indicators

SMITHS DETECTION (UK)				
Main indicators	**Smiths Group**		**Smiths Detection**	
	2007	2008	2007	2008
Turnover	€ 3,159.3m	€ 2,915m	€ 640.3m	€ 639.4m
Profit	€ 503.5m	€ 478.1m	€ 114.9m	€ 108m
R&D budget	€ 115.5m	€ 108m	€ 48.2m	€ 47.7m
Number of employees	20,800	22,600	2,100	2,300
Description of the company				
Smiths Detection, one of the five divisions of Smiths Group, is a global leader in the provision of threat detection and screening technologies for Military, Transportation, Homeland Security and Resilience applications. A leader in Transportation Security (38% of total Smiths Detection sales are devoted to this segment, mainly providing equipment to airports), Smiths Detection provides advanced, high throughput screening systems for people, baggage and freight. The company has Research and Development operations in six countries and systems deployed around the globe.				
Main products and technologies				
▪ Its products are mainly related to X-ray equipment (HI-SCAN and HCV series), X-ray (CT) based EDS equipment and ETD (Ioscan series). ▪ Smiths technology is deployed at nearly 80% of the world's commercial airports. Regarding screening technology, Smiths Heimann has developed an X-ray technology with a state-of-the-art image processing system. Other technologies used are Ion Mobility Spectrometry, Fourier-Transformed Infrared Spectroscopy, Millimetre-wave technology (for concealed objects) and Raman Spectroscopy.				

Source: www.smithsdetection.com and *Smiths Group 2008 Annual Report*

Table 4.5 GE Security: Basic company indicators

GE SECURITY (US)				
Main indicators*	**General Electric Company**		**GE Security****	
	2007	2008	2007	2008
Turnover	€ 119.9bn	€ 124.5bn	€ 3.1bn	€ 3.15bn
Profit	€ 16.4bn	€ 12.31bn	€ 474.1m	€ 469.9m
R&D budget	€ 2.15bn	€ 2bn	N/A	N/A
Number of employees	323,000	327,000	N/A	N/A
Description of the company				
GE Security is focused on communication and information technologies for security, safety and lifestyle enhancements. GE Security has operations in more than 30 countries, offering one of the industry's broadest product portfolios, including access control, explosives and narcotics detection, fire detection, intrusion, key management and video surveillance. GE detection and identification systems are deployed in more than 120 countries in airports, customs checkpoints, border crossings, prisons and a wide range of other facilities. GE is considered a leading provider of explosives detection systems (EDS) for the aviation security industry. The company, a wholly owned subsidiary of the General Electric Company until April 2009, has been recently bought by SAFRAN Group.				
Main products and technologies				
▪ Its products are mainly related to X-ray (CT) based EDS equipment (EntryScan, CTX and XRD series) and ETD equipment (Itemiser, VaporTrace, MobileTrace models). ▪ GE Security has developed the Clarity Data acquisition system, emerged from the expertise of GE Healthcare's pioneering 3D imaging technology, which permits scanning at unprecedented speed with a very high image resolution.				
** Note that GE Security has been recently bought by SAFRAN Group (April 2009). However, financial figures for 2008 are those related to General Electric Company.* *** GE Group is divided in different business segments, one of them being Technology Infrastructure. Within this, the Enterprise Solutions division includes security and life safety technologies such as detection systems, intrusion and access control, sensor equipment, etc. As there is not data available specifically for GE Security, figures shown correspond to financial data of the Enterprise Solutions division.*				

Source: www.gesecurity.com and *General Electric 2008 Annual Report*

Table 4.6 L3 Security and Detection: Basic company indicators

L3 SECURITY & DETECTION (US)				
Main indicators	**L3 Communications**		**L3 Security & Detection**	
	2007	2008	2007	2008
Turnover	€ 10,187.2m	€ 10,133.5m	€ 611.5m	€ 607.9m
Profit	€ 692.5m	€ 514.15m	N/A	N/A
R&D budget	€ 272.1m	€ 242.1m	N/A	N/A
Number of employees	65,000	N/A	N/A	N/A
Description of the company				
L-3 Communications Corporation is a leading supplier of a broad range of products and services used in a substantial number of aerospace and defense platforms. Within the group, L3 Security and Detection is one of the world's leading suppliers of security screening systems, including advanced systems for inspecting checked baggage, checkpoint screening and cargo and border security. L3 Security and Detection has more than 18,000 systems deployed around the world.				
Main products and technologies				
▪ Its products are related to X-ray equipment (PX series), X-ray (CT) based EDS equipment and ETD (Examiner series), ETD (OptEX), and millimetre wave imaging (ProVision). ▪ L3 screening products incorporate a variety of powerful and proven technologies: computed tomography, conventional and high-energy X-ray, metal detection, active millimeter wave imaging and energetic materials detection.				

Source: www.l-3com.com and L3 Communications 2008 Annual Report

Table 4.7 Rapiscan Systems: Basic company indicators

RAPISCAN SYSTEMS (US)				
Main indicators	**OSI Systems, Inc.**		**Rapiscan Systems**	
	2007	2008	2007	2008
Turnover	€ 388.2m	€ 423.6m	€ 136.2m	€ 153.3m
Profit	€ 13.7m	€ 9.5m	€ 4.8m	€ 3.35m
R&D budget	€ 32.4m	€ 30.8m	N/A	N/A
Number of employees	3,480	3,366	N/A	N/A
Description of the company				
Rapiscan Systems, the security division of OSI Systems, Inc. is a world leading screening equipment provider. The company's products are sold into four market segments: Baggage and Parcel Inspection, Cargo and Vehicle Inspection, Hold Baggage Screening and People Screening. The company has an installed base globally of more than 70,000 security and inspection systems. The Rapiscan Systems product line is manufactured at four locations and supported by a global support service network.				
Main products and technologies				
▪ Its products are related to X-ray equipment (600 and Eagle series), Gamma/Neutron equipment (GaRDS and VEDS series), millimetre wave imaging (Wavescan 200) and RTT baggage screening equipment. ▪ Rapiscan is a leading supplier of security inspection solutions utilizing technologies such as X-ray and gamma-ray imaging, and advanced threat identification techniques such as neutron and diffraction analysis.				

Source: www.rapiscansystems.com and OSI Systems, Inc. 2008 Annual Report

Table 4.8 Reveal Imaging: Basic company indicators

REVEAL IMAGING (US)		
Main indicators	**Reveal Imaging**	
	2005	2006
Turnover	€ 6.2m	€ 38.1m
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	± 200	± 200
Description of the company		
Reveal Imaging Technologies, Inc. was founded in 2002 in direct response to the United States Government's post-9/11 mandate for vastly improved aviation security screening. Hundreds of Reveal systems are now deployed around the globe. The company has expanded its automated screening solution offerings beyond airport-checked baggage to include cabin baggage and various kinds of parcel and cargo screenings for a wide variety of commercial and industrial facilities as well as public events.		
Main products and technologies		
▪ Reveal's products are focused on X-ray (CT) based EDS equipment for baggage, parcels, pallets and bulk cargo (ArrayCT or CT-80 series). Moreover, the company also integrates its equipment with in-line baggage handling systems. ▪ Reveal has recently acquired millimetre wave (MMW) sensor technology for security and screening applications. Moreover, the company has developed the Array Motion Imaging (AMI) system and the Dual Energy technology (Reveal's Computed Tomography technology) to provide higher performance in screening processes with a lower false alarm rate.		

Source: www.revealimaging.com and web research

Table 4.9 American Science & Engineering: Basic company indicators

AMERICAN SCIENCE & ENGINEERING (US)		
Main indicators	**American Science & Engineering**	
	2007	2008
Turnover	€ 111.8m	€ 113.4m
Profit	€ 18m	€ 11.9m
R&D budget	€ 5.2m	€ 8.3m
Number of employees	229	346
Description of the company		
AS&E has a strong and storied history of scientific innovation, particularly in the field of X-ray technology. Formed in 1958, AS&E began as a developer of scientific instruments and applications for NASA. In subsequent years, AS&E also developed innovative technologies in the fields of defense, education, medicine, non-destructive testing, and security. Currently, AS&E's X-ray inspection systems can be found in 137 countries around the world and are used by leading government agencies, border authorities, military bases, airports, and corporations worldwide in many mission-critical applications. International sales (outside US) accounted for approximately 36% of total company sales in 2008. Europe accounts for 14% of international company's revenue during 2008.		
Main products and technologies		
▪ AS&E's products are focused on all types of X-ray equipment for persons (Smartcheck), baggage & parcels (Gemini Series), bulk cargo and vehicles (Omniview and Z series). ▪ AS&E main technologies include Z Backscatter technology (high image clarity), Shaped Energy (patented high-energy transmission technology) and RTD (Radioactive Threat Detection (RTD) systems).		

Source: www.as-e.com and *AS&E 2008 Annual Report*

Table 4.10 Gilardoni: Basic company indicators

GILARDONI (IT)		
Main indicators	**Gilardoni**	
	2007	2008
Turnover	Around € 59m	Around € 59m
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	± 225	± 225
Description of the company		
Gilardoni is among the main European suppliers of X-ray and ultrasonic equipments, OEM components and services relating to security, medical and the non destructive testing sectors. Gilardoni offers a complete range of solutions to satisfy security market needs, from small control systems for hand baggage to mobile control systems for large objects such as cargo parcels. Its activities are centralised at its industrial plant in Mandello del Lario (Lecco, Italy). Around € 20 million of the total company's turnover relates to x-ray equipment, mainly for the aviation sector.		
Main products and technologies		
▪ Its products are mainly related to X-ray equipment (FEP series) and X-ray (CT) based EDS equipment (FEP ME 640 DEXGIL) as well as software systems (such as ADS: Advanced Detection System or TIP: Threat Insertion software, inserting false positive images into the operator screen –complying with EU Regulation 23/2008). ▪ GIlardoni manufactures its own monoblocks and X-ray tubes.		

Source: www.gilardoni.it and web research

4.3.3 Technology aspects

Although complex, the underlying technologies for x-ray based detection systems are well established. The main technological developments that have shaped the currently available x-ray systems have focussed on aspects such as increasing the resolution and clarity of the generated images, providing multiple views of screened objects (including 3D image generation based on computed tomography (CT) and real time tomography), and allowing for greater discrimination between substance types/densities (e.g. use of dual energy x-rays)[188].

By and large, current technological developments are based upon incremental advances to the underlying technologies. So-called advanced x-ray technologies (AT x-ray) provide high definition images and incorporate features such as multiple views, high definition zoom and automated detection capabilities[189]. Specific technological developments for security applications tend to be pushed by changes in threat perceptions (and consequential regulatory requirements); for example, as is the case with current preoccupations on the detection of liquid explosives in passenger luggage.

Taking account of the above, a major part of the focus for current product development – and a major driver of value added – relates to the development of data processing software and algorithms used for interpretation and assessment of x-ray generated images and data in order to reliably detect a wide range of explosives and explosive devices (and other prohibited/dangerous items).

[188] Backscatter x-ray techniques are of limited application in the area of cargo screening given their limited penetration.
[189] See, TSA advanced technology checkpoint x-ray: http://www.tsa.gov/approach/tech/advanced_technology.shtm

A further area of development is a move towards more automated systems that are less reliant on human operators – often seen as potentially the weakest link in the airport security chain[190]. Equally, if not more importantly, the development of more automated systems reflects the fact that labour costs for screening personnel represents a major component of the overall cost of operating screening equipment, while the reliance on human operators is a factor limiting the rate of throughput for screened items.

Specifically with respect to air cargo screening – as noted earlier – there exist considerable limitations in existing screening equipment, which largely rely on technologies that have been developed for screening of passenger luggage. The development of technologies and systems for screening cargo, especially for explosives detection, is an important challenge for equipment providers.

4.3.4 Component supply

With regard to x-ray based detection systems, these can be broken down into the following principle components: x-ray camera / generator, detectors, imaging systems, together with the accompanying software for data processing and image analysis and, finally, the casing in which the equipment is housed.

In terms of the main hardware components, these are either produced 'in house' or increasingly sourced from specialised components suppliers. Given the quality and size requirements for security screening equipment in the aviation sector, the number of global specialised components suppliers appears to be very limited[191]. An exception is in the manufacturer of the cabinets in which equipment is housed, for which OEMs can look for 'low cost' supply opportunities; for example, Smith's Detection is sourcing cabinets from Eastern Europe.

4.3.5 Equipment and sub-systems

The main suppliers of screening equipment to the air transport sector have been described in section 4.3.2.

Typical manufacturing activities – which increasingly relates to final assembly – is undertaken 'in-house' and at the main business locations of equipment suppliers (i.e. USA, W. Europe). This reflects the need for close oversight of product assembly and for maintaining proximity between manufacturing activities and technical and systems development activities[192]. Smaller companies (e.g. producers of specialised equipment) may outsource manufacturing/assembly activities but this is generally not the case.

---

[190] The use of threat image projection (TIP) software to monitor (and train) screeners is one area of technological development aimed specifically at enhancing the performance of screeners, and to assist in ensuring they are to effectively interpret the screening images and information provided.

[191] Leading suppliers of x-ray tubes/generators include, for example: COMET AG (Switzerland), Lohmann X-Ray GmbH (Germany), Spellman High Voltage Electronics (USA). For optoelectronic detectors, there exist a handful of leading global suppliers. In this respect, we can note the linkage between Rapiscan and OSI Optoelectronics (both part of the OSI Group); see footnote 181. Also notable is Varian (US), which is a leading supplier of products for x-ray imaging to cargo screening system manufacturers. Note: It has not been possible to systematically identify leading supplier of imaging components.

[192] An additional factor in production location decisions relates to equipment/technologies that may be classified by national authorities, which may inhibit location of production activities outside of Europe and/or the USA.

There is, however, the possibility that manufacturing / assembly activities may be relocated outside of US/Europe, partly to reduce costs but also in response to market opportunities; for example, in 2006 Smiths detection opened an x-ray production/assembly site in St Petersburg to serve the growing Russian market. Another aspect of production that may eventually become subject to outsourcing and/or off-shoring is software development, which can be extremely labour intensive[193]. However, software development is currently considered a core process and major source of value added and, in addition, an area of particular sensitivity for governments (and customers). Accordingly, it is unclear to what extent software related activities could be relocated.

4.3.6 Integration and customisation

For the aviation/airport market OEMs typically supply directly to the market, based on their range of available products/equipment. The degree of customisation for specific clients is limited, although there appears to be a shift towards more modular approaches to equipment design, enabling greater flexibility in production and greater ease of replacement and updating of sub-systems and equipment. Generally, the user (i.e. airport, air carrier etc.) has had the responsibility to develop and implement overall security solutions, including the integration of different types of equipment. There is, however, increasing demand for the provision of more integrated systems that address a range of security requirements (i.e. persons, luggage, cargo, perimeter, etc.), for example at the level of an airport or terminal. This is reflected in increased size of projects combined with enhanced requirements for networking of equipment and greater interoperability of systems.

Delivery of large projects remains the domain of the major systems integrators[194] and there appears to be a general consensus among equipment suppliers that they neither want nor are able to challenge the position of these large integrators. However, there is a question as to the position equipment suppliers should adopt in response to the demand for integrated systems. There seems to be mixed opinions as to whether the market will favour specialisation and expertise in specific product/technology domains or whether it will favour companies able to supply a broader range of equipment. Essentially this is a question of whether integrators will pick and chose the 'best' supplier for each type of equipment or will opt for a more limited number of suppliers able to provide security 'capabilities' covering a range of equipment requirements.

The market shift towards larger but fewer projects increases the 'risks' associated with failure to be selected as a supplier for a specific project, thus providing a further challenge for equipment suppliers. This can be expected to raise the intensity of competition among equipment suppliers while, at the same time, potentially strengthening the position of integrators/clients to demand cost reductions. In addition, larger but fewer projects, may lead to greater 'lumpiness' in received orders, with associated consequences for production planning.

[193] For example, Smith's Detection indicates that automatic explosives detection software development required ½ million man hours. Source: "Opportunities to create value" presentation made at Smith's Detection Investor Day, 27 January 2009, available at: http://www.smiths-group.com/presentations.aspx

[194] For example, Thales, Finmeccanica, etc. from the 'defence' sector or 'civil' systems integrators such as Siemens.

4.3.7 Related services

Customer support services

The main support services provided by scanning equipment suppliers cover equipment maintenance, operational testing and increasingly upgrade services (e.g. software and threat recognition for automated systems). The provision of these services, which may be covered in the purchase price or more typically by a service contract, are an important element in the overall revenue of equipment suppliers and of the total cost to the customer. Also provided is support in the event of equipment malfunctioning or failure.

An important aspect related to support services relates to the ability of equipment providers – and their related suppliers of components / sub-systems – to rapidly deliver 'spare parts' to customers. For this, it can be an advantage for OEMs to deal with suppliers of components and sub-systems, which operate extensive distribution (parts banks/warehouses) networks. In turn, given the relative limited size of the security market, this can be an additional factor favouring the use of external suppliers of components / sub-systems over 'in-house' manufacturing.

Related "operational" services

The main operational service associated with screening equipment is the provision of equipment operators. Depending on the legal and organisational structure, these may be staff of the infrastructure operator (i.e. airport operator, cargo handling facility operator, etc.) or be supplied by private security service providers, or may be customs personnel etc. The vigilance and expertise of these operators in interpreting images generated by screening equipment is a crucial element of the overall level of security provided by the equipment. However, the reliance on human operators is seen as a potentially weak link in security screening procedures and screening equipment systems are rated as 'complex' by private security services, requiring continuous and intensive training[195]. This is one factor behind efforts to develop more automated systems of screening. However, particularly in the context of cargo screening, the extent to which automated systems can be applied is limited.

The level and frequency (i.e. in response to new types of threat) of training provided for screening operators is an important associated operational service for screening operations. Such training will be provided by equipment supplier but can also be provided by larger private security service providers[196], specialised training service providers (including providers of training software)[197], or government agencies[198].

[195] Information gathered from COESS (Confederation of European Security Services) and ASSA-I (Aviation Security Services Association – International) questionnaires sent to their members for the purpose of this study.

[196] See, for example, G4S Aviation training services (http://www.g4s.com/uk/uk-what_we_do/uk-aviation/uk-aviation_training_services-2.htm)

[197] See: for example:

- Quadratica (http://www.quadratica.co.uk/)
- Renful Premier (http://www.renful.co.uk/)
- Smart Approach (http://www.smartapproach.com/)

[198] See for example the UK Department for Transport (http://www.dft.gov.uk/pgr/security/aviation/aviationsecuritytraining?page=6)

A further development related to maintaining the vigilance and expertise of operators is the integration of Threat Image Projection (TIP) into screening systems. TIP superimposes threat item images onto live screening images, which aims to heighten operator alertness by requiring them to more frequently interpret images and make decisions. At the same time TIP feedback can be used to assess individual operator's performance and identify where additional training may be required.

4.3.8 Linkages to final markets

All major manufacturers of scanning equipment have specialised departments in order to sell and distribute their equipment. These OEMs perform all tasks required to supply and install scanning equipment to clients. As noted earlier (see Section 4.3.6), the major systems integrators may provide the linkage between equipment suppliers and final customers. Occasionally, security service providers may also be involved, but typically the equipment used by these providers will be purchased by airport operator, air carrier, or cargo handling facility etc.

4.3.9 Overall assessment of the supply chain

As described above, the global supply of security screening equipment for use in the aviation sector is dominated by a few major players that are the main equipment integrators. This situation is in itself a reflection of the rather limited market size, and specific requirements for screening equipment within the aviation sector, which constitute an important barrier for the entry of new firms.

From a technology perspective, the main focus for the security equipment sector can be seen to be oriented towards the adaptation and refinement of underlying technologies to the specific requirements of security based applications. A specific focus is on "soft" elements (i.e. software development and system design), rather than on "hard" elements (i.e. devices and sub-systems). This development has important implications for the development and future shape of the supply chain. For example, although some firms continue to produce components/sub-systems in-house, there seems to be a trend towards disengagement from such activities. This may reflect the relatively small size of the security market, and the fact that specialised external components and sub-system suppliers are able to leverage a broader market demand, in terms of both production and investment in technology development. In this regard, it is questionable whether "breakthrough" technological developments are likely from within the security screening equipment sector, or whether they will be 'imported' and 'adapted' from technological developments made 'elsewhere'.

4.4 Main trends and developments

4.4.1 Market trends and developments

Changing facets of security threats

As noted earlier, changes in the *modus operandi* of terrorists have been a major driver in the type of security solutions required by the aviation sector and the overall level of demand. As has been seen, the changing facets of security threats create additional needs

that have required security solutions that go beyond metal detection or simple x-ray systems (e.g. detection of materials such as powders, ceramics, plastics, explosives, liquids, etc.) It is widely recognised that addressing these 'advanced' security needs is likely to require considerable investment and resources. On the one hand, part of these investment and resources will need to come from the security industry. On the other hand, policymakers and aviation security planners need to offer a clear strategy and planning in order to provide an environment in which solutions can evolve.

Typically, the past and sometimes current approach has been that changing security threats are addressed by 'adding-on' additional security capabilities to existing equipment and systems in a largely non-integrated way. This is to say, specific capabilities and technologies such as metal detection, x-ray scanning, and explosives or CBRN detection are provided through separate equipment and systems (and even relatively uncoordinated security procedures for their use). As described in Section 4.3.6, there is increasing demand for more integrated solutions, combined with increasing size in individual security projects. In general, the ambition is to achieve security solutions based on integrated platforms that address all (main) threats while being compatible with routine airport processes and with sufficient flexibility to integrate additional capabilities as new threats arise. However, the current situation is that such fully integrated solutions are some way from becoming a reality, not only for passenger and luggage screening but also for air cargo.

Legislative framework and governmental response

EU legislation aims to impose standard security requirements across all Member States and is likely to heighten overall demand for airport security equipment. The initial EU legislation was laid out in Regulation 2320/2002 and the European Commission subsequently moved to pass complementary legislation to bring simplification, harmonisation and clarification of the existing rules in this Regulation. New regulations aimed at further improving levels of security in the civil aviation industry across the EU, are set out in Regulation 300/2008 to enter into force no later than April 2010. (See section 4.5.1 for more details)

Despite the positive trends driven by these legislative developments, some commentators point to the sluggish response from the EU and individual governments when it comes to prioritising airport security that has resulted in low purchase rates for airport security equipment. The high costs associated with the purchase of airport security equipment also remain a major barrier to the faster adoption of increasingly essential equipment[199]. Nonetheless, the requirement that airfreight companies from EU countries must ensure that all cargo is safe – whether coming from a 'regulated agent'[200] or unknown shipper – means that cargo carriers need to invest heavily in buying necessary equipment and making required changes to their operations.

The situation in the USA, where 100% screening of all cargo carried on passenger aircraft should be implemented by August 2010, are similar (see section 0). However, there is hesitancy on the part of the aviation industry to invest in new screening equipment when

[199] Frost&Sullivan "The European Airport Security Equipment Market: A Growth Story in the Making" published in June 2007.
[200] See section 4.2.4.

final rules for cargo security are not defined and the Transportation Security Administration has not defined certification standards for the technology need to screen cargo. As the Air Transport Association has noted *"The biggest challenge in meeting the August 2010 deadline is the lack of TSA-certified screening technology to inspect large air cargo pallets. Most pieces of cargo transported on wide-body aircraft are consolidated into large shipments and 75 percent of cargo is transported on wide-body aircraft. … Shippers and freight forwarders typically create these pallet-size shipments before they are tendered to an airline. The dilemma is that screening is required at the piece level but existing technology cannot screen large consolidated shipments"*[201].

Economic conditions

The rise in air traffic witnessed over the past years has generated a growing need for efficient aviation security solutions capable of safeguarding the entire airport network (i.e. from measures to detect anomalies at the outer perimeter to measures inside the airport to identify intruders and detect suspicious movements) and air transportation. However, a prolonged economic slowdown and adverse macro-economic conditions could moderate the pace of this growth to some degree. For example, ACI-Europe report that overall freight traffic among European airports recorded a fall of nearly a quarter (-23.1%) in the first quarter of 2009 when compared to the same period in 2008[202].

Changes in the volume of freight being transported by air have an impact on the demand for cargo inspection and screening capacity and, in turn, the underlying demand for security equipment and systems for this purpose. Although the current economic slowdown is having the effect of reducing air cargo volumes and hence overall demand for inspection and screening capacity, perversely it may actually increase demand at air cargo handling / airport facilities. This may arise because, in an effort to reduce costs in a difficult economic period, agents within the supply chain may attempt to cut their own security-related activities/costs and push responsibility for cargo screening down the supply chain (i.e. ultimately to the cargo handler / carrier).

Acceptability of security technologies

The aviation security equipment market is also influenced by attitudes/acceptability of security technologies. For example, the use of body scanners: the USA have pushed forward development (e.g. support for R&D) of the whole body scanner, addressing 'privacy' issues through the development of equipment that produce standardised output images; in Europe, the European Parliament has passed a non-binding resolution[203] for the Commission to carry out an assessment of the technology, thus putting in doubt whether such technology will be adopted in European airports.

[201] Statement of James C. May, President and CEO, Air Transport Association of America, Inc. before the Subcommittee on Transportation Security and Infrastructure Protection of the House Committee on Homeland Security, March 18, 2009. Available at: http://www.airlines.org/government/testimony/2009/ATA+Testifies+on+Air+Cargo+Screening.htm

[202] ACI Europe Airport Traffic Report - May 2009'

[203] European Parliament resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection (non-binding resolution adopted on 23.10.08).

4.4.2 Technology trends and developments

Technology development: focus on 'soft' elements

In the absence of fundamental new technological discoveries that can be applied to the inspection and screening equipment sector, the underlying technologies and capabilities that companies can offer are similar. Thus, the main EU and US companies distinguish themselves on the basis of proprietary technologies that offer specific enhancements to the user (e.g. higher resolution images, greater differentiation of substances, faster processing, etc.). This requires considerable investments in research and technology development, in particular focussed on 'soft' elements that are largely specific to the security to security requirements (e.g. data processing and algorithms for threat interpretation and assessment).

Support for research and innovation

The EU Framework Programmes FP6 (2000-2006) gave only very little attention to the theme of security. For the first time, a separate security research programme was created in FP7 (2007-2013), which also included some projects involved in the field of aviation security. However, stakeholders from the aviation sector and security equipment providers seem to be of the opinion that much of the funded research is not end user-oriented and is directed to outputs that are of limited applicability in the 'real world'[204].

The US is devoting a significant budget to research activities on air security equipment and the related study and definition of security threats[205]. The increase in R&D and innovation initiatives for US companies has increased demand for new types of products and equipment in the United States.

4.4.3 Production trends and developments

Manufacturing: shift away from 'hard' elements

The focus on 'soft' elements (see above) appears to be combined with a shift away from 'hard' elements. This is reflected in a trend for suppliers of security inspection and screening equipment to disengage from the manufacturer of components and sub-systems, which they source from specialised providers that supply to a wider market (e.g. industrial, health, and consumer applications). Generally, the size of the security market alone is insufficient to offset the investment in research and technology development or to achieve the scale of production necessary to remain competitive in the production of specialised components and sub-systems. In addition, a broader market portfolio may be necessary in order to offset the volatility in demand within the security market. We see, therefore, that those companies active in the security domain that are also engaged in the development and supply of sub-systems tend to do so only where they are also supplying to wider markets.

[204] An issue raised in this connection is whether – given the fundamental importance of security for the welfare of EU citizens – such research programmes should prioritise 'blue sky' and 'multi-national collaboration' over research that is actually likely to enhance security.

[205] In the US, security is seen as a major responsibility for the State: President Obama has planned to spend $1bn on aviation security (mainly on hold baggage screening technologies, which were left behind in the past in favour of other types of equipment). Source: ACI-Europe and desk research.

Given the above, there is some hollowing out of the production process, with companies buying-in sub-systems and focussing their expertise on the integration of sub-systems and final assembly. Concerning the element of final assembly, this is an activity that may eventually become subject to increased outsourcing or the relocation of assembly activities to low cost locations, particularly if these are also in regions that offer sufficient market opportunities in themselves.

Development of more integrated systems

A further feature of the market that is shaping developments in production activities is the increased demand for more integrated security systems (see Section 4.3.6 and Section 4.4.1). This is characterised by projects that require increased networking of security equipment, and the integration of different equipment and systems to provide more comprehensive security solutions. One description of this development is that the *"business is moving towards total system capability, delivering that capability to airports or to critical infrastructure rather than just delivering boxes that can find bombs or chemical weapons."*[206] As noted earlier, this development raises issues concerning the position and relationship between equipment suppliers and the major security system integrators. It also highlights the importance of interoperability between equipment and systems in order to exchange information and deliver systems capabilities. More broadly, rather than focussing on individual 'boxes' it also brings to the forefront the need to focus on overall security processes; for example, in terms of procedures for analysing and integrating information from different sources, and implementing appropriate response procedures.

4.4.4 Overall assessment of trends and developments

In western countries, the overall market for aviation security inspection and screening equipment, and specifically the air cargo security market, is primarily driven by regulatory requirements and standards. These regulatory requirements and standards are, in themselves, a reflection of specific incidents and changes in perceptions of security threats. In principle, the general developments in the regulatory environment should provide the basis for sustained growth in demand for screening equipment.

There are, however, a range of remaining issues that have not yet been fully resolved. For example, in the case of air cargo, current technologies do not yet permit full screening of air cargo which presents a challenge to the equipment industry and regulators. Until resolved, this creates uncertainty over which technologies and systems will be approved and, in turn, what equipment will be demanded by the market. Also, choices need to be made as to how, and by whom, the costs of implementing enhanced air cargo security systems should be met and, furthermore, what impact this will have on the competitiveness of the air cargo sector and the companies operating therein. In turn, this will have implications for the budgets available for purchasing equipment and on the characteristics of the market.

[206] Stephen Phipsen – President, Smiths Detection. Source: Smiths Detection Investor Day (January 2009) transcript, available at: http://www.smiths-group.com/presentations.aspx.

Notwithstanding the kinds of uncertainties mentioned above, from both a supply and a demand side perspective, the key underlying trend appears to be a shift away from an equipment-based perspective of the sector to an integrated capabilities approach. Thus, it is no longer the case that value-added is generated through 'hard' elements (i.e. equipment and manufacturing) but through 'soft' elements (i.e. software, system capabilities, technology development). This may have profound implications, in terms of the knowledge and skills that will underpin future competitiveness.
International, European and national security-related regulatory conditions

4.5 Regulatory conditions and development

4.5.1 International, European and national security-related regulatory conditions

European (EU) and Member States' security-related regulatory conditions
EU regulations have stepped-up all aviation security standards since the events of 11 September 2001. These regulations make the security measures laid down by the International Civil Aviation Organisation (ICAO)[207] (see Box **4.3**); and the European Civil Aviation Conference (ECAC)[208] compulsory within the European Union. In particular, these provisions establish a system of unannounced inspections, introduce more rigorous screening of passengers, luggage and staff, and require Member States to introduce national security programmes and common standards for equipment.

Box 4.3 ICAO Standards

'Standards and Recommended Practices' (SARPs):

Annex 17 to the Chicago Convention contains several SARPs dealing with passengers and baggage security, cargo security and aircraft and in-flight security. One of the main aims is at preventing explosives and incendiary devices from being placed onboard the aircraft, either through concealment in the otherwise legitimate shipments or through gaining access to aircraft via cargo handling areas.

Annex 9 to the Chicago Convention contains security-related provisions dealing with the facilitation of control processes and including, apart from general principles, security provisions related to: Entry and departure of persons and their baggage, entry and departure of cargo and other articles and a categorisation of inadmissible persons and deportees.

Source: www.icao.int

[207] The International Civil Aviation Organization, a UN Specialized Agency, is the global forum for civil aviation. ICAO has the responsibility for regulating the many technical aspects of international civil aviation, with the main purpose of promoting aviation safety and security through cooperation amongst its member States. Website: www.icao.int

[208] Founded in 1955 as an intergovernmental organisation, ECAC's objective is to promote the continued development of a safe, efficient and sustainable European air transport system. In so doing, ECAC seeks to: 1) harmonise civil aviation policies and practices amongst its Member States; 2) promote understanding on policy matters between its Member States and other parts of the world. Website: www.ecac-ceac.org.

Overall, the aviation security sector is a heavy and complex regulatory environment. The current legislation (EC) 2320/2002[209] has continuously been under review and subjected to various amendments in order to enhance the level of security or to adapt the legislation to new technological developments.

Based on a Commission proposal on common rules in the field of civil aviation security (2005)[210], the new Commission Regulation 300/2008[211] (already approved by Council and Parliament) will come into force in April 2010. The new regulation has been motivated by seeking simplification, harmonisation and clarification of the existing rules and the improvement of the levels of security. Moreover, it has been conceived to be able to adapt to evolving risk assessments (flexibility) and to allow new technologies to be introduced. In terms of the types of equipment and systems that may be used for screening, these are specified in Commission Regulation (EC) No 272/2009, to be implemented by no later than April 2010[212].

EU air cargo security regulation

As previously mentioned, EU Regulation 2320/2002 established common rules in the field of civil aviation security as well as appropriate compliance monitoring mechanisms, applicable to any airport located in the territories of the Member States of the EU. The framework legislation includes specific rules for cargo handling screening and protection, with air cargo security being primarily a responsibility of airlines. Rules are applicable to all cargo, to be carried either on passenger or all-cargo aircrafts. According to point 6 of the Annex to Regulation 2320/2002, all cargo, courier and express parcels intended to be carried on passenger or all-cargo aircrafts shall be subjected to the security controls (established under point 6.3; see Box 4.4)

Box 4.4 Air Cargo Security (Point 6.3, Annex to Regulation 2320/2002)

1. Cargo, courier and express parcels shall only be carried by air where the following security controls have been applied:

(a) the reception, processing and handling of cargo shall be performed by properly recruited and trained staff;

(b) cargo shall be:

(i) searched by hand or physical check; or

(ii) screened by x-ray equipment; or

(iii) subjected to simulation chamber; or

(iv) subjected to other means, both technical and bio-sensory, (e.g. sniffers, trace detectors, explosive detection dogs etc.)

[209] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security

[210] COM(2005) 429 final: Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security

[211] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

[212] The Regulation also allows for the use of other methods for the purpose of testing new technologies: "In order to evaluate methods of screening using new technologies not foreseen at the time of adoption of this Regulation, the implementing rules to be adopted pursuant to Article 4(3) of Regulation (EC) No 300/2008 may allow the use of other methods on a trial basis and for a limited period of time on condition that such trials do not prejudice the overall levels of security."

2. Once security controls have been implemented, including controls on cargo from known consignors, whether on or off airport grounds, sterility of the shipments shall be maintained until such time as it is placed onboard aircraft and maintained until the departure of the aircraft.

3. The security controls detailed in paragraph 1 need not be applied in respect of:
(a) cargo received from a known consignor;
(b) transhipment cargo;
(c) cargo whose origin and handling conditions ensure that it presents no security threat;
(d) cargo which is subject to regulatory requirements providing for an appropriate level of security protection.

Source: Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security

As mentioned above, Regulation 2320/2002 includes the obligation of maintaining the 'sterility of the shipments' and also introduces the terms *regulated agent* (an agent, freight forwarder or other entity that conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo) and *known consignor* (the originator of property for transportation by air for his own account and who has established business with a regulated agent or air carrier).

Normally, the screening requirements are applicable for the country of origin (i.e. screening of outbound cargo); this is the case in Europe with the application of Regulation 2320/2002. Each airline must comply with a specific security programme and the equipment used must be certified (at national level).

There is normally no requirement to screen inbound cargo at the arrival point; i.e. there is no requirement to screen inbound cargo entering Europe from a 'third' country. Similarly, the EU does not impose screening requirements – at the outbound location - on inbound cargos destined for the EU. By contrast, the USA is setting requirements that mean that inbound cargos are screened at the outbound airport (i.e. screening of cargos at airport from which it is sent); this means cargo from the EU – or at least currently an agreed proportion of cargo – destined for the USA must be screened)[213].

US aviation security-related regulatory framework

In the US, the Transportation Security Administration (TSA) is responsible for ensuring the security of all modes of transportation, including cargo placed aboard airplanes and particularly focuses on passenger-carrying planes. With respect to air cargo security, the TSA states[214] that its vision is the creation of a layered solution designed to protect against security breaches by using a combination of process along with information and technology-based solutions, while preserving the integrity of the air cargo supply chain. In response to possible threats to air cargo security, TSA uses a multi-layered approach that includes:

[213] TSA Cargo Security measures require different screening measures to be applied for cargo accepted for flights departing from an EU airport to the U.S. (currently at least 50% of cargo on passenger flights must be screened). However, European Airlines consider these TSA security measures as redundant and would cause widespread impact on the manufacturing and supply chain reaching far beyond EU airports. Source: European Commission, DG TREN F/5 (Aviation Security Unit) and AEA Cargo Security Working Group.

[214] Source: Transport Security Administration: http://www.tsa.gov/what_we_do/tsnm/air_cargo/index.shtm

- Vetting companies that ship and transport cargo on passenger planes to ensure they meet TSA security standards.
- Establishing a system to enable Certified Cargo Screening Facilities (CCSFs) to physically screen cargo using approved screening methods and technologies.
- Employing random and risk based assessment to identify high-risk cargo that requires increased scrutiny
- Inspecting industry compliance with security regulations through the deployment of TSA inspectors.

The US regulatory environment for air cargo security is summarised in Box **4.5**.

Box 4.5 US regulatory environment for cargo screening

Under the US 9/11 Bill[215], which was signed into law on August 3, 2007, the Secretary of Homeland Security is required to establish a system to screen 100 percent of cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all such passenger aircraft carrying cargo. The system for screening shall require, at a minimum, that equipment, technology, procedures, personnel, or other methods approved by the Administrator of the Transportation Security Administration, are used to screen cargo carried on passenger aircraft to provide a level of security commensurate with the level of security for the screening of passenger checked baggage as follows:

- 50 percent of such cargo is so screened not later than 18 months after the date of enactment of the Bill (i.e. February 2009).
- 100 percent of such cargo is so screened not later than 3 years after such date of enactment (i.e. August 2010).

For the purposes of the relevant section of the Bill, the term `screening' means a physical examination or non-intrusive methods of assessing whether cargo poses a threat to transportation security. Methods of screening include:

- x-ray systems,
- explosives detection systems,
- explosives trace detection,
- explosives detection canine teams certified by the Transportation Security Administration, or
- physical search together with manifest verification.

Furthermore, the Administrator may approve additional methods to ensure that the cargo does not pose a threat to transportation security and to assist in meeting the requirements [of this subsection]. Such additional cargo screening methods shall not include solely performing a review of information about the contents of cargo or verifying the identity of a shipper of the cargo that is not performed in conjunction with other security methods authorized under this subsection, including whether a known shipper is registered in the known shipper database. Such additional cargo screening methods may include a program to certify the security methods used by shippers … and alternative screening methods.

According to the TSA[216], it has met the mandates of the law to date and currently 50 percent of air cargo on passenger carrying aircraft is screened. One hundred percent of the cargo on 96 percent of the flights originating

[215] Implementing Recommendations of the 9/11 Commission Act of 2007
[216] http://www.tsa.gov/what_we_do/layers/aircargo/index.shtm

in the United States is now screened[217]. In addition, by October 2008, 100 percent of cargo transported on narrow-body (single-aisle) aircraft was achieved[218].

A TSA testimony in March 2009[219], noted that the Administration is "*turning our attention to the development of appropriate technology for the screening of air cargo. One of the challenges we face is the limitations of the currently available technology - specifically, the effectiveness of existing technology for detecting explosives in cargo, its operational feasibility, and its general availability for deployment to the industry to meet the mandate of the 9/11 Act. Until recently the focus of research and development of explosives detection technology has been on the development of screening technology for checked baggage, not cargo. … The characteristics of checked baggage are vastly different from those of cargo - in size, weight, variety of content, and configuration. Consequently the technology designed to screen one is not automatically suitable to screen the other. Because checked baggage screening technology (for example, Explosives Detection Systems (EDS), Explosives Trace Detection (ETD), and X-Ray) is available, however, TSA is working with the DHS Science and Technology Directorate (S&T) to explore ways in which checked baggage screening technology can be adapted to the cargo screening environment. To this end, TSA has created a list of approved technologies to screen cargo based on checked baggage screening technologies. To ascertain the effectiveness of baggage technologies on screening cargo, we are conducting a voluntary pilot program with certain IACs (Indirect Air Carriers)".*[220,221]

4.5.2 Industry and market based standards

Security procedures and performance-based standards

Regulation 2320/2002 introduces some guidelines for equipment contained in the Annex of the Regulation regarding metal detection equipment and X-ray equipment (this includes conventional x-rays as well as EDS/EDDS[222] used in indicative mode).

EU performance standards for security equipment are based on a sliding scale that increases in stringency over time. This scale is used to match evolving security requirements with new technological developments[223]. So far, these standards affect metal detectors, x-ray screening equipment and EDS. The sliding scale is mainly based on

[217] This implies that eighty-five percent of the passengers flying each day from U.S. airports are on planes where all of the cargo has been fully screened.

[218] Although these aircraft carry only 25 percent of domestic air cargo on passenger aircraft, they account for the majority - approximately 95 percent - of domestic passenger flights and more than 80 percent of all passengers on flights originating in the United States.

[219] United States Department of Homeland Security, Transport Security Administration, statement of Edward Kelly, General Manager, Air Cargo before the Subcommittee on Transportation Security and Infrastructure Protect Committee on Homeland Security, United States House of Representatives (March 18, 2009), available at: http://www.tsa.gov/press/speeches/031809_kelly_air_cargo.shtm

[220] Otherwise referred to as freight forwarders. An Indirect Air Carrier (IAC) means any person or entity within the United States not in possession of an Federal Aviation Administration air carrier operating certificate, that undertakes to engage indirectly in air transportation of property and uses for all or any part of such transportation the services of a passenger air carrier. Source: http://www.tsa.gov/what_we_do/layers/aircargo/indirect.shtm.

[221] IACs participating in the assessment must agree to purchase specified technologies to screen cargo and report to TSA on its effectiveness. TSA is partially funding this research and the IACs are responsible for the remainder of the costs.

[222] 'EDS' refers to Explosive Detection System while 'EDDS' responds to Explosive Device Detection System.

[223] One important issue when considering the influence of legislative developments on market conditions for security equipment is that legislation – specifically where such legislation sets minimum performance standards for security equipment and systems – might actually become a limiting factor on the market and technological development. In a commercial and competitive environment, where security costs have an impact on the financial performance of, for example, airports and air carriers (or other actors in the supply chain), provided that the minimum performance standards are met then there may be a disincentive to invest in equipment or systems offering higher performance if this implies higher costs. The introduction of sliding scale requirements that increase in stringency over time can be seen as a mechanism to avoid a situation in which minimum standards become the 'norm' within the sector.

either the detection of smaller harmful or unlawful objects or the improvement of visual acuity. However, European-level standards do not exist for all technologies (e.g. trace-detection, hand-held screening, body-scanners and canine methods do not having standards at EU level). The European Commission is looking at developing standards for the aforesaid technologies/equipment in the future[224].

However, as explicitly expressed by the European legislation, EU regulations only provide 'guidelines' which have to be further developed by Member States. The adoption of different approaches to determining and setting specific standards by Member States contributes to continuing fragmentation of the EU markets.

Quality/performance related standards within the secure supply chain

The secure transportation of goods by air implies that organisations working within or relying on the logistics industry such as freight forwarders[225] have a framework to assess security risks and implement controls and mitigating arrangements to manage potential security threats and impacts on the supply chain:

- **ISO/28000 series**: It establishes a high level management standard that enables an organisation to establish an overall supply chain security management system. It requires the organisation to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization (or freight forwarder) should implement mechanisms and processes to meet these needs.
- **TAPA requirements**: TAPA (Technology Asset Protection Association[226]) has established Freight Security Requirements (FSR) to ensure the safe and secure in-transit storage and warehousing of assets through the world. The FSR specifies the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards.

Certification schemes

International systems for approval and certification of identification and detection security equipment do not currently exist. This is the case within the EU, where approval and certification of equipment takes place at the national level (i.e. no EU-level certification). A lack of mutual recognition of national approval and certification systems, combined with differences/anomalies across countries in testing and approval procedures, results in a complex market situation. For example:

- Technologies/procedures recognised in one country are not recognised in another; for example, Germany does not recognise the use of dogs as a reliable system for explosives detection but they are used in France and the UK; ETD is certified in the US as a stand-alone technology whereas in most EU countries ETD has to be complemented with other approaches.

[224] Based on interview with Mr. Eckard Seebohm (DG TREN, Head of Unit, Aviation Security) and Mr. Robert Missen (DG TREN, Deputy Head of Unit, Aviation Security).

[225] According to CLECAT (European Association for forwarding, transport, logistics and customs services), European freight forwarders and customs agents clear 95% of all goods in Europe and handle 65% of the cargo transported by road, 95% of the cargo transported by air and 65% of the maritime.

[226] TAPA is an association of security professionals and related business partners from high technology and high value companies who have organised for the purpose of addressing the emerging security threats that are common to the high value industry supply chain (www.tapaonline.org).

- Equipment approved in one country is not approved in another. This may occur even where the same required performance characteristics are required but differences in testing procedures lead to approval in one country but rejection in another.

However, new initiatives are recently emerging to counteract this situation. The Network of Testing Facilities for CBRNE detection equipment (CREATIF Network)[227] has been running since February 2009 under the Framework Programme 7 (Security – Cooperation action). Its objective is the provision of a platform for the exchange of views and knowledge in order to discuss testing protocols and standards for detection practices (both at geographical –EU27– and technical level). The network is also planning to publish a roadmap for a European certification system for CBRNE detection products and services.

4.5.3 Overall assessment of regulatory conditions and related policy initiatives

In the area of air transport security there are some suggestions that the EU security equipment industry is in a disadvantageous position *vis à vis* the US. Although EU legislation sets an overall framework for aviation security, Member States are responsible for implementation and for setting specific requirements within this framework. Consequently, the European market is seen as being fragmented and arguably the US is ahead of Europe in creating a coherent framework for security equipment and technologies employed. The following features of the regulatory environment are considered to have greater influence on the competitive position of Europe:

Absence of a centralised body/agency at EU level for transport security

Following the 9/11 events, the US formed the TSA (Transportation Security Administration) as the agency responsible for security of the US transportation systems. The agency oversees security issues for all 450 airports based in the US. Moreover, it controls security initiatives in airports as well as their security budgets. In Europe, a single entity with the same competences does not exist and Member States are relying on their own national authorities (and the respective National Aviation Security Programmes) which impede the homogenisation of practices and procedures at EU level and have a harmful influence on the functioning of the market.

Regulatory framework disparities at EU level

Disparities in legislation across Member States mean that air carriers, airports and freight forwarders are unable to adopt uniform security systems throughout the European market, which has the effect of increasing cost while making economies of scale unfeasible. Thus, companies and other organisations that need to comply with air transport security requirements must adapt to different Member States' legislations if their activities are cross-border and internationally oriented. This implies that, for instance, and in relation to the equipment, airlines may have to purchase and utilise different sets of screening technology and equipment depending on the country they are operating in.

[227] See the CREATIF Network website: http://www.creatif-network.eu/home.html. More information also on Chapter 5.

Lack of certification schemes and standards at EU level

There is no common system of certification at an EU level for security equipment used in the aviation sector, which remains a national responsibility. This results in cases where equipment may be certified in one Member State but may not be certified in another. This can be contrasted with the situation in the USA, where certification is a federal responsibility and where certification normally follows a process linked to *principle → technology → equipment* based on the 'additionally' of new applications and systems. There is also a perception that the approach taken by the Transportation Security Administration is more conducive to the development and eventual adoption/certification of technologies/equipment because the TSA has a more hands-on approach to working with equipment suppliers while certification bodies in Europe are more hands-off in their approach.

The air transport industry and related stakeholders consider that international standards for the screening of passengers, cabin baggage and hold baggage would have the potential to increase security, while also driving down costs down for users. Organisations such as CLECAT or IATA believe that international specifications for screening equipment should also be developed, for instance via the International Civil Aviation Organisation (ICAO) or the International Organisation for Standardisation (ISO).

Today, the lack of common international standards and certification (or, alternatively the multiplicity of standards and certification systems within the EU) are seen as having an unnecessary negative impact on the global outreach of EU security equipment manufacturers. On the one hand, there is not a single European market for security equipment employed in the aviation sector and there are additional costs and procedural delays that result from the need to obtain certification for different Member States (since there is no system for mutual recognition of approvals). On the other hand, in markets outside the US and Europe, US certification – for which procedures seem to largely favour US-based equipment suppliers – is taken as a more relevant demonstration that equipment meets necessary operational standards than national-level EU certification. The absence of common EU certification – or, more broadly, accepted common international standards/certification – place EU equipment providers at a competitive disadvantage.

Competitiveness of EU transit cargo shipments

Competitiveness in the air cargo industry is not only related to technology. There are also policy and regulatory requirements. Depending on the requirements on airlines for physical screening at transfer points, and if EU airports are not able to have cheaper and faster security processes (i.e. adequate capacity), there is a possibility that cargo transiting via the EU may be deviated to other countries. Thus, there is potential for tougher security requirements in the EU and/or delays due to screening capacity constraints to result in displacement of cargo. For example, it is estimated that tougher UK regulatory requirements in the UK result in a 30% reduction in the volume of cargo transport (i.e. cargo was rerouted through other countries with less stringent requirements)[228].

[228] Note: Luxembourg was mentioned as a case where good cargo handling/security facilities have actually strengthened cargo business.

Security choices remain key – airlines using quicker and cheaper technology will increase their competitiveness. However, future legislation could be a constraint, as it may oblige to screen any box/cargo in Europe, making the whole security check longer and more expensive. As a consequence, cargo could be easily deviated to outside Europe (reduction of cost/time).

Stakeholders in the freight-forwarding sector argue that harmonisation of air cargo security throughout EU airports should be addressed by adopting detailed regulations and standards starting at EU level and by facilitating and promoting an equal enforcement of security legislation by all countries to prevent a distortion of competition[229]. In this respect, legislation should put emphasis on two basic concepts in order to increase the competitiveness of EU industry:

- *Supply chain security:* Under such a system, the financial liability of carriers and regulated agents in case of a terrorist action through air cargo should be clarified by the regulatory authorities, at national and European levels. As potential liabilities could largely exceed the financial capability of any commercial company beyond the level which is covered by insurance companies. Some national legislations do not limit the exposure of carriers and regulated agents in case of failure in cargo security checks and this could endanger the survival of (small) forwarding agents.
- *One-stop security:* This concept should facilitate exchanges worldwide, by reducing duplications and secondary requirements. Although cargo departing from third countries might not have been adequately secured, the European Commission could establish agreements with like-minded countries determining that cargo standards in place within the two parties are equivalent[230].

4.6 The global competitiveness position of the EU industry

As described in Section 4.3, the inspection and screening equipment sector has developed primarily in response to specific terrorism acts that – post 9/11 – has generalised into a more acute perception of potential threats. This has been reflected in acquisition activity – driven primarily by investments aimed at securing technological capabilities – that has defined the current structure of the sector, which is dominated by a handful of major players. Further consolidation in the sector is not unforeseeable, though current economic conditions and some lack of clarity in regulatory requirements may place a brake on further industry consolidation.

Given the relative size and growth of the US market and the preference of national administrations for local suppliers, it is unsurprising that many of the major players are US-based companies. However, Smiths Detection retains a strong position in the inspection and screening equipment sector and specifically in the aviation sector, and the European position has been reinforced through Safran's acquisition of a major part of GE Homeland Protection. Rapiscan also retains a strong presence in the UK for baggage and

[229] CLECAT (European Association for forwarding, transport, logistics and customs services) and AEA (Association of European Airlines) consider that while harmonization should provide a baseline of measures, security screening of cargo should be risk-based, i.e. targeted to high-risk shipments. The nature of the risk posed by each shipment should be determined by customs authorities, which are in possession of intelligence and consignment data information. Source: Interviews with CLECAT and AEA representatives.

[230] AEA Cargo Policy Statements: *'Securing cargo while facilitating trade'*.

cargo screening development and manufacturing. Nonetheless, it is evident that for all these players, access to the US market has been a crucial factor in enabling them to occupy their current market position.

Looking below the first-tier of what are essentially global players, the European inspection and screening equipment sector industry appears somewhat fragmented and fragile. There is only one European supplier of security inspection and screening equipment of any notable size (i.e. Gilardoni), beyond which the sector is characterised by companies of relatively limited size. As noted in Section 4.3.2, these companies tend to be focussed on the development of specific technologies and/or offer specialised or niche products to the market. However, they have neither the size nor the capability to compete with the major player, with whom they must often develop partnerships to have access to broader market segments.

One important constraint on the competitiveness of European equipment suppliers – both large and small - concerns the fragmented nature of security regulations, standards and procurement systems in Europe. This lack of harmonisation creates fragmented markets that translate into higher costs and reduced opportunities for achieving economies of scale for equipment suppliers orientated towards European markets. Accordingly, a move towards more harmonised regulations with Europe, which would appear to have the support of vast majority of industry stakeholders (both suppliers and customers), could help to reduce costs and hence raise the competitive profile of the EU security industry. Specifically, greater unification would provide European companies with a larger and more stable 'home' market base vis-à-vis their international competitors, notably from the US.

One specific concern is that the fragmented nature of the European market might have the effect of reducing the overall level of R&D, technology development and innovation. Specifically, market fragmentation implies higher barriers of entry for the adoption of new technologies within the market, potentially reducing the return on investment in development. Consequently, there may be a negative impact on the competitive position of European suppliers as a result of insufficient investment in technological developments and innovation.

The major US and European companies are competing with each other at a global level, although subject to the specific peculiarities and preferences within the main Western and other international markets. In terms of other international competitors, the only significant company in the aviation inspection and screening equipment sector is Chinese (e.g. Nuctech). The growing presence of this 'low-cost' player in the global market presents a challenge to EU and US companies, particularly in a market that may become increasingly cost conscious. Given the limited scope to compete on price, US and European suppliers need to maintain and protect their technological lead – and also reputation and service quality – to remain competitive, especially in the broader international marketplace.

In terms of size and growth, the major markets for inspection and screening equipment are likely to remain in Europe, North America and other 'western' countries. Nonetheless, the very global nature of international transport, and rising security threat perceptions in

other regions, imply potential inspection and screening equipment throughout the world. Given the necessary investment and technological expertise to enter the market it is questionable whether a 'globalisation' of demand will lead to the entry of new players into the market but, as the Chinese experience illustrates, this cannot be completely discounted. For US and European companies, growing demand may become sufficient for them to consider investing in production facilities in other regions of the world. This may be particularly the case if it enables them to take advantage of lower production costs, subject to maintaining the integrity of their control over core production processes.

4.7 Conclusions and potential policy issues

The assessment of the inspection and screening equipment – specifically in relation to the aviation and air cargo sector – raises a number of potential policy issues that may be highlighted:

- **Enhance public-private dialogue**. Industry representatives and stakeholders in the aviation and cargo sectors point to a lack of dialogue, at a European and national level concerning aviation (specifically air cargo) security measures. Here the main issue appears to be achieving greater coherence between policy ambitions (and regulations), technological capabilities to be delivered by the security industry, and operations requirements and constraints of operators and users.
- **Reducing market fragmentation.** A major issue for development of the security inspection and screening equipment sector – and the security industry more generally – in Europe remains the fragmented nature of the market. Although in the case of aviation overarching security regulations are set at the EU-level, implementation of policy is the responsibility of Member States. In terms of setting security equipment requirement and systems for approvals/testing and certification, national differences remain that continue to prevent the creation of a Single Market for security equipment. This could be addressed through:
  - Development of a more harmonised approach to evaluating security technologies and equipment, to provide more consistent implementation policies and standard setting.
  - Development of a European level system for testing, approving and certifying security equipment, either through European level infrastructure and/or greater mutual recognition of national approvals and certification
- **Re-alignment of priorities and approaches for security research support.** A number of issues arise under this heading. First**,** security threat perceptions can change suddenly (e.g. liquid explosives) and require rapid responses that currently cannot be addressed by the (slow) procedures of public funding programs. Secondly, there is scope for greater alignment between research project support and security policy priorities (i.e. greater emphasis should be given to funding projects that support the attainment of security policy ambitions).
- **Improve product liability framework**. The US SAFETY Act provides security equipment suppliers – notably for identification and screening equipment – with the possibility to benefit from a dedicated liability regulation. This can reduce investment risk for the industry and thus stimulate investments within the supply chain, including technology development. Adoption of a similar European initiative – combined with a European certification system (see above) – could help to encourage investments in the sector.

5 Maritime transport of goods (cargo)

5.1 General description of the segment

5.1.1 Segment definition

The segment definition used for this segment is analogous to that used for air transport of goods (see Section 4.1.1) and covers generally the equipment for *detection, identification, tracking and tracing of goods for secure and safe maritime transport*. As the section on air transport security equipment covered already largely some of the main technologies and producers of detection and identification equipment, this sub-category will be left with less attention in this sub-section. Indeed, the main focus of this section is on the **tracking and tracing equipment** used in maritime transportation sector. In more detail, the focus is on vessel tracking equipment, container tracking equipment, container seals and identification equipment, software used for data management / systems integration and to small extend on mobile satellite services. The data management systems and mobile satellite services have been included in the analysis as they form currently one of the most essential parts of the tracking process; the amount of data from tracking devises is increasing rapidly and finding the correct data on the correct moment can be of vital importance, while similarly the tracking is based often on the satellite services.

5.1.2 Product overview

The equipment used for security purposes in the field of maritime transportation covers a wide variety of products. They can be classified according to the two main purposes (though large share of products are used for both purposes/objectives):

- To prevent any threats and attacks that harm the natural flow of goods throughout the global supply chain that might represent economical and/or human losses;
- To avoid the utilisation of the international supply chain as mode of transport of any type of illegal goods, radiological materials, or any other substances or objects that might represent any risk to the world trade community and its member states.

Products used mainly for the first objective have typically more mature markets and use both 'old' and newly developed technologies. By contrast, products used primarily for the second objective have increased rapidly during the last 10 years (especially after 9/11) and a vast number of new technologies are constantly being developed for the needs of the stakeholders. Table 5.1 lists some of the sub-markets under the maritime security equipment segment according to their main objective (defined above) and users.

Table 5.1 List of main security equipment in maritime transportation by their objectives and main users

Product	Objective 1	Objective 2	Main users / customers
Software used for data management / Systems integration / Satellite services	√	√	Defence, Private industries, Terminal operators, Shipping companies, other vessels
Scanning equipment for containers (i.e. explosives and nuclear/radiological screening)		√	Customs, Defence[231]
Vessel tracking equipment			
• **AIS**	√	√	Defence, Shipping companies, to lesser extent Port authorities
• **LRIT**			Shipping companies, Customs, Defence
• VHF radio vessel tracking devices	√	√	
• Radars	√	√	Shipping companies, Customs, Defence
Container tracking equipment			
• **Active and passive RFID systems**	√	√	Shipping companies, other private sector
• GPS	√	√	Shipping companies, Customs, Defence
Container seals and identification equipment			
• **Electronic seals**	√	√	Shipping companies, Customs, Private industry
• Barcodes and Code-reading equipment	√		Shipping companies, Private industry
Cameras			
• Normal cameras	√	√	Terminal operators, Customs, Defence
• Heat cameras		√	Customs, Defence
Keycards / Identification equipment	√	√	Terminal and port operators, Defence, Customs, Private industry

The following analysis concentrates on the products highlighted in bold in the above table, which are the products most closely related to the maritime security and that are in lesser use in other market segments. Many of the other products indicated in the table are in wide use in various other market segments and/or are characterised by rather mature markets.

The following subsections provide short overviews of the main product types under the categories of vessel tracking equipment, container tracking equipment, container seals and identification equipment and software used for data management / systems integration. The container scanning equipment technologies are relatively similar to the other scanning technologies and are discussed further in Chapter 3.

[231] Defence refers here to the various government agencies having the task of protecting the coasts and people, but which vary significantly between different countries. In other words, it refers e.g. to the coast guards, marine defence troops, police, etc.

5.1.3 Overview of vessel and container tracking and tracing technologies

Vessel tracking systems

Historically vessels have been able to move rather freely in the international waters without many possibilities for the interested parties to track where they come from and where they go. Since radars were invented and put into use for observing vessel traffic, many other systems have been developed as well. Especially during the last 10 years, various new systems and technical requirements have been applied to vessels, while radars are still in wide use as well.

According to the 2002 International Ship and Port Facility Security (ISPS) code of the International Maritime Organisation (IMO) all vessels involved in international voyaging with gross tonnage (GT) of 300 or more tons and all passenger ships (regardless of size need) are to be equipped with a satellite tracking equipment (i.e. Ship Security Alert Systems (SSAS)) and a line of site VHF radio vessel tracking devices (i.e. Automatic Identification Systems (AIS)).

Similarly, as of January 1, 2009, according to the International Convention for the Safety of Life at Sea (SOLAS), all passenger ships, high speed craft, mobile offshore drilling units and cargo ships of 300 gross tonnage and upwards regulated by the 160 Contracting Governments of the International Maritime Organization (IMO) must be tracked with a Long-Range Identification and Tracking system (LRIT).

Various other systems are still also used to track larger and smaller vessels (e.g. commercial fishing boats or recreational boats don't have to use AIS systems according to the ISPS regulations) ranging from cameras and radars to partnerships with marine operators who can act as "eyes and ears". Many of these older technologies/methods are still very much needed, since vessels could – deliberately or accidentally - turn off their AIS and LRIT systems. [232]

In addition, it should be noticed that many of the vessel tracking systems are based on mobile satellite services (e.g. LRIT) and for that reason these services providers are an essential part of the market.

- Automatic Identification Systems (AIS)

  AIS equipment transmits information such as the name of the vessel, its position, speed, course, and destination to receivers within range of its broadcast, allowing these vessels to be tracked when they are operating in coastal areas, inland waterways, and ports. It is using the line of site VHF radio technology. Receivers may be installed on other vessels, land stations, or other locations. AIS were created in navigation primarily for collision avoidance. The lack of positive identification of the targets on the displays, and time delays and other limitation of radar and other previously used systems for observing and calculating the action and response of ships around, especially on busy waters, sometimes prevented possible action in time to avoid collision. In addition, AIS is used for tracking vessels in busy waters and harbours in order to manage traffic flows and schedule maritime operations.

[232] GAO (2009), MARITIME SAFETY; Vessel tracking systems provide key information, but the need for duplicate data should be reviewed, Report to the Committee on US Homeland Security, House of Representatives

- Long-range identification and tracking (LRIT) systems

  The LRIT systems are mostly satellite-based equipment developed to transit information on the vessels' identity and position while at sea. The LRIT information from a vessel (vessel identity and position) is picked up by the satellites, retransmitted to the ground stations, and routed to a data centre that serves the country where the vessel is registered. LRIT data centres are the conduits for LRIT information to and from vessels at sea. They can serve individual countries, regional groups of countries, or a broad collection of various countries. For example, the United States will operate its own data centre and LRIT information from U.S. registered vessels will be routed to the U.S. data centres. [233]

  According to the SOLAS regulations, the contracting governments must implement national LRIT Data Centres, to which ships will report their positions four times per day. The global LRIT data centres are also communicating amongst themselves and exchanging position reports upon request. In particular, a ship having notified a port of impending entry (NOA) can be tracked by that particular port thanks to this system. Contracting governments will also be able to track any ship within a 1,000 nautical mile zone of its coastline, no matter what flag it is flying.[234]

Container tracking systems and container seals

Recently new regulations and customer pressure have created need for companies to show where the products that they sell are coming from, i.e. a need for tracing and tracking. The two main systems used for this purpose are Radio Frequency identification (RFID) equipment and satellite based GPS tracking equipment. Even though as such the RFID technology is already relatively old, its usability in the field of container security and tracking is still in development and the technology has still some limitations e.g. with respect to global use and consistency in operations given differing frequencies, power levels, competing footprints, and protocols.

Sealing and monitoring of containers has also benefited from new technologies including among others electronic seals (e-seals) in addition to e.g. barcodes and number identification systems that have been longer in use.

Software for data management, mobile satellite services and system integration

A major question for many stakeholders with respect to the new technologies developed and new regulations requiring more information to be submitted has been: who will analyse all the data provided by the new equipment and requirements? In order to combine the data needs and provisions, various integrated data management platforms/software have been developed. These services in the market seem to be also one of the best performing systems. As there are various different technologies becoming available providing the data on the movements of vessels, containers and their contents, the stakeholders are getting more and more interested in integrated systems that combine the various data sources together in order to track the required information and manage the information and logistics flows.

[233] GAO (2009), MARITIME SAFETY; Vessel tracking systems provide key information, but the need for duplicate data should be reviewed; Report to the Committee on US Homeland Security, House of Representatives.

[234] www.lrit-services.com

Furthermore, especially for the vessel-tracking equipment based on satellite communications (such as LRIT equipment), the cooperation with mobile satellite services producers has been vital in order to guarantee the technical interoperability.

5.2 Market (demand-side) overview

Around 16 million containers are currently flowing in the global supply chain (approximately 25 million TEUs in worldwide circulation). These are used in annual worldwide container traffic of roughly 153 million TEUs in 2008. Terrorist attacks like 9/11 have questioned some of the current security measures to protect the wellbeing of the flow of people and goods in the maritime transport supply chain. Consequently, new security policies and legislations have been adopted in order to increase maritime security measures around the globe. Responding to these measures - and in combination with the massive growth of the container world market - many companies have started to develop new technologies, while continuing to improve existing ones.

5.2.1 Overview of main market (customer) segments

Some of the main customers for security equipment used in the field of maritime transportation have been already listed in Table 5.1. The main customers include governments defence units (e.g. marine defence, coast guards, police, etc. depending of the defence structure in the relevant country), customs authorities, port authorities, terminal operators, shipping companies and private industry. A short description of each of these main user types and their reasons for buying the products is given below.

Governments/Defence units

Governments and their defence units have the main responsibility for securing the safety of the nation against any external threats. Consequently, defence departments have historically been some of the main developers and users of security equipment destined to protect people involved in the maritime supply chain (i.e. security objective 2). They are also one of the main users of vessel tracking equipment.

Customs authorities

Customs authorities are responsible for the inspection of products and persons arriving to the country. Hence, it is estimated that around 95% of current container scanning equipment is destined to Customs services around the world[235]. Similarly, customs use data from container identification equipment and potentially information from electronic seals and container tracking systems will be used in the future.

Port and terminal operators

For port and terminal operators, it is important to guarantee smooth flow of goods, while securing the safety of stakeholders involved. For example, they use cameras and port monitoring equipment for the basic daily security of their operations. In addition, vessel tracking systems and data management software can be attractive for port and terminal operators in order to optimise the flows of goods and vessels in their areas.

[235] Carluer, Frederic (2008). *Global Logistic Chain Security, Economic Impacts of the US 100% Container Scanning Law*. Paris, France: Editions EMS.

Shipping companies

Shipping companies utilise vessel-tracking systems both from operation and regulations point of view. In addition, some of the newly developed technologies for sealing and tracking containers are believed to be of interest to transportation companies for logistics management and tracking purposes.

Private industry

Some of the new regulations have created more demand and need for private companies to track their products (e.g. the e-Pedigree requirements for pharmaceuticals in the USA have created new demand from the pharmaceuticals industry for tracking and tracing their products). Similarly, consumer requirements have increased the need for various industries to track the origins of the products that they sell.

5.2.2 Current approaches to marine transport security

After the terrorist attacks of 9/11, the world and the international trade community realised the necessity to increase their security measures in order to prevent further attacks not only to the passenger sector, but also to the international trade sector. As a result, the term "Supply Chain Security" was employed, making the 'security factor' part of the equation of the supply chain[236]. As noted in Section 5.1.2, supply chain security focuses on two principal objectives:

- The first objective is to prevent any threats and attacks that harm the natural flow of goods throughout the global supply chain that might represent economical and/or human losses.
- The second objective is to avoid the utilisation of the international supply chain as mode of transport of any type of illegal goods, radiological materials, or any other substances or objects that might represent any risk to the world trade community and its member states. In order to reach these objectives the world trade community has participated in several security programs applying security standards and measures within their organizations.

The US Department of Homeland Security conducted a study[237] in order to find out similarities among different supply chains of international cargo flows and to identify nodes to enforce security measures. The analysis revealed 16 similar nodes in every supply chain that could serve as a standard security control for any intermodal flow of goods. The 16 nodes identified in the study by the DHS are described in Table 5.1 and represented in Figure 5.1 (Generalised International Cargo Supply Chain).

[236] *"A supply chain consists of all parties involved, directly or indirectly in fulfilling a customer request, including not only the manufacturer and the supplier, but also transporters, warehouses, retailers, and even customers themselves"*. Source: Chopra, Sunil and Meindl, Peter (2007). *Supply Chain Management, Strategy Planning & Operation*. New Jersey: Pearson Prentice Hall.

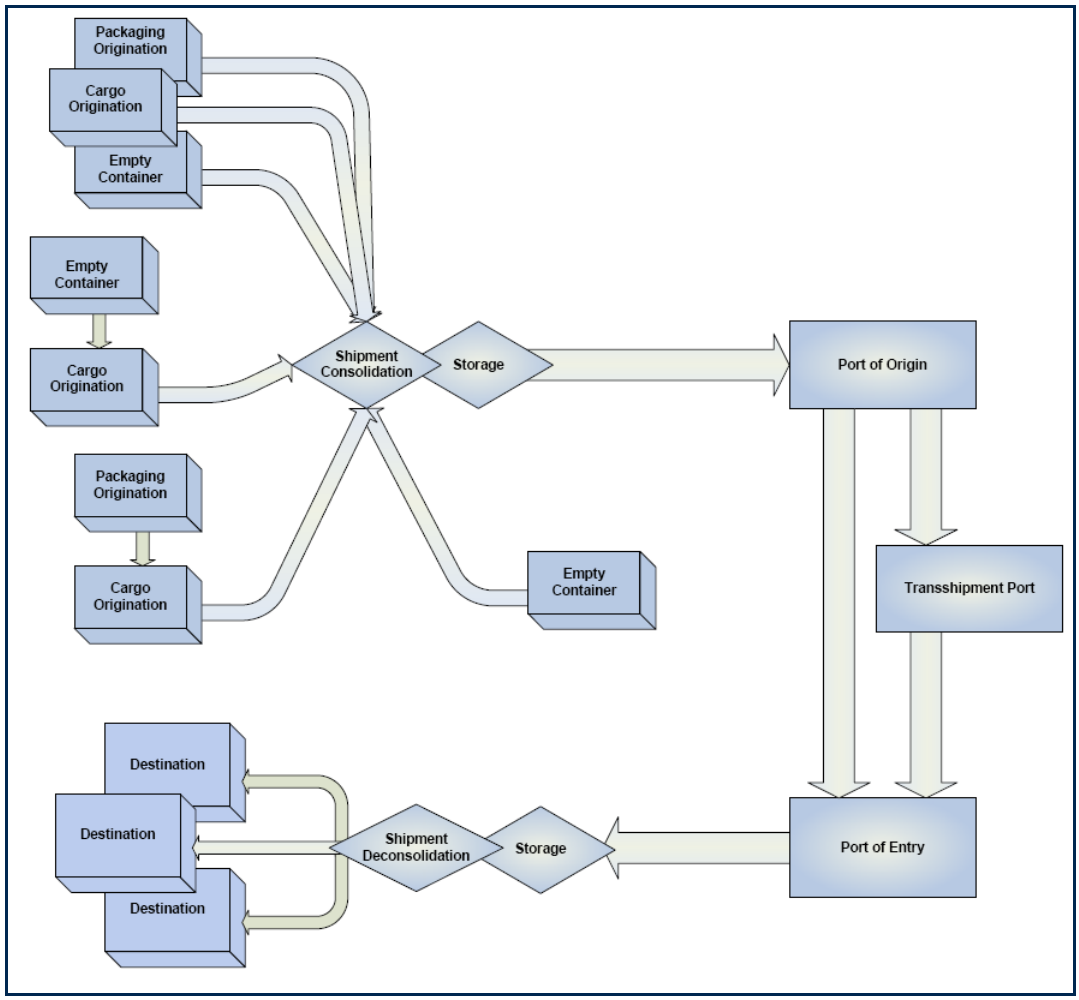
[237] Department of Homeland Security (2007). *Strategy to Enhance International Supply Chain Security*. Obtained on July 30, 2008 from http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf

Table 5.2 Identified nodes for standard security control in intermodal flow of goods

	Node	Description
1	**Origination of cargo**	The goods are produced at the factory or storage by the supplier ready to package.
2	**Origination of packaging**	The packages materials are sent to the factory or supplier to wrap up the final goods.
3	**Origination of container**	In this part of the process the empty container (if is containerized cargo) departs to the factory or retailer to load the final goods.
4	**Mating of cargo and packaging**	The goods are placed inside the package and setting all the final product details until the goods are ready to ship.
5	**Consolidating of cargo/sealing of container**	The final goods are loaded in the container and sealed (if containerized cargo), ready to leave the factory or the retailer warehouse.
6	**Storage awaiting transport**	The container is at the factory or warehouse yard waiting for the transport mode.
7	**Movement of cargo to port of origin**	The transport mode moves the container from the warehouse or factory yard to the terminal (air, sea, rail or land).
8	**Port of origin**	In the terminal the container is stored awaiting for the transport mode (airplane, ship, rail or truck).
9	**International transportation**	The transport mode (airplane, ship, rail or truck) moves the container from the port of origin to the port of entry.
10	**Port of entry**	The container arrives at the port of entry (airport, marine terminal or facility, border port of entry).
11	**Movement to deconsolidation point**	In this part of the process the container is unloaded or split from the transport mode.
12	**Storage waiting for processing**	The container is placed in the terminal yard ready to be processed by the terminal, customs or any other activity to be realized.
13	**Deconsolidation**	After all the release process the container is placed at the terminal yard ready to be moved to the final destination.
14	**Movement to destination**	The transport mode (airplane, ship, rail or truck) takes the container and drops it at the final destination.
15	**Destination**	At the warehouse of destination, the container is received and unloaded by the final consumer, where another supply chain could restart.
16	**Information flow associated with cargo (end to end)**	This part refers to all the information generated by the flow of goods throughout the supply chain.

Source: Department of Homeland Security (2007). *Strategy to Enhance International Supply Chain Security*

Figure 5.1 Generalised International Cargo Supply Chain



Source: Department of Homeland Security (2007). *Strategy to Enhance International Supply Chain Security*

5.2.3 International market profile and market size estimates

The global maritime security market

Similar to the aviation security industry, the Homeland Security Research Corporation (HSRC)[238] has estimated the size of the total maritime security equipment market for the period of 2009 to 2018. Unlike in the rest of this chapter, the market value estimations of HSRC include all maritime safety equipment sub-markets (also the ones that have not been studied in detail in this chapter) including, but not limited to: seaport security control, communication and IT systems, container scanning equipment (nuclear and explosives screening), container tracking systems, vessel tracking systems, swimmer terror threat mitigation systems, cruise ship and ferry passenger screening systems, deepwater security systems, seaport perimeter protection systems, etc. Hence, the coverage of the equipment is significantly larger than what has been studied in detail in this chapter and covers all the some 2.000 larger seaports in the world and all vessels.

[238] Homeland Security Research Corporation (HSRC), *Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018*. Published in 2008.

As Table 5.3 indicates, the value of this total global maritime security market is expected to be some €6.7bn ($9.4bn) in 2009 according to HSRC and the market is forecasted to grow to €11.5bn ($15.7bn) by 2018 with a CAGR of 4.8%.

Table 5.3 Global Maritime Security Market Outlook 2008-2018 (€ billion)

	2008	2009	2010	2012	2014	2016	2018	2008-2018	
								Total	CAGR
Global Maritime Security market	6.7	6.6	7.4	8.3	9.4	10.3	11.5	98.2	4.8%
Maritime Market as % of global Homeland Security Market	14.9 %	12.9 %	13.7 %	13.7 %	13.7 %	13.3 %	13.2 %	N/A	N/A

Source: Homeland Security Research Corporation (HSRC)

According to the 2008 regional breakdown of the total maritime security market estimates, the European Union had the second biggest market share with some 22% of the total market. The EU's share was valued at €1.5bn in 2008 and it is expected to grow to €2.5bn by 2018. The North American region is expected to be the leading player also in the future, although their market share is meant to drop somewhat and, for instance, East Asian countries are expected to increase their market share significantly from 2008 to 2018 as Table 5.4 indicates.

Table 5.4 Global Maritime Security Market: Regional breakdown (€ billion)

	Global market value (€ bn)		Global market share (%)		2008-2018 CAGR
	2008	2018	2008	2018	
North America	2.5	3.6	37.8%	31.0%	2.7%
Latin America	0.3	0.4	4.4%	4.1%	4.1%
European Union	1.5	2.5	21.7%	21.8%	4.8%
Middle East	0.6	1.2	8.2%	9.9.%	6.8%
East Asia (CN+IN)	1.2	2.6	17.7%	22.8%	7.4%
Pacific Region (JP+AU)	0.3	0.6	5.2%	4.9%	4.2%
Other countries	0.3	0.6	5.0%	5.6%	6.0%
Total	**9.9**	**11.6**	**100%**	**100%**	**4.8%**

Source: Homeland Security Research Corporation (HSRC)

Sub-segments specific market estimates

As the market for detailed researched tracking and tracing equipment is characterised by the dual use of the equipment (for security reasons and for optimisation of the logistics flows), the estimations of the sub-segment specific market sizes are difficult. For example, the data management systems are offered for various other markets as well in addition to the maritime transport industry, which complicates the estimations on the size of the market. As the market for container tracking equipment is still very much in development, the market size estimations for that market are extremely difficult.

The only sub-segment within the studied maritime security equipment products of which the size can be estimated at all, is the market for vessel-tracking equipment. According to the Lloyd Register, the world trading fleet was around 50,525 ships at 2008.[239] While fishing boats are not officially obliged to carry AIS or LRIT equipment, many of them have still opted for doing this. The number of fishing boats in the world is estimated at some 23,000 to 25,000, making the total number of potential market for AIS and LRIT equipment to some 75,000 vessels.

The prices of AIS products seem to vary between some €150 to €1,100 per terminal[240]. Assuming an average price of €650 and lifetime of around 3 years for the equipment, **the yearly market size for AIS equipment can be estimated to be between €10 million to €20 million** (depending on the number of potential vessels that will use the equipment).

The current prices of (relatively basic) LRIT equipment are estimated to be between €3,000 to €8,000 per terminal depending on the model (and service packages) according to market studies. The more complex satellite equipment that fulfils the LRIT requirements, can cost significantly more − adding up to around €30,000 per terminal (e.g. Inmarsal Fleet 77 models). Assuming an average life time of around 5 years for the equipment, **the yearly turnover of the basic LRIT equipment market can be estimated to be between €55 million to €80 million.** This does not include the costs of satellite services, testing, maintenance, etc. associated services. It should be also noticed that, for example the market for mobile satellite services (which Inmarsat has been dominating until now) is estimated to be significantly higher in the latest market studies. The demand for the more sophisticated equipment, which can be used also for various other satellite services, is increasing faster than the demand for the basic LRIT equipment. Hence, the actual market of vessel tracking equipment for pure security purposes could be even lower than the above estimations. For comparison, Thrane&Thrane has estimated in their Annual Report 2008 the size of the total satellite communication equipment market at DKK 1,2 billion, which equal around €160 million[241].

5.3 Description of the supply (value) chain

5.3.1 General description and overview

Figure 5.2 provides a simplified picture of the supply chain in the field of security equipment used in maritime transportation. Although there are a variety of products, the structure of supply/value chain is relatively similar and can be separated into the following parts, which are described in further detail in the following sub-sections:

- **Technology development:** technology developments are made mostly by public institutions and large companies with only some innovative SMEs involved due to the high costs (which are often unbearable for most of the SMEs).

[239] http://www.marisec.org/shippingfacts/worldtrade/number-of-ships.php?SID=05ec0f4ee2b62a5bd3b91425b5e9fd3c

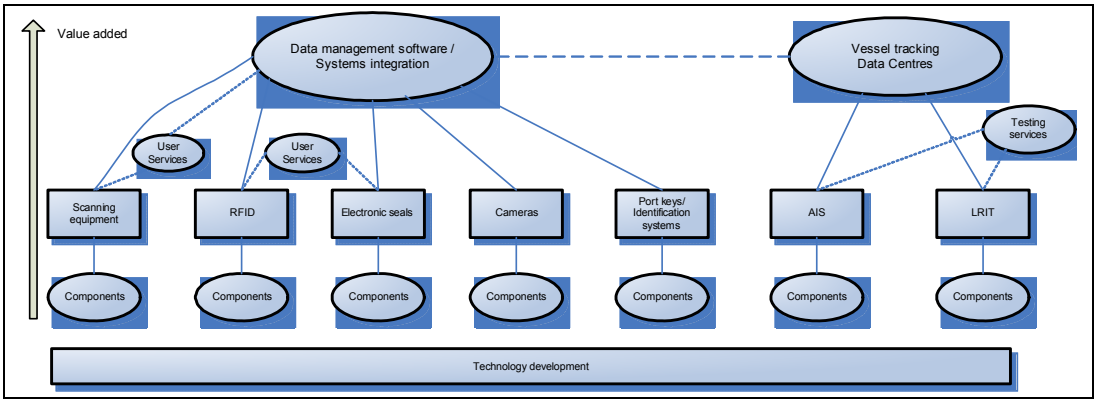
[240] Based on internet search of the AIS equipment prices from suppliers websites.

[241] Exchange rate of EUR/DKK = 0,134 has been assumed. Further, according to the same report, the market share of Thrane&Thrane in this total maritime satellite equipment market was around 46% at 2008.

- **Component supply:** which can be divided to low-cost (and low value added) component production, which is mostly outsourced, and specialised components production, which is done often in-house.
- **Equipment manufacturing:** both lower value added hardware and high value added hardware production involved.
- **User, maintenance and testing services:** including testing services for AIS and LRIT equipment (for certification purposes) and user, maintenance and training services for scanning equipment and vessel tracking systems (often provided by the producers).
- **Systems integration and data management:** management of various data streams in order to provide all the needed data at the right time; this is a major source of value added and is considered one of the most profitable areas of the overall supply/value chain.

Overall, value added is increasingly moving away from 'hard' aspects (i.e. components and equipment) towards 'soft' elements of the supply chain, with data management solutions being at the top. According to some company estimations, in terms of value added or profitability, the software / hardware ratio could be as high as 80% / 20%.

Figure 5.2 Supply chain of the maritime security equipment



5.3.2 Overview of main market players

Due to the extremely varying natures of the equipment used in maritime transportation for security purposes, the main suppliers of the equipment are also categorised by the main product types analysed.

Vessel-tracking equipment manufactures

The introduction of mandatory AIS and LRIT systems for larger scale vessels by the international regulations has significantly increased the production of this equipment during the last years. Especially the AIS market is currently characterised by large numbers of players varying from very large companies to small ones. Similarly, the number of companies producing LRIT equipment has been increasing during recent years rapidly, but the market still has fewer players than the AIS market. Out of the newer technologies in the field of maritime security equipment, the AIS and LRIT have one of the most developed markets.

AIS providers include e.g.:

- Northrop Grumman Space & Mission Systems Corp, USA;
- Kongsberg Maritime – Group Kongsberg, Norway;
- Jotron, Norway;
- Sam electronics, Germany;
- Thrane & Thrane, Denmark;
- CNS Systems, Sweden;
- Maris, Norway;
- Samyung, USA;
- Savic, China;
- Transas, Ireland;
- Comar Systems, UK.

The large number of AIS producers has dropped the company-level market shares and it is difficult to say which companies would be really leading the market. On the other hand, in the relatively more recent market for LRIT equipment, for example the Danish **Thrane&Thrane** has been one of the leading players. Other companies provide LRIT equipment and systems include among other:

- Furuno, Japan;
- JRC, Japan;
- Bluetraker, Slovenia;
- Marinetrack, UK;
- Bureau Veritas, France;
- SkyWave Mobile Communications Inc, Canada;
- Satamatics, UK.

Container tracking and sealing equipment manufactures

As the market for container tracking systems and electronic container sealing (and surveillance) equipment is still a relatively young, developing market, it has few main players and most of them are still developing their products. Many of the developers are relatively large, international companies and involved in various other sectors as well. Some of the main developers/players are listed below:

- **Motorola/IAS:** The Container Visibility System of Motorola/IAS is providing RFID container tags. The readers are land-based requiring access to physical infrastructure and maintenance. Motorola and IAS, based on their technology and industry experience believe that such a system could be fully deployed within a few years.
- **SAVI Networks:** Savi Networks, a joint-venture between Savi (owned by Lockheed Martin) and Hutchinson Whampoa located in the USA. It is building a global RFID-based information network to track and manage containerised cargo shipments. Key product within this global network is the SaviTrack, an RFID based technology. Data are transmitted wirelessly over radio waves to a software platform that can be accessed by shippers and service providers to keep better track of their RFID-tagged containers. It, too, is land-based, providing historical data, and limited like all RFID container system by frequencies and protocols. SaviTrack is already commercially available at the port of Hong Kong and Shenzen, two of the biggest load ports for US imports.

- **The SPC GlobalTrak** (USA) is providing a Container Monitoring Unit (CMU) that contains a suite of on-board sensor and communication hardware. The CMU communicates via cellular or satellite networks based on customer requirements and/or network availability. There is a two-way communication capacity to remotely configure sensor thresholds, transmission interval and mode of communication as well as poll the device for on-demand reporting.
- **European Datacomm** (EDC) is a smaller, European player in global satellite communications, which provides and develops tracking & tracing applications, security and telematics solutions for several sectors such as the automotive, shipping and transport sector. Their headquarters are based on Belgium.

Data management, satellite services and systems integration providers

Similarly to the container-tracking and sealing technologies, the data management and integration systems are still mostly in development and large players dominate the oligopoly.

- IBM, USA;
- Raytheon, USA;
- SAP, USA;
- Microsoft, USA;
- SaviNetworks, USA.

The mobile satellite services (MSS) market was still some years ago mainly dominated by **Inmarsat (UK)**, but lately some other (new) players have emerged as well, including for example:

- Iridium, USA;
- Globalstar, USA;
- Thuraya, United Arab Emirates (UAE);
- Orbcomm, USA.

5.3.3 Technology aspects

Due to the nature of the security equipment and the push of regulations for new technologies, a significant share of the initial technology development is taken forward with government/public funds and many of the technologies used have their roots in the defence industry. For example, the first tags nowadays also used for container-tracking were already developed by KGB after the second WW for surveillance purposes. However, currently many private companies take also part in (often public funded) R&D projects and some of the larger players do also considerable amounts of own R&D. For example, Bureau Veritas and Kongsberg have been involved in the further development of AIS and LRIT technologies for maritime safety purposes within the Marnis project funded by the EC[242]. In general, equipment and technologies used for the second overall security objective (security for stakeholders) is often getting significant funding from the public sector. In addition to the vessel tracking systems, e.g. scanning equipments and e-seals have received public funding in the technology development.

[242] Source: http://www.marnis.org/home.asp

Equipment with wider industrial use tends to attract more private R&D funds. For example, IBM and SAP have been investing in the development of data platforms that could be used for the information needs of private companies (e.g. product tracing via transportation information).

Europe has been traditionally strong in the R&D functions and technology development. However, recently some outsourcing of R&D functions has been taking place and new players have been entering the technology development field. IBM has been among others moving some of the software development centres to India. In addition, Hutchison Whampoa, a major Chinese company in the field of maritime transportation, has been involved in the development of various security technologies used in ports and harbours.

The interoperability of especially LRIT equipment with the satellite services has been also a major issue in the technology development and in practice until now most of the LRIT equipment has been using Inmarsat technologies (where for example Inmarsat C has been a relatively popular terminal type for basic LRIT equipment).

5.3.4 Component supply

For economic reasons many of the vessel-tracking system manufacturing companies have outsourced their components production to lower costs countries or have formed subsidiaries for producing the components in lower cost countries. The separation of the lower value added parts production creates economies of scale, but also provides more possibilities for smaller companies. Indeed, the field of components production seems to have larger share of SMEs than the production of higher value added products in the industry.

Even though the off-shoring and outsourcing of the components supply has increased, core components are still mostly produced in developed countries by the companies own production plants. This is done especially in order to keep the intellectual properties in house and protect the innovations from counterfeiting (of lower cost producers)[243].

5.3.5 Equipment and sub-systems

Some of most important players in the field have been listed in section 4.3.2, by main product types. In general, most of the companies involved in the field are relatively large, with SMEs appearing mainly only in the market for vessel tracking systems. Many of the companies have also a background in the military field or supply for defence departments as well.

While the field of data management software is mainly occupied by American companies, there are many European companies working in the other analysed fields of maritime security equipment.

[243] Smiths Detection (2009). Smiths Detection Webpage. Obtained on May 8th, 2009 from www.smiths.com

The following tables (Table 5.5 onwards) summarise some of the companies with information on their main (relevant) product types, total turnover, employment, activities situated in Europe and location of main manufacturing sites. It shows that operations in the field of maritime security equipment in the EU cover mainly services, sales, and R&D, but also manufacturing.

In addition, many of the large, international companies have offices in the EU countries. (e.g. SAIC, Rapiscan Systems and IBM). In general, most of the operations done inside the EU require relatively high skills and also include some of the more demanding assembly functions.

Table 5.5 Thrane & Thrane: Basic company indicators

THRANE & THRANE (DK)		
Main indicators	**Thrane & Thrane**	
	2007	2008
Turnover	€ 168.2m (satellite maritime equipment: € 61.5m)	€ 165.77m (satellite maritime equipment: € 74.23m)
Profit	€ 2.95m	€ 11.4m
R&D budget	N/A	N/A
Number of employees	761	693
Description of the company		
Thrane & Thrane is the world's leading manufacturer of equipment and systems for global mobile communication based on sophisticated satellite and radio technology. Thrane & Thrane offers communication solutions for four market areas: Maritime, land mobile, aeronautical and systems. Thrane & Thrane's products are based on the satellite system Inmarsat. The existing Inmarsat-3 satellite system consists of four satellites plus one spare satellite. At a height of some 36.000 km above the earth the four satellites provide coverage of 98% of the earth's surface. The satellites have been in service since the end of 1996, and the next generation of satellites - named BGAN - was introduced in the beginning of December 2005. BGAN provides voice and data services at transmisssion speeds of up to 492 kbps, almost 8 times faster than ordinary ISDN. Thrane & Thrane offers terminals to four market areas, of which one is the maritime market. Thrane & Thrane's products for **the maritime market** target professional users and are used, among other purposes, for the GMDSS distress and safety system. The equipment is typically used by merchant vessels, commercial vessels, fishing vessels and pleasure craft for radio and satellite communication. Customers include mainly shipyards and commercial and private ship-owners. According to the annual report 2008 the market share of Thrane&Thrane in the maritime satellite communication equipment was around 46% with most competition coming from two Japanese companies.		
Main products and technologies		
AIS, LRIT, SALOR system,		

Source: Thrane & Thrane website (http://www.thrane.com/About/Press/Press%20Kit.aspx)

Table 5.6 Kongsberg: Basic company indicators

KONGSBERG MARITIME – GROUP KONGSBERG (NO)		
Main indicators	**Kongsberg Maritime**	
	2007	2008
Turnover	€ 606.25m	€ 783.5m
EBITA	€ 70m	€ 84.27m
R&D budget	€ 1.75m	N/A
Number of employees	2,510 (in 25 countries)	3,309 (in 25 countries)
Description of the company		
Kongsberg Maritime delivers systems for dynamic positioning and navigation, marine automation, cargo management and level sensors, maritime training simulators and position reference systems. Important markets include countries with large offshore and shipyard industries. Kongsberg Maritime is a wholly owned subsidiary of KONGSBERG. Market segments: ▪ Merchant marine ▪ Offshore ▪ Subsea ▪ Marine information technology ▪ Simulation ▪ Process automation ▪ Fishery and fishery research - Under the brand name Simrad ▪ Oil & gas - Kongsberg Oil & Gas Technologies Kongsberg Maritime delivers products and systems for dynamic positioning, navigation and automation to merchant vessels and offshore installations, as well as for seabed survey ing, surveillance, training simulators, and for fishing vessels and fisheries research. Important markets include countries with significant offshore and shipyard industries.		
Main products and technologies		
AIS, Autonomous Underwater Vehicles (AUV), camera systems, DP Systems, engine room systems		

Source: Kongsberg Maritime website (www.km.kongsberg.com) and Annual Reports

Table 5.7 Jotron: Basic company indicators

JOTRON (NO)		
Main indicators	**Jotron**	
	2007	2008
Turnover	N/A	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
Jotron AS is a private limited Norwegian company with more than 40 years of continuous operation in international markets allied with a sound financial base. Jotron has been at the forefront when it comes to safety communication products. Jotron has been a major supplier of the specified emergency radio equipment necessary to fulfil the requirements of the Global Maritime Distress & Safety System. In addition Jotron can provide reliable and professional communication products for commercial vessels, fishing vessels and large pleasure crafts as well as high intensity marker and emergency lights for various marine and personal applications as diverse as hiking, diving, fish farms and lifeboats.		
Main products and technologies		
▪ EPIRD ▪ Radar Transponder ▪ AIS Family ▪ S-VDR Float Free Storage Capsule ▪ VHF Radios ▪ Emergency and Marking Lights ▪ EPIRD Test kit		

Source: Jotron website (http://www.jotron.com/Default.asp?Cat=4)

Table 5.8 Sam Electronics: Basic company indicators

SAM ELECTRONICS (DE)		
Main indicators	**SAM Electronics**	
	2007	2008
Turnover	N/A	€ 246.6m
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
SAM electronics is one of the world's leading manufactures and suppliers of maritime electrical and electronic systems. Our prime customers are the international shipping and shipbuilding industries. They are the only company in the world capable of supplying from a single in-house source: ▪ Electrical power packages; ▪ Electrical drive systems; ▪ Automation systems; ▪ Navigation equipment; ▪ Communication equipment; ▪ Maritime services. Products are available in either standalone mode or as part of functionally integrates systems and are designed for operation aboard commercial vessels of all types and sizes.		
Main products and technologies		
AIS, INS NACOS, RADAR, Bridge Alarm System, Navigator Watch Alarm System, VDR/S-VDR,		

Source: SAM Electronics website (http://www.sam-electronics.de/dateien/company/facts.html)

Table 5.9 CNS Systems: Basic company indicators

CNS SYSTEMS (SE)		
Main indicators	**CNS Systems**	
	2007	2008
Turnover	N/A	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
C.N.S. Systems AB (CNS) provides solutions for communication, navigation and surveillance within maritime transportation and aviation based on the AIS and VDL Mode 4 standards. For the crew of a ship at sea, the advantages of a reliable SOLAS compliant AIS system are essential. Robust and flexible base stations and network software solutions are critical components in systems for safety and efficiency in coastal and inland waters, and harbours. With innovative technology and expertise in our customers' areas of operation, CNS provides solutions for increased safety and efficiency wherever the need exists. The ship borne AIS Class A systems, based on state of the art technology, gives SOLAS compliance at a very attractive price. Installed on a large number of vessels worldwide, they not only ensure reliable operations, but also provide the users with the features necessary to utilise the full advantages of the AIS technology.		
Main products and technologies		
AIS		

Source: CNS Systems website (www.cns.se)

Table 5.10 Maris: Basic company indicators

MARIS – THE GRIEG GROUP (NO)		
Main indicators	**Maris**	
	2007	2008
Turnover	N/A	€ 7.8m
EBITDA (loss)	(€ 0.47m)	€ 0.3m
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
MARIS is a private limited company with head office in Tonsberg, Norway a recognised centre for maritime information technology. The majority owner is the Grieg group: ship owning, ship broking, fish farming and processing, insurance broking and asset management. More than 1,500 navigation systems have been delivered to customers in more than 30 countries. The company was founded in 1997 by a group of engineers who perceived a business opportunity in commercializing electronic chart systems as a replacement for the traditional paper charts in the merchant fleet and in the navy. In addition, the founders had a high degree of radar competence. Grieg Shipping Group became a shareholder in 1999 and has since 2001 been active in developing the company to what it is today.		
Main products and technologies		
Products: ▪ Onboard systems ▪ Fleet management ▪ Maritime security systems ▪ Electronic charts		

Source: Maris website (www.cns.se) and Grieg Group website (www.grieg.no)

Table 5.11 Transas: Basic company indicators

TRANSAS (IE)		
Main indicators	**Transas**	
	2007	2008
Turnover	N/A	> €135m
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	> 1,500
Description of the company		
Transas is a world-leading developer and supplier of a wide range of software, integrated solutions and hardware technologies for the aviation and marine transportation industry, including both onboard and shore-based applications.		
Main products and technologies		
AIS, LRIT, Onboard systems, Simulation system		

Source: Transas website (www.transas.com)

Table 5.12 Comar Systems: Basic company indicators

COMAR SYSTEMS (UK)		
Main indicators	**Comar Systems**	
	2007	2008
Turnover	N/A	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
Formed over 25 years ago, Comar manufactures a range of marine Automatic Identification System (AIS) products specifically for the Light Commercial and Leisure markets. Pioneering the AIS market, in 2004 Comar launched one of the world's first "receive only" AIS units, the SLR 200. With the aim of providing mariners additional information about the status of vessel traffic within VHF range, the unit has been chosen by many navies, harbour authorities, monitoring stations, workboat companies, diving companies fishermen and yachtsmen all over the world. In November 2006, Comar launched the CSB 200 Class B AIS Transponder. Specified by the IMO as a non mandatory requirement suitable for vessels under 300 GT's, the CSB 200 receives and transmits AIS information ensuring that not only can the user "see" other vessels, they can also be "seen". Comar is completely committed to the AIS market and maintains a policy of continuous development and improvement. The range and variety of AIS products was expanded again in 2007, enabling Comar to become a world leader in this sector. You can expect to see new innovations every year as the market develops.		
Main products and technologies		
AIS		

Source: Comar Systems website (www.comarsystems.com)

Table 5.13 Bureau Veritas: Basic company indicators

BUREAU VERITAS (FR)				
Main indicators	**Bureau Veritas (Group)**		**Marine Division**	
	2007	2008	2007	2008
Turnover	€ 2,066.9m	€ 2,549.4m	€ 247.2m	€ 293.5m
Profit	€193.2m	€ 231.4m	€ 70.1	€ 87.5
R&D budget	N/A	N/A	N/A	N/A
Number of employees	8,395	8,536	N/A	N/A

Description of the company

Bureau Veritas delivers to its clients customised services helping them to create added economic value through risk management and performance optimisation. Its marine Division contributes to improving and maintaining safety and quality standards in the maritime industry in accordance with its general conditions. It offers a broad range of services :

- Classification of ships and offshore units;
- Statutory Certification of ships and offshore units, quality (ISM) and security (ISPS) systems certification, and certification of marine equipment and materials;
- Additional Services to classification and certification, that can be delivered for any ship;
- Training solutions dedicated to ship-owners technical staff and to ship officers.

The Marine business has four central departments:

- The technical department, responsible for relations with international organizations (such as flag administrations and IMO); the drafting of the Group's classification rules; internal quality control and supervisory tasks;
- The department responsible for the ships-in-service activities;
- The department responsible for consulting and outsourcing activities; and
- The commercial department, which coordinates the network efforts to serve the major ship owners and shipyards.

Main products and technologies

LRTI

Source: Bureau Veritas website (www.bureauveritas.com) and Bureau Veritas FY 2008 Results

Table 5.14 Satamatics: Basic company indicators

SATAMATICS (UK)		
Main indicators	**Satamatics**	
	2007	2008
Turnover	> €15m	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	N/A
Description of the company		
Satamatics is a global telematics company providing customised tracking and monitoring solutions that are used throughout the world. Our offerings enable land transport, security, maritime, and oil and gas organisations to locate, track and communicate with mobile assets, safeguard fleets, cargo and personnel, and to monitor fixed assets in the most hostile or remote terrains in the world. The maritime sector, providing: • Position reporting for fishing and commercial fleets as well as catch monitoring for fishing fleets; • Asset tracking; • Supply chain management. Satamatics products and services can provide complete end-to-end solution to solve all your maritime asset tracking, tracing, micro-telemetry and security requirements, enabling owners and operators to: • Trace, track, monitor and communicate with all types of seagoing vessels • Secure maritime assets and client cargo and safeguarding crews.		
Main products and technologies		
LRTI		

Source: Satamatics website (www.satamatics.com)

Table 5.15 Bluetraker: Basic company indicators

BLUETRAKER (EMA Group)		
Main indicators	**Bluetraker**	
	2007	2008
Turnover	N/A	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	50
Description of the company		
EMA Group consists of three companies in three countries (Slovenia, Hungary and Croatia) with 50 employees. During the last 17 years EMA Group becomes the leading marking, coding and traceability specialist in Eastern Europe. In 2004 a new division was created to develop our Telematics and Machine to Machine (M2M) communication systems. This led to a new range of solutions for intelligent transport systems and mobile communications. EMA develops solutions for end users, service providers, product providers and system integrators. The BlueTraker® range offers global tracking, monitoring and surveillance of vessels at low investment and for modest air-time cost.		
Main products and technologies		
LRIT, Vessel Monitoring System, Fleet Management		

Source: Bluetraker website (www.bluetraker.com)

Table 5.16 European Datacomm (EDC): Basic company indicators

EUROPEAN DATACOMM (EDC) (BE)		
Main indicators	**European Datacomm**	
	2007	2008
Turnover	N/A	N/A
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	50
Description of the company		
EUROPEAN DATACOMM (EDC), a major player in global satellite communications since 20 years, today provides and develops vehicle tracking & tracing applications, security and telematics solutions for the automotive sector and also acts as a service provider for satellite-based voice- and data communications for defense, shipping, monitoring of fixed and moving assets, data collection a.s.o. . By providing mobile connectivity and information wherever and whenever it is needed, our aim is to reduce your costs, improve your security and performance, and provide more efficient ways of working. EDC delivers services worldwide to private customers as well as governmental institutions.		
Main products and technologies		
Container tracking equipment, Iridium, viasat		

Source: European Datacomm website (www.europeandatacomm.be)

Table 5.17 Inmarsat: Basic company indicators

INMARSAT (UK)		
Main indicators	**Inmarsat (Group Limited)**	
	2007	2008
Turnover	€ 406.7m	€ 431.8m
Profit	€ 72.2m	€ 260.14m
R&D budget	N/A	N/A
Number of employees	454	466
Description of the company		
Inmarsat has stood at the forefront of mobile satellite services for 30 years. They are internationally recognised as pioneers in our field and we continue to introduce new technologies that redefine the standard for the industry. Founded in 1979 to ensure that ships could stay in constant touch by telephone, Inmarsat is the world's leading provider of global mobile satellite communications. The company provides voice and high-speed data services to almost anywhere on the planet - on land, at sea and in the air.		
Main products and technologies		
Mobile Satellite Services and VSAT: BGAN, R-BGAN, IsatPhone, LandPhone, FleetBroadband, Fleet 77 & 55, Fleet 33, FleetPhone, Inmarsat C and SwiftBroadband		

Source: Inmarsat website (www.inmarsat.com)

5.3.6 Integration and customisation

The level of integration and customisation needed depends on the specific equipment in reference, but most of the discussed maritime security equipment has relatively low levels of customisation as such. For example, most of the AIS and LRIT equipment have very low customisation levels, while some of the more service oriented products (like the data management services) can have already significant customisation requirements.

On the other hand, the level of integration and needed technological interoperability is relatively high in the industry. The vessel tracking equipment producers have to cooperate with the satellite services producers in order to guarantee the interoperability with their services.

5.3.7 Related services

Data management services

As a result of recent technological developments in the field, the security needs of the various stakeholders can be filled relatively easily with the existing technologies. In fact, significant amounts of data are available that can be used for the various security needs of customs, shipping companies, private industry, etc. This has created more and more need for integrated data maintenance services. For example, with regard to the new scanning equipment, a large question has been raised on who should analyse the data/information provided by the equipment. The provision of scanning images is in itself not enough for the security needs, but they should be analysed in order to find the suspicious transfers. Similarly, the various LRIT and container-tracking technologies can provide large quantity of information on the movements of cargo and containers. However without a reliable analytical tool, data from single source could lose significance or finding the correct information might be challenging. Hence, many of the larger ICT developers have started the development of integrated data management platforms and software. These services can be used for the needs of the pharmaceutical companies in tracing the products (see section 5.5 for further details on the new tracing requirements for pharmaceutical products).

As listed in section 5.3.2, companies such as IBM, Raytheon, SAP and Microsoft have started the development of database software for managing the information flows in maritime transportation. However, the market is still relatively young and many of the systems are still in development (or in testing/pilot stages). Most of the solutions are based on the data provision from GPS and RFID technologies[244].

In addition, various support services are provided especially by the equipment manufacturers for maintenance and training. Similarly, next to the suppliers of AIS and LRIT equipment a wide range of service providers have appeared to provide among others data centre and testing services[245].

Compared to the maritime security hardware provisions, the related services production is considered more profitable and the market is expected to expand rapidly.

Mobile Satellite Services

Mobile satellite services have a strong link with the vessel-tracking equipment producers by providing the link to the actual satellite tracking. Inmarsat, situated in the UK, has been for a long time the main provider of these services, while during the last years especially Iridium has provided some competition for them. For a long time the Inmarsat C was in practice the main provider of LRIT data services, but lately also some lower cost

[244] Source: http://www-03.ibm.com/solutions/sensors/us/list/solution/distribution/index.html
[245] Source: http://www.lrit-services.com/html/regulations_en.html

providers have fulfilled the IMO requirements. However, most of the vessel-tracking equipment producers have, for historic reasons, a lot of Inmarsat (C) equipments on offer.

5.3.8 Linkages to final markets

The structure of the distribution channels and intermediaries differs between the different product types. While many AIS producers use various distribution channels and intermediaries, many of the other types of security equipment studied are sold nearly exclusively by the producers own internal sales departments and offices. The choice for the appropriate distribution channels mostly depends on the complexity of the product and the need for customisation.

5.3.9 Overall assessment of the supply chain

As Figure 5.2 shows, the value added in the maritime security equipment supply chain seems to be the highest in the level of support services provided, while most components have lower value added (though few exceptions exist).

The European producers/offices of multinationals have mostly specialised in the relatively high value-added products and technology development. Both vertical and horizontal networking and cooperation takes place in the field. The field of technology development is characterised by the most intensive cooperation: the public sector, equipment producers and the final users cooperate together in the development of new technologies needed. Cooperation between equipment manufacturers and data management services exists to a lesser extent, and cooperation seems to be lowest between some component manufacturers with lower value added and the equipment producers. Vertical networking has, for example, occurred in the field of container tracking devices development, where Motorola and IAS have been planning to develop together some new equipment and earlier a joint venture company (by GE Security, Mitsubishi Corporation, Samsung Corporation, and Siemens Building Technologies) called CommerceGuard was active also in the development of container tags (according to the company website their operations are currently suspended).

5.4 Main trends and developments

5.4.1 Market trends and developments

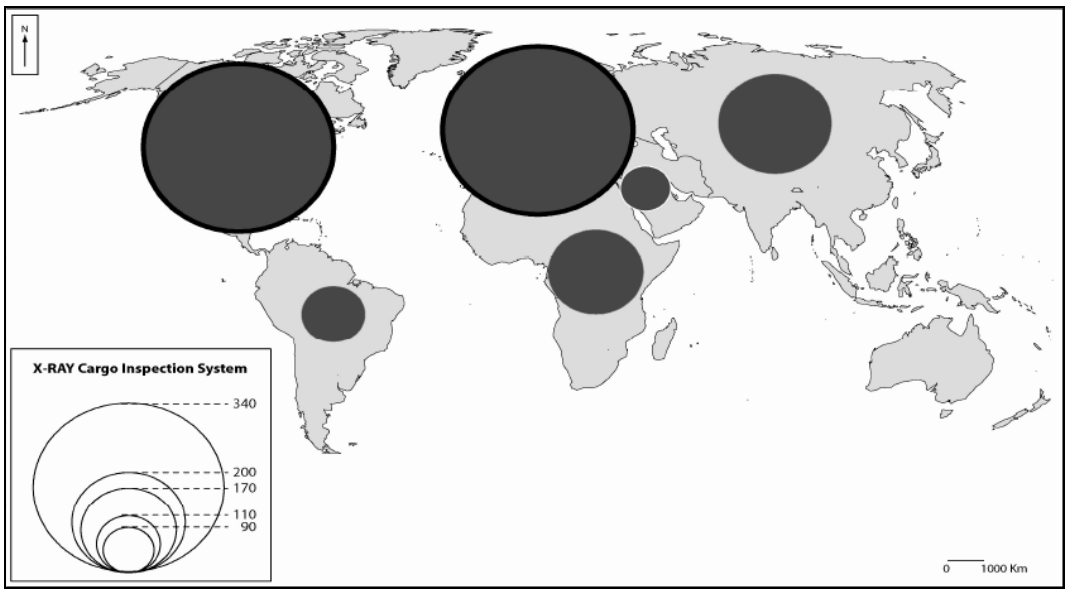
The maritime security equipment industry is driven by few core factors:

1) New (security) regulations and potential of new regulations;
2) Security threats and liabilities of stakeholders;
3) Demand from shipping companies and private customers on more transparency in the flow of goods (i.e. demand for tracing); and
4) Need for further optimisation of operations and securing the flow of goods.

Especially since the September 11th attacks, the large number of new security-related regulations have generated new demand for security equipment. For example, the new IMO regulations concerning need of AIS and LRIT equipment on certain vessels have driven demand for these equipment types (although they were already in use before that

to a smaller extent). Figure 5.3 provides an overview of the quantity of container scanners in use in the world. Even though a complete container scanning of US boundaries has not come in to force, it provides an example of the impacts of planned legislation.

Figure 5.3 Number of operational Scanners in the world by continent at the end of 2007: total 1,250



Source: Carluer, Frederic (2008). *Global Logistic Chain Security, Economic Impacts of the US 100% Container Scanning Law*. Paris, France: Editions EMS.

Secondly, the demand for these types of products is driven by the foreseen security threats and the liabilities of stakeholders. For example, shipping companies and terminal operators responsible for the safety and security of cargo require security equipment to meet their obligations. For example, scanning equipment could become more popular among terminal operators even if 100% container scanning regulations are not implemented, as there is a need for terminal operators to secure the flow of goods. Similarly, major events like the Football World Cup in South Africa in 2010 and the Olympic Games in 2012, are also drivers for the security equipment market.

The liabilities of stakeholders create need for the security equipment to be efficient and reliable. However, with regards to costs there is often a trade-off between buying security services (or service systems with other equipment) against buying security equipment, where the costs often determine the final option. Further, easy integration of all the security systems (e.g. databases and communication equipment) is a major consideration for the clients.

New regulations, such as the e-Pedigree in the USA, and consumer requirements have also created more demand for tracking and tracing of goods. Hence, companies express further need to collect information on the exact sources and movements of their products, which have also been driving the demand for container and vessel tracking devices and for database services (which combine the data from various information sources according to the needs of the customer).

Security equipment, such as the vessel and container tracking systems, can also be used for the optimisation and safety of the flow of goods. For example, AIS systems can be used by port authorities for assisting the management of operations. Similarly, the majority of cameras and security equipment on buildings are used for both security objectives in ports and harbours: securing the flow of goods and securing the safety of stakeholders involved in the system. It should be noticed that when security equipment are primarily used for the optimisation of flows of goods, price can be a larger factor than usually (other equipment together with security service companies might be used if they are cheaper). In this case, the security equipment in Europe can often be cheaper despite the relatively high labour costs and service costs. In addition, the interconnectivity/ flexibility of the equipment to other equipments and systems is found to be an important competitiveness factor.

5.4.2 Technology trends and developments

As explained before, technological developments are often totally or partially publicly funded and spill-over effects from the defence industry are common. For example, GPS technologies, which were originally developed for the need of the US defence and aeronautics industries, have also found a strong position in the field of maritime security.

During the last ten years the technological developments in this field have made good progress with the introduction of new tracking and scanning technologies described earlier. However, many of the older technologies have still not been totally replaced by the new ones, and they co-exist (e.g. radars and GSP systems are currently both in use). Hence, especially technological integration and cooperation has been a major issue in the field and requires still some additional research.

Intellectual property rights and patents play a relatively large role in this field, which explains the interest of companies to be involved in the development of new technologies as early as possible. The company with the patent for the new technology is entitled an advantage over the latecomers. However, wider use in the market takes some time due to the often high costs of new technology. For example, the e-seals and container tracking devices have not yet become extremely popular due to their still relatively high costs compared to older tracking systems. In addition, the new equipments related service costs are compared to the current systems. Similarly, the analysis of the data provided by the scanning equipment will take considerable time or possibly require support from other systems, which leads to a rise in the total costs of the new technology.

5.4.3 Production trends and developments

The production trends have largely followed global trends with increasing importance of horizontal and vertical networks and growing number of offshoring and outsourcing taking place.

The level of economies of scale is mostly dependant on the maturity of the technology and the level of demand; for example, the fields of tracing and sealing have little potential for economies of scale. However, the introduction of more stringent scanning requirements would lead to higher demand and more potential for economies of scale.

High production volumes allow manufacturers greater opportunities to negotiate lower costs of the components in order to produce their products and represent greater lean manufacturing opportunities across their product lines. Hence, the industry is especially sensitive to new regulations since they have make or break the potential demand for the new products and technologies.

5.4.4 Overall assessment of trends and developments

The maritime security equipment industry is especially driven by new regulations and standards, which create potential for new technological developments (as R&D needs also often receive support from the public sector). The new, tighter security regulations in the maritime transport sector have indeed also resulted in various new technologies being developed during the last 10 years.

5.5 Regulatory conditions and development

5.5.1 International, European and national security-related regulatory conditions

The maritime security equipment industry has been largely affected by the recent regulations, which have created significant additional demand for (new) security equipment. Some of the most important international, US and EU regulatory developments that have affected the sector have been listed below.

International Ship and Port Facility Security Code (ISPS Code)

The ISPS Code was created by the International Maritime Organization (IMO) as a response and solidarity to the US after the terrorist attacks on September 11th 2001, including a mandatory (Part A) and a guidance/non-mandatory (Part B) section of security standards for port facilities and vessels. In general terms, the Code establishes a standard and consistent framework for evaluating risk, enabling governments to react in threatening situations that involve risk for their facilities or vessels. The regulation sets minimum requirements for security standards of vessel and facility emergency plans, physical security, security audits, personnel responsibilities, training and emergency exercises. Many countries comply with the ISPS Code and establish good levels of security measures from the moment the vessel is being loaded in a foreign port, across international waters, until the cargo is unloaded at the destination port. However, the implementation and adoption of new standards still remains of national competence, but as most of them have implemented the new guidelines the demand for AIS and LRIT products has increased rapidly[246].

Container Security Initiative (CSI)

The US Customs and Border Protection (CBP) created the Container Security Initiative (CSI) programme. The objective of the programme is to guarantee that all containers representing a potential risk of terrorism should be identified and detected at foreign ports before arriving in the US. This programme set up together with foreign ports that voluntarily accept to work jointly with multidisciplinary teams of the CBP and Immigration Customs Enforcement (ICE) offices. Their mission is to target and pre-

[246] Source: www.imo.org

screen containers for investigative analysis of destined cargos that might represent a possible threat to the United States. The core elements of CSI are: identifying high risk containers, pre-screening of high risk containers before shipping, and utilisation of technology to ensure that screening can be done rapidly without slowing down the trade flows (CBP, 2008). Through CSI, foreign Customs officers work together with CBP officers determining security standards, infringing upon their national sovereignty, in order to identify high-risk containers with the aid of non-intrusive inspection (NII) and radiation detection. Reciprocally, foreign officials are invited in US ports to cooperate in the identification of target containers that are destined to their countries and might represent a threat to their nations. Currently there are 58 foreign ports participating in the CSI program, representing around 85% of the container traffic bound for the United States[247].

International Port Security Program (IPS)

Created by the US Coast Guard (USCG), the International Port Security Programme was developed to protect the global shipping industry by the facilitation of security improvements in ports around the world. With the help of host nations, the Coast Guard will work together to evaluate countries' overall compliance with the International Ship and Port Facility Security Code (ISPS). The Coast Guard utilises the information collected during visits to improve security practices and to determine if additional precautions should be taken for vessels arriving to the United Stats from other countries. Vessels that arrive at US ports from countries that are not participating in the IPS programme and from countries that are not in compliance with the requirements of the international code, can be denied entry[248].

WCO SAFE Framework of Standards

The World Customs Organization (WCO) has developed a strategy called SAFE Framework of standards to secure the flow of goods through the supply chain in order not to disrupt the flow of operations and to facilitate trade among countries. The SAFE framework establishes four principles as a minimal threshold of what must be done to ensure security. First, it harmonizes the advance electronic cargo information requirements on inbound, outbound and transhipments. Second, each country that joins the SAFE Framework commits itself to employ a consistent risk management approach to address security threats. Third, it requires that at reasonable request of the receiving nation and based upon a comparable risk targeting methodology, the sending nation's customs administration will perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment (NII) such as large-scale X-ray machines and radiation detectors. Fourth, the SAFE Framework defines benefits that Customs will provide to businesses that meet minimal supply chain security standards and best practices[249]. The SAFE Framework also shows the importance of joint efforts from Customs to Customs and Customs to Business partnerships in order to benefit security levels and the trade community alike.

[247] Source: US Customs and Border Protection (www.cbp.gov)
[248] Source: US Coast Guard (www.uscg.mil)
[249] Source: World Customs Organisation (www.wcoomd.org/home.htm)

Potential US 100% container scanning legislation

After the U.S. government enacted the H.R.1 Law or so-called 100% Container Scanning Legislation the scanning market increased considerably due to the fact that each foreign port is expected to scan their U.S.-bound container prior to arrival in the U.S. Even though many foreign governments and the international trade community are expecting President Barack Obama to decline its implementation in 2012, the truth is that no official announcement has rejected this controversial law so far. If the H.R.1 is implemented in 2012 as planned, more than 600 ports around the world and around 160 Customs agencies would demand scanning equipment and services.

EU regulations

After 2001, similar regulations have been passed in the EU, of which many are based on the international ISPS regulations. These include, for example: Regulation (EC) No 725/2004 on enhancing ship and port facility security and Directive 2005/65/EC on enhancing port security. Similarly, the EU amended the Community Customs Code in 2005 (with Regulation 648/2005 and its implementing provisions in 2006 –Regulation 1875/2006) to respond better to the new security threats and comply with the EU's commitment to implement the standards foreseen on the World Customs Organisations SAFE Framework. The new legislation provides also the framework for the EU Customs Security Programme. The CSP covers the following aspects:

- All traders must provide the custom authorities with information for security risk analysis on goods prior to arrival or departure from the Community customs territory, using the pre-arrival/pre-departure declarations. The regulations were foreseen to apply as of 1/7/2009; however, compulsory obligation for trade has been postponed to 1/1/2011. During this transitional period voluntary submission of the pre-arrival/pre-departure security declarations is possible until the 31 December 2010 inclusive.
- Reliable traders involved in the already implemented Authorised Economic Operator (AEO) programme, which is compatible with the US C-TPAT programme, will be able to benefit from trade facilitation measures once a Mutual Recognition agreement/arrangement has been put in place.
- Introduction of mechanisms for setting uniform Community risk-selection criteria for Controls supported by computerised systems are currently underway.[250]

Most of the EU Customs Code does not directly affect the demand or supply of vessel tracking systems, but does create more demand for container scanning equipment and data management services.

Other regulations

Other regulations affecting the demand for security equipment include e.g. the new Californian regulations concerning the traceability of pharmaceuticals products, the laws concerning e-Pedigree under the 2004 Californian legislation on anti-counterfeiting and anti-diversion (SB 1307). The law was passed in an attempt to prevent counterfeit medicine from entering the legitimate supply chain in California. Under the legislation, as of 1/1/2009, no wholesaler or pharmacy may sell, trade or transfer a prescription drug at wholesale without providing, and no wholesaler or pharmacy may acquire any

[250] http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/security_initiatives/index_en.htm

prescription drug without receiving a pedigree. The pedigree is a record in electronic form containing information regarding each transaction resulting in a change of ownership of the given prescription drug, including returns.[251] This has directly increased the need for tracing provisions for the pharmaceutical products and IBM has for example created data management software for these tracing needs.

5.5.2 Industry and market-based standards

The industry has also various standards that affect the producers and add requirements to meet.

ISO standards

Various ISO standards are used for the quality certification of maritime safety equipment. For example, already at least ISO standards 18185 and 10189 concern the electronic container seals and tags. Even though the ISO standards are not mandatory, they provide a significant reliability indicator for potential buyers.

IMO standards and certificates

Similarly, the International Maritime Organisation provides certification for products that fulfil their requirements and are authorised. For example, IMO has specific certificates for AIS and LRIT equipment and a large number of maritime security service companies provide the required testing services for the certification.

US Safety Act certifications

The US SAFETY Act from 2002 by the US Department of Homeland Security (DHS) provides legal liability protections for providers of Qualified Anti-Terrorism Technologies – whether they are products or services. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability limitations for ‘‘claims arising out of, relating to, or resulting from an act of terrorism’’ where Qualified Anti- Terrorism Technologies have been deployed. The Act affects hence security technology manufacturers directly by cutting the potential liabilities. It is possible for European companies to obtain US certification provided that they can demonstrate the utility and effectiveness of the technology.

Other standards and certificates

In addition to the IMO certificated, the LRIT equipment needs to be tested and certified by an Authorised Testing ASP appointed by the vessel Flag (state). The Authorised Testing ASPs will, on behalf of the Flags, issue LRIT Conformance Test Reports (certificates) for terminals that pass the test. Further, Type Approval certificates for LRIT equipment are issued for example by Lloyds Register, Germanischer Lloyd (GL), Det Norske veritas (DNV), American Bureau of Shipping (ABS), Chinese Classification Society (CCS), Russian Maritime Administration (RMA), and US Coast Guard.

[251] Source: http://www.pharmacy.ca.gov/laws_regs/e_pedigree_laws_summary.pdf

5.5.3 Overall assessment of regulatory conditions

The recent and rapid increase of regulations has been both beneficial and threatening to the industry. While many new regulations (such as the IMO rules on AIS and LRIT) have been creating more market opportunities for the security equipment producers, the various regulations and standards also create additional quality demands to meet as well as challenges. Similarly, the future of new legislation (such as the potential 100% scanning legislation in the US) can either create a new market (for scanning equipment) or undermine the costly development of new equipment and market opportunities.

On balance, new regulations have mostly helped to create new market opportunities and bigger demand for the maritime security equipment producers. With regard to new legislation, the consultation of the industry should be important during the legislation making process and the large effects on the industry should be noticed. In addition, similar types of legislations in different countries (EU, US) with small differences can create large additional costs to the producers and international legislation should be preferred if possible.

5.6 The global competitiveness position of the EU industry

Thanks to the early and intensive involvement of European and multinational companies with European-based facilities engaged in the technology development, the competitive position of European producers in the global market remains relatively strong. This is especially true for the supply of new integrated systems (both hardware and software solutions) characterised by relatively strong demand and value added opportunities for the producers (e.g. LRIT equipment). However, most of the data management systems and new container-tracking devices are being developed by large multinationals with headquarters in the USA.

Some threats for the European industry are visible. Low costs countries (such as China) create threats as an increasing share of (lower value added) production is moving towards these countries. As technologies mature, more and more production can be outsourced/offshored. Although possibilities for cost-cutting strategies can be overall beneficial for European companies (helping them to survive in this toughening competition), they may have negative employment effects in the EU. In addition to manufacturing, there is also evidence that some R&D functions are being offshored (e.g. software development to India). However, despite these threats, a relatively large share of the maritime security equipment production seems to remain in the EU.

The long, strong initial position of Inmarsat in the mobile satellite services production and the early development of LRIT equipment in Europe has allowed some of the European companies (such as Thrane&Thrane) to lead the market in LRIT products manufacturing. According to the own estimation of Thrane&Thrane, their market share in the total maritime satellite equipment market would be around 46%. While there are increasingly also companies from the USA providing mobile satellite services (e.g. Iridium), most the LRIT equipment consistent with their systems are still also produced by European companies. The main competition arises from Japanese companies, while also some American companies have tried an access to the market.

The competition situation in the AIS equipment market is quite different and as an already relatively mature market, a lot of producers from lower cost countries are evolving next to the European and American companies. However, considering their relatively low market size, this is not likely to affect the overall European production and economies much. Untill now it has been mostly American and European companies leading the market.

5.7 Conclusions and potential policy issues

Based on the market structure, framework conditions and competitiveness analyses, the maritime security equipment sector is relatively strongly affected by (new) regulations and the development of new solutions can bear significant costs. Hence, especially the following issues raise potential for policy implication and considerations:

- **Importance of cooperation with industry stakeholders with regard to new regulations in planning**: Especially the security related regulations made after 9/11 have had a large effect on the industry and pose both market opportunities and challenges to the maritime security equipment industry. For example, the IMO requirements for the use of AIS and LRIT equipment have significantly increased the demand for these products and hence provided also some market opportunities.
- **International cooperation in (new) standards development**: The interoperability of the technologies used is relatively important in the sector and hence (continuing) international cooperation in the development of the (new) industry standards would benefit the whole industry.
- **Public support for development of new technologies often needed, but can provide significant support to involved companies**: The R&D costs in the sector are typically relatively high and the development of new technologies risky and time consuming. Hence, it should be noticed that public support especially to the development of new technologies can be extremely beneficial and needed in the sector in order to correct some of the market failures, but it can also provide direct market advantages to any private companies involved in the (public) development processes. Hence, possible market distortion effects of the public support should be always analysed.

6 Chemical, biological, radiological, nuclear or explosive (CBRNE) detection

6.1 General description of the segment

The increasing threat potential of terror attacks requires a wide range of detection principles within a fast and flexible reaction time to recognise and detect unknown and new kinds of threats. Before the 1990's, terrorist attacks were mostly based on explosive threats. Since that time the situation has changed and new agents as chemical and biological threats have become more and more an important issue in the security market. Unlike the explosive detection which is a warning indication for possible threat, chemical and biological detection directly indicate a threat.

6.1.1 Segment definition

'CBRNE detection equipment' is a commonly used term for equipment to detect chemical, biological, radiological, nuclear or explosive materials. Putting aside the threat posed by explosives – which have been frequently used – various terrorist groups have in the past employed or threatened to employ CBRNE agents although there have been few actual attempts by terrorists to cause mass civilian casualties using CBRNE agents. However, as information and capabilities become progressively more widespread via the Internet etc, governments and the general public alike view the potential threat of CBRNE weapons being in the hands of terrorists with growing concern.

As a response, owners and operators of 'critical infrastructures' such as airports, sea harbours, postal distribution centres, and those of infrastructures used for 'mass events' such as sport games, rock concerts or political rallies, have started to implement measures to protect themselves against the impact of those threats. As part of this development, equipment to detect CBRNE agents is being purchased. Detection systems are seen as a fundamental aspect of any successful CBRNE programme. Generally speaking, detection aims to establish the presence or release of a CBRNE agent in a given area.

The present analysis will focus on equipment designed to detect any traces of explosives, and chemical, biological, radioactive and nuclear substances. Furthermore, the study will not cover the design and production of "integrators" and the overarching networks used in detection systems.

6.1.2 Product overview

Current detection solutions involve a range of machines and technologies. Detection of explosives residue is typically carried out by swabbing the item to be analysed, and then processing this sample with an ion mobility spectrometer. This can be configured to not only detect explosives, but also traces of narcotics. Explosives detection trace portals (or 'puffers') use a non-contact method, blowing particles which are then analysed using ion mobility spectrometers. These are currently produced by Smiths Detection and GE Security, and can be found at a number of airports and other high profile locations.

For the identification of chemical agents devices in a variety of forms are available, from handheld units for first responders, to units which are intended for continuous monitoring of a given location. The technology used for detection of biological agents often uses Polymerase Chain Reaction (PCR) and is also available in portable forms.

6.1.3 Overview of CBRNE technologies

This section describes some of the main detection equipment in terms of the technology used to detect a particular component of CBRNE.

Technologies for detecting explosives

There are basically two types of detection technologies: one for the detection of explosives and one for the detection of traces of explosives. In the context of this report, x-ray based explosive detection systems (EDS) have been dealt with in Chapter 3 whereas the present chapter will deal with explosive trace detection devices.

Explosive Trace Detection (ETD) systems are also used in airports. About the size of a laser printer, they can cost less than € 1,000. They detect tiny traces of explosives on a bag's surface that may have been produced by a bomb placed inside or by someone who touched the bag after handling explosives. While ETD machines have lower false positive rates than EDS systems, current versions are slow and labor intensive. Someone has to "swab" the bag and then analyze the swab with the ETD machine. ETD has recently been built into much more expensive new systems such as "puffer" portals through which passengers walk, devices that check the tickets or other travel documents for traces of explosives, and systems to automate ETD of bags. It is also used in portable "sniffers" and other devices, such as lasers, that can test traces from bags or other objects.

Technologies for detecting radiological and nuclear agents

Technologies to detect radiological and nuclear (RN) threats are regarded as fairly mature. Typically, the architecture combines fixed and hand-held detectors. Fixed detectors are used at airports or harbours to help detect radiological or nuclear materials or weapons. Hand-held devices are also used for detection or confirmation of the presence of RN material.

The four basic types of radiation detection equipment are:

- **Fixed radiation portal monitors** (RPMs) are pass-through type monitors typically consisting of two pillars containing gamma radiation detectors and usually neutron detectors, and monitored from a display panel. Portal monitors are used for personnel,

vehicles, packages and other cargo in a variety of venues. Typically, all these applications use instruments that are either personnel or vehicle portal monitors.

- **Personal radiation detectors** (PRDs) are radiation detectors approximately the size of a telecommunications pager, which can be worn by front line officers or security personnel. PRDs can provide a flashing light, tone, vibration or numerical display that corresponds to the level of radiation present.
- **Hand-held gamma and neutron search detectors** (GSDs and NSDs) are radiation detectors used to identify the location of radioactive material. GSDs and NSDs provide greater sensitivity than do PRDs.
- **Hand-held radionuclide identification devices** (RIDs) are radiation detectors that can analyse the energy spectrum given off by a radionuclide to identify it. They can be used also as survey instruments to locate nuclear and other radioactive material.

Recent efforts have involved the development of non-intrusive technology, i.e. devices that do not necessitate manual inspection of the contents of a container or vehicle. These are primarily used for screening containers or vehicles in strategic transit points, such as seaports. Many of these devices can also be used to protect critical infrastructures. For example Radiation Portal Monitors can also be placed at international mail and package handling facilities to screen for radiation.

Technologies for detecting chemical agents

- ***Point detectors:*** Potential chemical agents are presently detected by first responders at the scene using either spot papers for detection (which have a limited degree of identification) or, in a few cases, more sensitive systems for chemical vapours using ion mobility spectrometry (IMS) or combining IMS and surface acoustic wave (SAW) devices for detection, limited identification and monitoring. These provide a useful first warning that is subsequently confirmed, typically after 6 to 48 hours depending on the agent, by more sensitive laboratory techniques such as gas chromatography-mass spectrometry (GC-MS). Reduction of false positives is being achieved both by combining the two techniques and by 'profiling' for background signals at specific installations in repeated *in situ* tests. However, there is little consensus on the reliability of such systems and broadening the range of analyses, reduction in false positives, and lowering of detection limits would be welcome.
- ***Chromatography:*** GC-MS and high performance liquid chromatography (HPLC) are widely accepted as the standard method for identification and quantification of chemical agents. Mobile (but far from hand-held) systems have been successfully deployed and there is a substantial body of work on further miniaturisation of mass spectrometry systems, including matrix-assisted laser desorption ionisation time-of-flight mass spectrometry. Current limitations of miniaturised or microfabricated MS instruments relate to poor mass-resolution. The parent systems are the existing standard for identification and may become more widely applicable for detection with further advances in miniaturisation and integration.

Technologies for detecting biological agents

Biological detectors are designed for a constant automatic standoff surveillance of an indoor facility (e.g., mall, postal distribution centre), an outdoor environment, or manual usage by first responders to check whether or not suspect traces consist of bio-terror

agents. Such systems are mainly designed to mitigate the effects of biological terrorism. There are four modalities of bio-detection:

- Outdoor Automatic Standoff-Detectors (e.g., project BioWatch)
- Indoor Automatic Standoff-Detectors
- Emergency Responder Biological Mobile Labs
- Emergency Responder Biological Hand-Held Detectors

6.2 Market (demand-side) overview

6.2.1 Overview of main market (customer) segments

The CBRNE market segment is part of the larger "mitigation segment" which involves protecting against, detecting, deterring, or mitigating the terrorist use of mass destruction. In addition, this larger segment includes efforts or planning to decontaminate buildings, facilities, or geographical areas after a catastrophic event. The market for detection equipment is one of several submarkets under this segment.

There are three types of venues that are viewed as potential terrorist targets, where detection equipment for CBRNE agents is used[252]:

- Ports of entry or departure; these include airports, harbours or border crossings.
- Critical infrastructures such as public water systems, mail distribution centres, stock exchanges or major banking centres, chemical facilities, power generation facilities, nuclear power plants, etc.
- High profile facilities such as landmarks, amusement parks, shopping malls, sports stadiums and business headquarters.

The bio-chemical agent detection market is one clearly identifiable market segment. These types of detectors are used for automatic standoff surveillance of an indoor facility (e.g. shopping mall, postal distribution centre), outdoor environments, or manual usage by first responders to check suspect traces for presence of bio-chemical agents. The nuclear/radiological detection market includes detectors used to identify and locate nuclear/radiological threats and they are intended to be used by governmental ports-of-entry agents, first responders, and other client agencies.

Depending on how the responsibilities at these facilities are defined, the buyers of CBRNE equipment is either a government agency or a private sector operator such as private security firms, banks, industrial companies and transport companies.

6.2.2 International market profile and market size estimates

Geographical distribution and specialisation

The majority of the companies active in this market segment are based in the USA. Other important centres are Europe (mostly UK and Germany) and Israel. Given the dominance of the US, it is not surprising that the EU does not have a particular technical advantage over other geographical areas. The only exception here is Smiths Detection, a UK leading producer of various types of detection equipment (as already showed in Chapter 3).

[252] Please note that the 'demand' for detectors coming from the military is not part of the analysis of this assignment.

Estimates of the size of the global CBRNE detection equipment market segment are hard to obtain and estimates based on various industry sources provide a range from €2 billion to €5 billion. The variation in market size estimates is due to the difficulties in defining the market on the one hand and the sensitiveness of companies to provide financial data on their operations on the other.

The Global Homeland Security, Homeland Defence & Intelligence Markets Outlook 2009-2018[253] puts the global CBRN Mitigation Market at nearly €8 billion for 2009 of which the share of the EU market is estimated at 20%. However, detection equipment is clearly a small part of this market and the industry figures quoted above are therefore likely to be overstating the market size.

In addition to the difficulty of estimating the overall size of the market, there is also the issue of large variations in time. There are undoubtedly peaks in demand - such as those caused by Gulf Wars 1 and 2, the period post 9/11 and localised heightened threat levels in different countries, but in years where no major crises occur, budget may drop fast, especially when economic crises are putting pressures on security budgets.

6.3 Description of the supply (value) chain

6.3.1 General description and overview

The supply chain for CBRNE detection equipment is characterised by the presence of a limited number of big global players in the upstream market, whereas downstream market is characterised by a similarly limited number of specialised firms that deliver highly sophisticated components such as microelectronic devices and optical components (also in combination: optoelectronics), and sensors and filters.

Many of the upstream companies originate from and still have strong connections with the military. This is one of the reasons "buying in" of components is limited: information on the equipment was highly classified and the components often represented the most innovative aspect of the equipment. With the move into the market for 'home security' products there is a general trend towards smaller products that can be handled by relatively untrained or at least non-expert personnel.

The supply chain is short (two levels) as most companies develop and manufacture most components of the end products. Two types of components are usually purchased: highly specialised parts such as lenses, small electronic devices or sensors.

6.3.2 Overview of main market players

From a supply point of view, the development and production of detectors has long been the domain of defence authorities or of companies that enjoyed long-lasting and close relationships with the military. With the increased demand for CBRNE detection

[253] Homeland Security Research Corporation (HSRC), *Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018*. Published in 2008.

equipment for homeland security purposes, these companies have been swift in seizing this new market, and at the global scene the resulting market structure is therefore dominated by not more than a dozen companies and only a few have their headquarters within EU borders.

The companies active in this domain have still largely integrated the research and development aspects into their production. This integration is not only technology driven, but the market size is not yet sufficient to warrant the development of a new class of companies specialising on the commercial development of CBRN detection equipment.

Table 6.1 indicates the most important (global) players in this market, ordered by the type of equipment they produce. Very few companies have their headquarters in Europe (exceptions are Smiths Detection and Siemens).

Table 6.1 Main global providers of CBRN equipment

Type of agent detected	Company
Chemical	Ahura, Bruker, Environics, GE Security, ICx Technologies, RAE systems, Smith Detection
Biological	Bruker, ICx Technologies , Smith Detection
Radiological/ nuclear	Bruker, Canberra, ICx Technologies, SAIC, Siemens, Smith Detection
Explosives (Trace Detection)	Bruker, Nuctech, GE Security, ICx Technologies, L3, Rapiscan, Smith Detection

Some companies offer the whole range of detection equipment. Some basic information of these companies is provided below. It has usually not been possible to isolate information on detection equipment from other activities the company is involved in:

- *Smiths Detection*[254] is a global leader in the provision of detection and screening technologies and for government regulated systems to detect and identify CBRNE they double its nearest competitor (see Table 4.4);
- *GE Security*, recently acquired by Sagem, is a global player selling detection and identification systems in 120 countries. Although it is developing and producing its own equipment, most of its profits are derived from integrating systems and (after sales) services (see Table 4.5);
- *Bruker Daltonics* is an operating company of Bruker Corporation with major facilities in Germany, where its CBRNE detection equipment is produced, and in the US. The share of CBRNe detection equipment produced by Bruker Daltonics in the mother company is 2% (see Table 6.2);
- *Environics Oy*[255] provides complete CBRN security solutions from early warning to consequence management and the company's detectors are being used by both civil and military agencies (see Table 6.3);
- *ICx Technologies* is a US based company that offers advanced capabilities to detect threats in all of the CBRNE segments. The company has offices throughout the US, Canada and Europe and employs over 800 people (see Table 6.4).

[254] www.smithsdetection.com

[255] Environics is part of the Finnish TEMET group. Apart from Environics, the group consists of TEMET oy, specialised in shelter systems and TVI vision oy, which is specialised in line scan imagery.

Other companies produce only equipment that is used to detect one or two substances:

- *RAE systems*[256] is a global provider of multi-sensor chemical and radiation detection monitors and networks for industrial applications and homeland security. RAE Systems' products are used in civilian and government atmospheric monitoring programs in over 50 countries (see Table 6.5);
- *Ahura Scientific Inc* (USA) manufactures handheld optical systems for chemical identification and it has customers in the homeland security, public safety, pharmaceutical, industrial and medical markets. It employs about 100 staff.
- *Canberra Industries*[257] USA is focussed on nuclear measurements and has a strong presence in Europe and particularly in France where it employs two-thirds of its 75000 employees. It delivers services to the nuclear industry and other clients to safely handle radioactive substances. It also delivers scanning equipment for security purposes. The company has production facilities in North America and in Europe;
- *Nuctech*[258] is also focussed at the detection of nuclear substances. The company, originating from Tsinghua University in China, has become a leading worldwide company with has around 1,200 employees and it currently holds the largest market share in the field of high-energy security inspection systems. The company served so far over 50 countries and regions in Europe, America, Asia, Oceania and Africa. In 2005 the total revenue was over USD 100 million generated by approximately 1200 employees.

[256] http://www.raesystems.com/

[257] www.canberra.com Canberra is part of the newly formed $9 Billion (2001) AREVA Group COGEMA, Inc. and Framatome ANP. AREVA is focused on all aspects of the nuclear power generation and nuclear fuel cycle fields. Canberra operates a total of 12 production and engineering facilities in the US, France, Belgium, England, and Canada.

[258] http://www.nuctech.com/index_en.jsp. No further company data available.

Table 6.2 Bruker Daltonics: Basic company indicators

BRUKER DALTONICS (US)				
Main indicators	**Bruker Corporation**		**Bruker Daltonics**	
	2007	2008	2007	2008
Turnover	€ 826m	€ 885m	N/A	€ 160m (€ 32m correspond to CBRNE equipment)
Profit	€ 110m	€ 86m	N/A	N/A
R&D budget	€ 89m	€107m	N/A	N/A
Number of employees	4,400	4,250	N/A	700*
Description of the company				
Bruker Daltonics is in the business of manufacturing and distributing mass spectrometry instruments that can be integrated and used along with other analytical instruments. Bruker Daltonics is an operating company of Bruker Corporation, a global operator who designs, manufactures and markets products based on mass spectrometry for pharmaceutical, biotechnology, proteomics and molecular diagnostics companies, academic institutions and government agencies. The company is headquartered in the US, with major facilities in Germany (Bremen and Leipzig) and the US (Billerica, MA), as well as worldwide sales & service centres.				
Main products and technologies				
Bruker Daltonics has diverse technology platforms that integrate mass spectrometry systems with automated sample processing systems and productivity-enhancing software for life science applications. They are also a worldwide leader in supplying systems for substance detection and pathogen detection in security, defence and anti-terrorism. Bruker Daltonics' CBRN detection customers are highly fragmented, and the company competes with a number of companies in this area, of which the most significant competitor is Smith Detection which is located in the UK. The main types of equipment are the following: ▪ Nuclear detection: RAID-AFM (Automated Facility Monitor for Nuclear and Chemical Detection), SVG2 (A new generation of nuclear radiation detectors), GRAETZ ED 150 (with doserate indication and alarm functions), GRAETZ X 5 C plus - for personal radiation protection; ▪ Biological/chemical detection: BioProfiler (Microorganism Identification based on MALDI-TOF-Mass Spectrometry), CWA Detection (E²M - Enhanced Environmental Mass Spectrometer), MM 1 (Mobile Mass Spectrometer for reconnaissance vehicles), MM 2 (Mobile Mass Spectrometer) , RAID series (Rapid alarm and identification devices for CWAs), RAID-M series (Hand-held Chemical Agent Monitor), RAID-XP (NC Detector), RAID-AFM (NC Version, Automated Facility Monitor for Nuclear and Chemical Detection), RAID-S2 (Mounted Trace Gas Detector), RAPID (Stand-off detector for volatile chemical hazards).				
** From these, less than 200 employees are working on CBRNE equipment*				

Source: Bruker Corporation website (www.Bruker.com) and Bruker Daltonics website (www.bdal.com)

Table 6.3 Environics Oy: Basic company indicators

ENVIRONICS OY (FI)				
Main indicators	**Finntemet group**		**Environics Oy**	
	2007	2008	2005	2008
Turnover	€ 33m	N/A	N/A	N/A
Profit	N/A	N/A	N/A	N/A
R&D budget	N/A	N/A	20%	N/A
Number of employees	N/A	N/A	100	N/A
Description of the company				
Environics Oy is a technology enterprise providing a full range of services and products for chemical detection branch. Environics has a more than 20 years experience in the CBRN field. The company's detection technology dates back to the early 1980's resulting from some R&D started within the Finnish Defence forces. The company was established in 1987. It now has subsidiairies in the USA, the Middle East and in China. The majority shareholder is Finntemet group, a family owned enterprise. In total the company has manufactured and delivered over 10,000 CWA detectors, many hundreds of integrated systems delivered to over 40 countries.				
Main products and technologies				
Environics provides portable CWA Detectors, handheld Chemical Detectors , CWA -Detection Systems for vehicle applications, CWA -Detection Systems for naval applications, CWA -Detection Systems for fixed applications, Integrated multisensor systems and Accessories, service and spare parts etc.				

Source: Environics OY website (www.environics.fi)

Table 6.4 ICx Technologies: Basic company indicators

ICx TECHNOLOGIES (US)				
Main indicators	**ICx Technologies**		**ICx detection segment**	
	2007	2008	2007	2008
Turnover	€109m	€ 137m	€ 63m	€ 73m
Profit	€ 50m	€ 57m	€ 18m	€ 34m
R&D budget	€ 17m	18m	N/A	N/A
Number of employees	N/A	833 (60 in DE)	N/A	N/A
Description of the company				
ICx is involved in the development and integration of advanced sensor technologies for homeland security, force protection and commercial applications. Their proprietary sensors detect and identify chemical, biological, radiological, nuclear and explosive threats. The company has offices throughout the US, Canada and Europe and employs over 800 people. They rely on a substantial portion of their revenues on contracts in which they act as a subcontractor to other contractors, typically prime contractors and system integrators who sell directly to government agencies or private customers.				
Main products and technologies				
In the CBRNE Detection segment, product revenue is primarily derived from the sale of Fido explosive detectors, Identifinder and Interceptor radiation detectors, AirSentinel bioaerosol sensors and the cheMSense 600 line of products.				

Source: ICx Technologies website (www.icxt.com)

Table 6.5 RAE Systems: Basic company indicators

RAE SYSTEMS (US)				
Main indicators	**RAE systems**		**Detection segment**	
	2007	2008	2007	2008
Turnover	€ 72.6m	€ 76.3m	N/A	N/A
Profit (loss)	(€ 8.8m)	(€ 5.7m)	N/A	N/A
R&D budget	€ 6.4m	€ 5.4m	N/A	N/A
Number of employees	N/A	1,324	N/A	N/A
Description of the company				
RAE Systems Inc. was founded in 1991 to develop technologies for the detection of hazardous materials in environmental remediation and chemical spill clean-ups. RAE is a global developer and manufacturer of rapidly-deployable, multi-sensor chemical and radiation detection monitors and networks for application in five key markets: oil and gas, hazardous material management, industrial safety, civil defence and environmental remediation. RAE has significant operations in People's Republic of China including research and development and manufacturing.				
Main products and technologies				
RAE Systems' products include portable, wireless and fixed atmospheric monitors and photoionization detectors and gamma and neutron radiation detectors for the detection and early warning of hazardous materials. The company offers handheld spectroscopy instruments for rapid chemical identification. FirstDefender (a Raman spectroscopy device), and TruDefender FT (Fourier Transform Infrared spectrometer).				

Source: RAE Systems website (www.raesystems.com)

6.3.3 Technology aspects

Functional requirements

The specific functional requirements of the detection of CBRNE substances depend heavily on the specific substance being targeted, and the environment in which sensing will be carried out. However, these general functional requirements are common to almost all applications.

The *reliability* of a detection device describes the extent to which it generates false positive or false negative results. Whilst the consequences of a false negative result can be very severe, it is important to note that excessive false positives also have a cost, requiring investigation and response.

The *sensitivity* of a device is often expressed as the quantity of a substance required to generate a detection result. This is measures in parts per million (PPM) or parts per billion (PPB). The target sensitivity depends on the substance being detected; in the case of anthrax, a single spore can be deadly, and so this should be the target sensitivity threshold.

Stability relates to the consistency of detection performance in a range of environmental conditions - such as differing temperatures, vibrations, shocks.

The *cost* of a detection device, in relation to its lifetime and effectiveness, is a critical factor. An explosive detection sensor for an airport is likely to be in constant use, and thus a higher cost can be amortised over a longer time period and a greater number of

operations. A node in a distributed sensor network, which may need to be replaced more regularly, should typically have a lower per piece cost.

The *speed* with which a detector operates is an important factor in many applications. If a harmful substance is present, it should be detected in time to mitigate its effects; to order an evacuation, or to stop a vehicle carrying dangerous material.

Power consumption of devices, which are not connected to mains supply, such as portable detectors, is low.

Most of the detection applications described in this chapter occur outdoors, and so the detection technology must withstand a range of environmental conditions, including high and low temperatures, direct sunlight, wind and rain.

Nature and origin of technology

Most if not all of the technology used in the production of detection equipment has been developed for military purposes and the market (development) is still driven by military or homeland defence/security concerns and budgets. Two characteristics of civilian application require major adaptations of the military type equipment. One is the need for smaller (often handheld) equipment and the other is the requirement of processing large numbers (of people, bags, containers, etc.) in a short period of time.

Research and Development

Most of the companies active in this market devote a large share of their budget to R&D (sometimes up to 20%). Although the basic technologies have been developed years ago, many applications have not yet reached satisfactory levels of reliability and often give false (positive) signals when no dangerous materials are present. This is especially true for CB and RN detection where amount of substance is often very small and the detectors of easily 'fooled' by other substances in the direct environment or are physically challenged by environmental conditions such as humidity (at airports), high winds (in sea ports), low temperatures etc.

Many countries also have government-owned facilities where (basic) research is carried out, often in conjunction with the private sector.

6.3.4 Component supply

The components of CBRNE detection equipment range from specialised components such as filters, lenses and electronic measuring devices to more standard components such as batteries, caskets, belts etc. The more specialised components are mostly developed and produced in-house, and if not, they will be sourced from a limited number of highly specialised firms – often located in the vicinity – with which a long standing relationship will exist. Most of the more standard components are sources from other companies.

This means that the value chain is highly integrated, if not by ownership than by other means. An example is where the equipment producer owns the patent on one of the components (or the technology used in it) and in exchange has contracted itself to buy a minimum number of that component from the particular component producer.

The profile of the component producers in this market a diverse, but most are small to medium sized companies that operate in a particular technology niche.

6.3.5 Equipment and sub-systems

A number of producers (Bruker is an important example) produce customised sub-systems for other companies, and relationships between these companies is often close and long-standing. However, this process is often geographically limited, either because of the good understanding needed to enable the development and production of essential parts of the detection equipment, or simply because there is a national security aspect involved that prohibits a company from buying abroad (this if mostly the case in the US).

6.3.6 Integration and customisation

Integration is the key word for CBRNE detection and most of the larger companies that produce the equipment are also active as 'integrators' either in mobile units such as cars or small airplanes or into larger units used at airports, seaports or border crossings. The demand for integrated systems has grown with the call for equipment that can scan large number of people in a short time such as in mass transport systems or at airports where both people and their luggage need to be checked in a short time.

An example of a large company that is mostly active as an integrator is Thales. This company offers security systems that integrate one or more detection components with software, perimeter protection, satellite observation, etc.

6.3.7 Related services

Almost all maintenance and repair is carried out by the company that constructed the equipment, there are no known 'service companies' in the market for this kind of equipment. The companies use two strategies: they either charge a separate fee for services, thereby adding important revenues to the sales revenues, or they include the servicing in the original sales price.

Besides maintenance and repair services, operators often have contracts with the supplier that allow the latter to improve the performance, either by adapting software or by installing or replacing parts of the equipment.

6.3.8 Linkages to final markets

Equipment manufacturers will usually have their own sales department with sales and products are usually delivered directly from the company to the client, without using intermediate services of distributors or storage facilities. This is mostly related to the high value of the product in combination with the sensitivity of the instruments.

6.3.9 Overall assessment of the supply chain

The market for CBRNE detection equipment shows the same characteristics as those of most other security equipment industries: most of the value added in the chain occurs at the level of integrators and service providers. For EU companies, the production of components has low value added. This explains why many companies are integrated along the supply chain and some (such as Thales) operate only as integrators.

Horizontal networking takes place to limited extend with research organisations firms, but most companies have their own R&D facilities and participation in research programmes has limited (commercial) value, although it is valued as a source of networking and benchmarking.

6.4 Main trends and developments

6.4.1 Market trends and developments

The market for CBRNE detection equipment is expected to continue its expansion due to several factors. Not only are governments designing and implementing security policies and regulations which demand higher levels of security in and around critical infrastructures, airports etc., but private sector operators such as banks and supermarket chains are becoming increasingly aware that the threats of CBRNE are to be taken seriously. For the industry the widening of the market is a welcome development, not only because of the potential for growth, but also because it can stabilise the somewhat volatile growth patterns caused by heavy fluctuations in government budgets.

Although there are no figures to attach to this assessment, one estimate from the US sets the amount to be spent on this type of equipment for the next 5 years at 5 billion USD. However, in view of other information, this estimate should be seen as an upper limit.

Although the general feeling among industry players is that the market will continue to grow, two threats to this growth have been pointed out. First is the global economic downturn. This leads to budget cuts in both the private sector and the government sector and the feeling is that security will not be able to retain its prime position. Secondly is the growing awareness that equipment can only perform well if the operator knows how to handle it properly. This leads to two trends: a continued development towards 'foolproof' instruments and more emphasis of owners and operators of critical infrastructure on training (at the cost of hardware budgets).

EU companies are increasingly operating outside of the EU and it is estimated that more than half of the revenues are now coming from outside the EU (mostly Asia and the Middle East). EU companies have no access to the US market (except through their US subsidiaries) and South America. Although there are talks between the EU and the US, it is not expected that this will result in any change during the next 5 years.

6.4.2 Technology trends and developments

Two kinds of trends can be identified: those related to the technology used and those related to the use of technology. The first concerns new technologies that provide better and smarter technological solutions and the second allows for easier use by operators.

New technologies

Recent progress in miniaturisation of low power electronics has also made the development of compact gamma and neutron detectors possible. These can be broadly distributed to different categories of personnel for routine use. These instruments are similar to message pagers. They are small, hands-free, low-power instruments which can be worn by law enforcement or customs officers for continuous monitoring and they are also relatively cheap. However, their performance is generally poorly rated and they cannot function as independent detection devices and need to be coupled to other more sensitive sensors, in the event of a positive alarm.

A more recent technology, called RadNet combines a cellular telephone, a personal digital assistant with Internet access, and a global positioning system (GPS) locator with a radiation sensor. The RadNet detector is also fairly inexpensive, lightweight, able to operate at low power and is precise enough to eliminate background radiation emitted by food, medical devices or soil.

Globally, R&D efforts are directed towards ease of use and integration of several systems for increased efficiency. For example, integrated systems would combine information from a portable radiation detection system with that of hand-held detectors and video cameras, or information from gamma-ray detectors, with neutron detectors and detectors that take visual images.

Laser standoff systems are not yet available for practical use but are being developed for both liquid and solid chemical contamination. Those reported in the literature are either visible or UV Raman systems with upwards of ten meters range. High-intensity, low-cost and miniaturised laser sources are being developed rapidly and should benefit the creation of portable laser standoff systems. If these approaches can reach appropriate specifications for sensitivity, selectivity and response time, they will be ideal for detection and monitoring applications.

Increased automation and integration

For effectiveness and throughput to increase, and for the cost of transaction to come down, there is an ongoing search for detection systems that will become almost fully automated. Human participation in the screening and analysis process is the major cause of human errors and sluggish throughput.

One of the industry trends is to increase the integration of the detection equipment with larger security setups such as biometrics, databases, and communication networks. The goal is to create early warning systems (e.g. during checks on people, baggage or goods) that can help to prevent CBRNE attacks or facilitate a rapid deployment of emergency or evacuation measures in a crisis through early detection of warfare agents.

Against this background, the interdisciplinary topic of 'multi-sensor systems for CBRNE risks' should preferably promote multi-modal and multi-functional detector platforms, new types of mobile sensor concepts as well as new types of sensor and data merge concepts and procedures to achieve a sustainable improvement in security at the point of deployment and to accelerate security checks. Essential criteria for the development and integration of multi-sensor components for both local and long-range detection of CBRNE substances include not only a high level of sensitivity, resolution and selectivity but, above all, ease of use, autonomy, a high level of automation, robustness as well as low susceptibility to false alarms and real-time capability.

6.4.3 Production trends and developments

The projected growth in the market for detection equipment is luring many companies - who up to recently produced mainly for the military - to enter the market for civilian applications. It is therefore expected that a large number of mergers and other type of shifts in the market will take place in the coming years.

It is not expected that the market constellation in terms of production chain will change in the near future but as the competition becomes fiercer it can be expected that companies will divert at least some of their production (of components) to countries outside of the EU or the US.

6.4.4 Overall assessment of trends and developments

The overall trend in the market for CBRNE detection equipment is towards more integrated systems, which will be easy to operate, but with higher reliability. Since there is a growing public awareness of the need for protection against possible terrorist attacks where CBRN substances are involved, the market for detection equipment will continue to grow although the present economic crises will dampen the high growth figures predicted by marketing analysts and industry sources. This trend will also lead to an ever growing share of detection equipment within the lager market CBRNE 'mitigation' equipment and services[259].

6.5 Regulatory conditions and development

6.5.1 International, European and national security-related regulatory conditions

There is no internationally agreed regulatory framework for the production of CBRNE detection equipment, neither at global level, nor within the EU. For the production (or use) of CBRNE equipment all Member States have their own laws and regulations. The same is true of standardisation and development of methodologies and limits for detection of CBRNE agents can be considered.

[259] According to the *Global Homeland Security, Homeland Defence & Intelligence Markets Outlook 2009-2018* by Homeland Security Research Corporation, this share is to grow from 13.5% in 2008 to 16.3% in 2018.

In September 2006, the Commission adopted a Green paper on detection technologies in the work of law enforcement, customs and other security authorities, and the paper recognises that modern detection technologies have an important role to play in the fight against crime and terrorism. The Green Paper aimed at further stimulating the public-private dialogue and partnership, allowing for focussing of investment in standardisation, research, certification or interoperability of detection systems and for transforming research results into useful and applicable tools. It addressed the following issues:

- Standardisation;
- Certification of detection tools;
- Information and experience exchange on the use of new and innovative detection tools;
- Integrated detection systems (multi-sensor systems);
- Procedures for how best to deploy and use detection tools;
- Improvement of the protection of mass events.

In 2007 the EU Justice and Home Affairs Council Conclusions wrote that "effective policies to address CBRN risks should be further developed in close consultation with national authorities and, as appropriate, the industrial sectors concerned, academic institutions and other relevant stakeholders, notably with a view to ensuring the viability and proportionality of measures which may be required (…)".

Furthermore, Decision 2007/149 of 20 December provides for civil protection modules, in particular for CBRN detection and sampling and for Search and Rescue in CBRN conditions.

It has been found that in some instances, exports from the EU of CBRNE detection equipment to certain countries is blocked by custom authorities, because these countries are on a list that prohibit exports of dangerous (i.e. CBRNE) materials.

6.5.2 Industry and market-based standards

The development of standards is a cost-effective and efficient means of improving detection capabilities. Such standards should ensure similar level of safety and security across the EU, and allow benchmarking of detection solutions and this is recognised by EU authorities and the security industry itself. Several discussions in this field are ongoing and a CBRN Task Force of the JRC is not only working on certification, testing and trialling of schemes involving CBRN but is also working on standardisation.

These efforts should go some way to strengthen the position of EU firms vis-à-vis their US counterparts as they operate in a single market with clearly defined standards and requirements.

As mentioned before under Chapter 3, other initiatives such as the CREATIF Network (Network of Testing Facilities for CBRNE detection equipment) have been put in place under the umbrella of the 7th Framework Programme. This network sets a platform for the exchange of practices and information on test facilities and their portfolio of expertise while promoting the following actions:

- The harmonisation of testing practices through initiatives to produce harmonised EU-wide standards (geographic harmonisation);
- The exchange of formal and informal information on best practices around Europe in order to promote a Europe-wide uniform technical level of testing (technical harmonisation, quality assurance);
- The definition of a set of minimum requirements for testing and generating certification strategies for facilities, service providers and devices;
- The support of user decisions, industry products and service development while offering an open forum of exchange and debate involving decision-makers and other relevant stakeholders in the field.

One of the most relevant deliverables of the network (a funded FP7 project) will be a roadmap for a European certification system for CBRNE detection products and services and the reflection on the continuation of the CREATIF network as an autonomous body after the end of the funded project[260].

6.5.3 Overall assessment of regulatory conditions

There is a need for a regulatory framework that encompasses the production and marketing CBRNE detection equipment market and possibly capturing the wider market of CBRNE mitigation. This would accomplish two objectives: i) it would level the playing field between EU operators and clarify some of the issues regarding the use and export of CBRNE equipment, and ii) it would provide a framework for targeted interventions by public authorities, either through financing research or by promoting and investing in certain equipment or solutions. Both actions would improve the competitiveness of EU companies vis-à-vis companies based in other parts of the world.

6.6 The global competitiveness position of the EU industry

There are only a few major EU companies in this market segment who compete on a global scale; notably Smith Detection and Sagem Sécurité - which recently acquired GE Security. However, a number of US based companies have an important EU presence and some small and medium sized companies are important suppliers of larger firms.

Although it is expected that this market segment as a whole will continue to grow, it is unlikely that - with the ongoing concentration of the industry - the EU presence in this segment will grow at the same speed. In addition, there is a number of non-EU or US companies – such as Nuctech - who are successfully competing in third markets.

According to the publication Global Homeland Security, Homeland Defence & Intelligence Markets Outlook 2009-2018, North America will actually increase its share of the market and that of the EU will be somewhat reduced.

[260] More information on the CREATIF Network can be found at www.creatif-network.eu or on the FP7 info brochure prepared for the project: http://ec.europa.eu/enterprise/security/doc/fp7_project_flyers/creatif.pdf.

The fact that EU companies are not able to export to the US (the biggest market CBRNE detection equipment) is the single biggest disadvantage of these companies. It is not clear if any progress in opening up this market has been achieved over the last five years.

6.7 Conclusions and potential policy issues

A number of policy issues regarding the market for CBRNE detection equipment can be raised:

- **A fragmented market.** As already mentioned in Chapter 3, the European industry for detection equipment is fragmented in the absence of coordinated policies and inter-industry standards. Addressing these two issues, in addition to implementing a harmonised approach to security technologies would improve the global competitiveness of the EU industry. The issue of export bans to certain countries can also be addressed under this heading;
- **Public investments in the sector are uncoordinated and insufficient**. There is no policy or concerted action by Member States to provide the sector with a similar stimulus as in the US, where large amounts of public funds are spend on R&D. Without this type of funds, EU companies may loose their technology edge. The EU should review what options it has to improve targeting of its buget for this purpose;
- **Various restrictions on exporting to the US** make it difficult for EU companies to enter the US market. There is possibly a role for NATO to look into this issue.

7 Biometric solutions

7.1 General description of the segment

7.1.1 Segment definition

Biometrics is a general term referring to a characteristic or a process:

- **Biometric characteristic**: a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for recognition purposes;
- **Biometric process**: encompasses the automated methods of recognizing an individual by measuring, comparing, biometric characteristics;

Several bio-characteristics, also called modalities, can be used in order to perform people identification/authentication tasks. Fingerprints are the most commonly used but others are being either investigated or already in use depending on application requirements:

- Behavioural recognition;
- Dynamic signature;
- Facial recognition;
- Fingerprint;
- Hand geometry;
- Iris;
- Palm print;
- Voice recognition;
- Vascular.

There is not one biometric modality that fulfils the requirements of all security applications and many factors have to be taken into account when implementing a biometric solution including location, security threats, application profile (authentication vs. identification), number of users, etc. Biometric modalities are in addition at different stages of development, as we will see later on.

Biometric solutions are essentially used to perform two types of control:

- **Authentication** corresponds to the action of comparing a biometric characteristic with one embedded in any form of ID paper (ID credential, access pass, etc.). This process is called 1:1 control and is used to verify the holder identity.
- **Identification** corresponds to the action of comparing a biometric characteristic with a set of characteristics registered/stored within a database. This process is called 1:n control and is used to verify one individual identity against a predefined population. It not only provides identity checks but also ensures the uniqueness of all database entries, thus reducing fraud capabilities.

Following from the two types of control mentioned above, one approach to describing the segmentation of the biometric equipment industry is to consider the functionality of biometric solutions. Two main markets can then be distinguished:

- **1:1 solutions:** The purpose of 1:1 biometric solutions is to authenticate the holder of a credential title containing one or several biometric templates. The credential title can either be a smartcard with dedicated security hardware and encryption process or a standard pass (company card, etc.). This type of biometric solution is mainly used for physical and logical access control procedures in order to provide increased comfort and security to standard procedures already in place.
- **1:n solutions:** These biometric solutions consist of capturing the biometric signature of an individual and compare it with a defined biometric datasets corresponding to 'n' enrolled individuals that are being registered in a database. The added value of such biometric systems compared to 1:1 biometric applications is to verify the uniqueness of an ID credential and to reduce ID spoofing risks. For such type of application, the heart of the system is the biometric engine, i.e. the software in change of the comparison and matching procedure between the captured biometric datasets and the database. Of course, the number of companies having this type of know-how is much more limited on a worldwide basis. The 1:n biometric market can then be divided in 2 sub-segments depending on the number of individuals:
  - **Small 1:n applications**. For this type of application, 'n' can represent up to few thousands people. These applications correspond to access control solutions in dedicated area that may represent special security measures like power plants, embassies, highly secured IT network, etc. The complexity of biometric engines for such type of application is rather small considering the limited size of the database. The number of suppliers is thus important although considerably smaller than for 1:1 biometric solutions.
  - **Large 1:n applications**. For this type of application, 'n' can represent up to millions of people. These applications correspond to large systems for governmental applications (criminal, healthcare, ID cards, VISA and passports, etc.). In this very specific market, the number of suppliers having the required degree of expertise is very limited due to the complexity of the biometric engine and the required level of performance (accuracy, speed, etc.).

Following from the above, the biometric 'security' market covers two major application profiles:

- **Commercial application with low security levels**, close to comfort applications (e.g. logic access to computers or IT networks); typically these require 1:1 solutions[261].
- **Public systems with high security constraints**, interoperability issues and large population coverage; typically these require (large) 1:n applications.

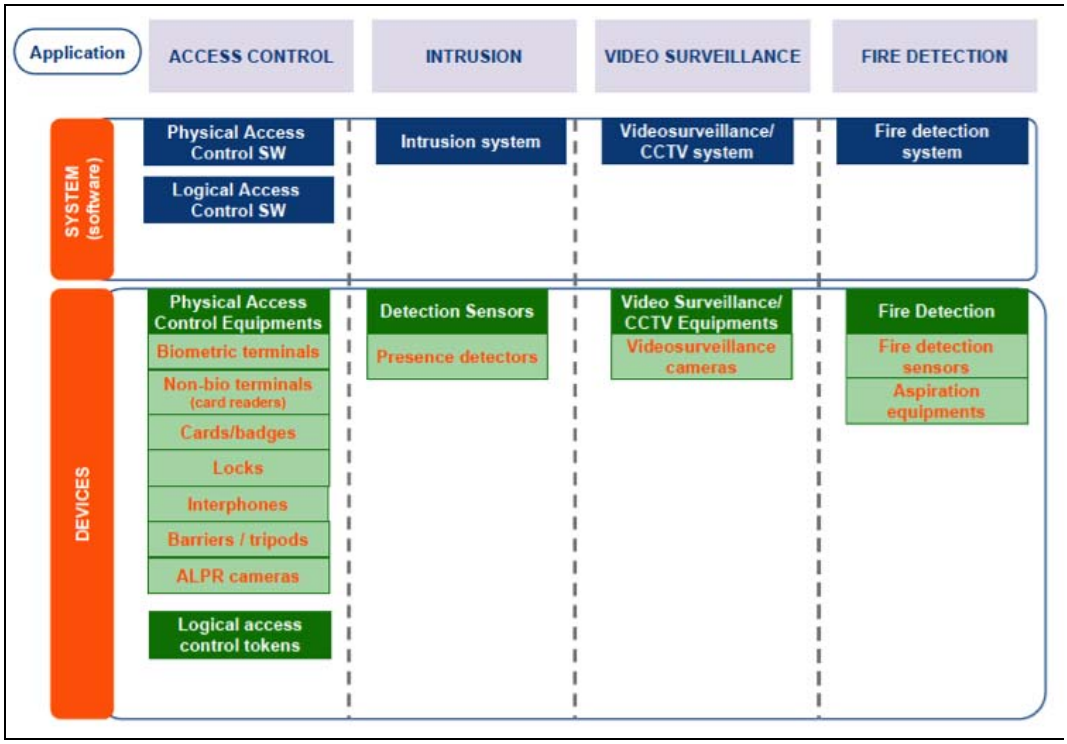
In this Chapter the specific segment that will be covered is **'Biometric solutions for entrance/barrier control of protected areas, buildings or events'** and, accordingly, the analysis will mainly focus on the second application profile corresponding to important security threats in rather large public systems.

[261] For 1:1 solutions, equipment/product performance is typically not very important and the market is usually cost-driven with a large number of suppliers. Their competitive advantage tends to be based on application software and customization capabilities to adapt a standard solution to the customer needs.

7.1.2 Product overview

Figure 7.1 provides a segmentation of the security industry from a product and functional perspectives. We can see from this figure that biometric is only a part of a global security solutions. It also indicates that biometric products mainly perform access control functions within a security system, where it competes or collaborates with other access control technologies including cards/badges, locks; interphones, etc.[262]

Figure 7.1 Electronic security system market segmentation



Source: Sagem Sécurité

Equipment categories and components

Typically, a biometric system comprises five integrated components:

- **Sensor**: used to capture the biometric characteristic and convert it into a digital format;
- **Signal processing algorithms**[263]: used to verify the quality of the biometric image provided by the sensor and create a digital biometric template that will then be transferred to the system;
- **Data storage**: this component is used to store the biometric template. It can either be a centralized database for identification application or a personal ID credential (generally a smart card) held by an individual;

[262] Biometric solutions present some key advantages compared to other identification solutions, notably in terms of greater difficult to steal and/or to falsify, and enhanced comfort of use.

[263] An algorithm is a sequence of instructions that tells a system how to solve a problem. It is used by biometric systems, for example, to tell whether a sample and a template (a mathematical representation of biometric data) do match. Cryptographic algorithms are used to encrypt sensitive data files, to encrypt and decrypt messages, and to digitally sign documents.

- **Matching algorithm**: also called biometric engine, this software compares a new biometric template with an existing one, either stored in a database or in a personal credential;
- **Decision process**: this component uses the result of the matching algorithm in order to define a system-level decision and perform corresponding actions (alarms, access grant, etc.) based on pre-defined rules of acceptance that are defined based on application, environment, security level parameters, etc.

The specific segment analysis will cover the following equipment categories, including both devices and software components:

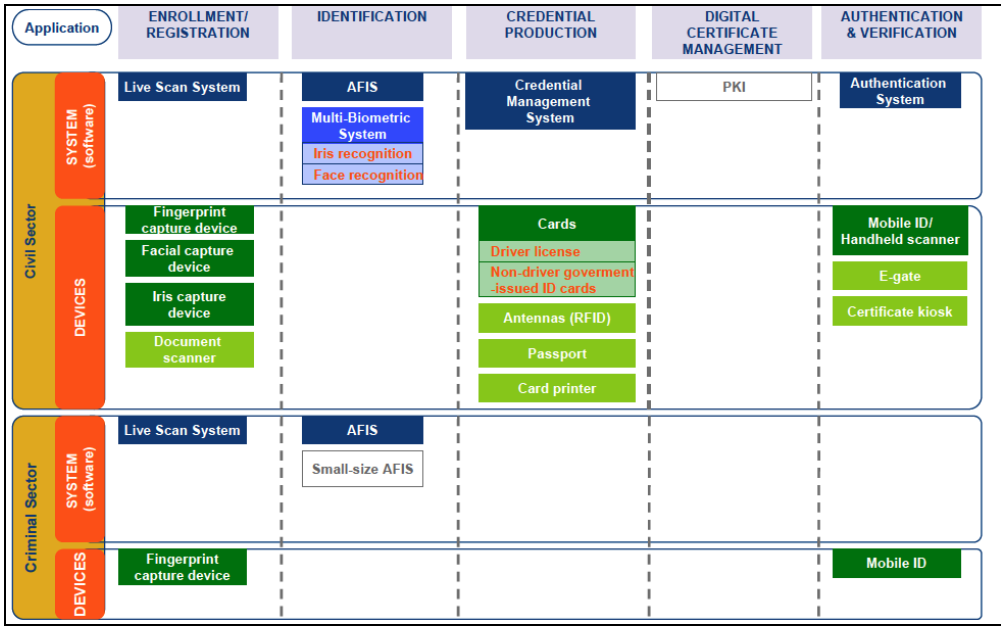
- **Devices**: sensors, as well as portals and kiosks (for enrolment procedures[264] and/or access control purposes);
- **Software**: signal processing and matching algorithms;
- **Specific IT network infrastructure** that may be part of the full identification solution provided by major suppliers;

It should be noted that data storage and smart cards are not included in the segment analysis as those equipment categories are not specific to the biometric industry and thus fall out of the scope of the present study.

Functional segmentation

Figure 7.2 illustrates the complex environment in which biometric products/technologies are implemented, and identifies five functional segments that come together within a complete system. From this perspective, the specific segment analysis undertaken in thi Chapter will concentrate on the three identified functions that are the most specific to the biometric industry supply chain, namely **'Enrolment/Registration', 'Identification' and 'Authentication/Verification'**.

Figure 7.2 Identification management system market segmentation



Source: Sagem Sécurité

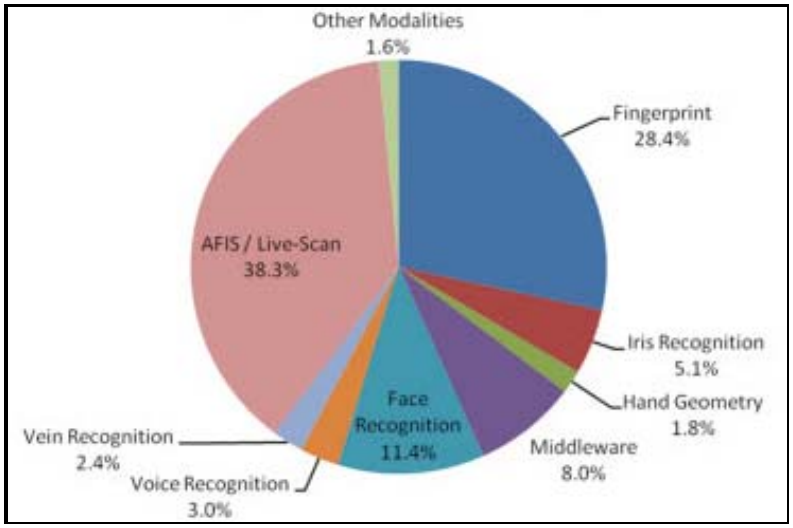
[264] Initial process of collecting biometric data from a user and then storing it in a template for later comparison.

7.1.3 Overview of biometric security technologies

Several biometric modalities can be used for authentication and identification purposes and it is likely that additional solutions may develop in the future. Most of these technologies are based on a good understanding of human anthropometry in order to accurately characterise and process individual 'bio-signatures'.

Fingerprints continue to be the leading biometric technology in terms of market penetration, which is directly linked to the anteriority of this technique and to its large application scope. As shown in Figure 7.3, estimates for 2009 indicate that fingerprints (including AFIS systems[265]) represent two-thirds of the biometric market, followed by face recognition systems (11% est.), while iris detection systems are still limited (5% est.). This latter technology could develop further in the future like other 'trace-free' technologies (e.g. vein and facial recognition systems).

Figure 7.3 Biometric industry revenues by technology, 2009



Source: International Biometric Group

Fingerprints

Fingerprint analysis was pushed forward in the USA by the FBI which funded the development of this technique during the 1970s in order to automate the classification and extraction of fingerprint individual patterns (also called minutiae), which gave birth to AFIS systems. Depending on application, several hardware technologies can be used in fingerprint sensors including optical (most common today), capacitive, ultrasound and thermal. The resulting image of the fingerprint is then processed by a software programme in order to create an individual biometric template, which can then be used for comparison purposes to other samples.

[265] An Automated Fingerprint Identification System (AFIS) is a system originally developed for the use by law enforcement agencies, which compares a single fingerprint with a database of fingerprint images.

Face recognition

Although less mature than fingerprints recognition techniques, face recognition has achieved major advancements in the 1990s following large technology evaluation sponsored by the Defence Advanced Research Products Agency in the USA. There are three main approaches to face recognition systems including geometric (feature based), photometric (view based) and algorithms based, which provides the highest ratio of performance with respect to the quantity of information that needs to be stored.

Face recognition is being heavily investigated due to the synergy that it may provide if coupled with existing camera surveillance networks. One could indeed envisage 'non-cooperative' biometric identification controls based on image records or even in real time depending on performance achieved by future face recognition systems.

Image sensors and image processing are obviously the key research fields in this domain.

Iris recognition

It was only during the 1980s that the concept that no two irises are alike emerged, providing the base for a very efficient biometric modality. It then took 10 years to see the first commercial products entering the market in 1995. Iris recognition techniques are based on high-quality digital cameras using infrared light to illuminate the iris without causing harm or discomfort to the subject. Specific algorithms are then applied to extract the iris template.

The commercial development of Iris recognition systems has been limited due to a US patent filed on the iris recognition concept, which forced the utilisation of a specific template algorithm. This in turn limited the access of other companies having developed different algorithms techniques. This patent fell in the public domain in 2005.

Vascular recognition

Vascular imaging has been in development in Japan since the 1990s. The first research papers on vascular recognition techniques were published as late as 2000, only just preceding the introduction of a first commercial device using subcutaneous blood vessel pattern in the back of the hands. The vascular sensor device is based on near-infrared rays generated from a bank of Light Emitting Diodes. Blood vessels absorb part of the ray and a Charged Coupled Device camera is then used in order to capture the reflected image of the vascular pattern.

Relative advantages and disadvantages of different biometric technologies

Table 7.1 indicates the relative pros and cons of different biometric technologies. Although fingerprint techniques do not demonstrate very high performances as an identification technique, they present a decisive advantage for applications requiring traces like criminal applications. Moreover, technology is improving to enhance fingerprint solutions performances and prevent in particular ID spoofing.

From a more general perspective, this table also indicates that technological performance is not directly driving market development. From a general perspective, we can notice that the biometric market structure in terms of technology is directly related to the sequence of biometric modalities introduction. Older technologies tend indeed to have

larger market shares, reflecting the long technology introduction process due to standardisation, market acceptance and technology development timings.

Table 7.1 Classification of biometric technologies for 1:1 authentication solutions

Technique	Security	Accuracy	Price	Speed	Devices size
Vein patterns	High	High	Low to medium	Medium to High	Small to medium
Palm patterns	Medium	Medium	Low to medium	Medium to High	Small to medium
Fingerprint	High	Medium to high	Low	Medium to High	Small
Facial	Medium	Medium	Low	Medium to High	Small
Iris	High	High	Medium to high	Low to Medium	Large

Source: DECISION

7.2 Market (demand side) overview

7.2.1 Background to the development of the biometrics market and industry

Although humans have always used faces to recognise familiar and unfamiliar people, the true origin of biometrics goes back to the mid-1800s and the industrial revolution when the first attempts to characterise biometric recognition systems and procedures were engaged. Indeed the demographic boom in conjunction with the development of large cities, productive farming, etc. has stressed the need to identify people for both commercial and justice purposes[266].

The true development of biometric systems and industry is however much more recent and corresponds to the development of automated biometric comparison/matching systems, coinciding with the rise of computer systems in the second half of the twentieth century. The biometric market really took off during the 1970s and 1980s thanks to large contracts in the United States for police forces (e.g. FBI) on one hand and for civil registration purposes in developing regions on the other hand (ID card for election purposes)[267].

[266] For example, the Bertillon system was implemented in France, which consisted in the systematic measure of different body characteristics (arm length, height, etc.) in case of a criminal act. These records were stored on a card to identify first-time offenders and adapt justice decision in case of recidivism. This corresponds to the birth of anthropometrics science. At around the same time, fingerprints started to be used by police forces in South America, Asia and Europe, providing more accurate and individualized biometric profiles than the Bertillon system. It is only late in the 1800s that such fingerprints were scientifically indexed and classified in order to facilitate research and matching procedures. This system of indexation is called the Henry system and is still in use for classifying fingerprints nowadays.

[267] Many developing democracies in emerging countries did not have access to any form of citizenship records (birth certificates, marriage licences, etc.) and credentials that are necessary to control voting procedures at the national level in any form of democracy. Biometrics solutions were thus used in such context in order to rapidly implement an ID infrastructure at the national level.

During the 1990s, developed countries considered new application fields for biometry technologies, including identity frauds, immigration flow, secured access control, etc. In turn, this triggered the development of new types of secure ID credentials taking the form of smart ID cards and then e-passports. The development of new application segments resulted in a real explosion of market demand during the 1990s and a subsequent generalisation of market applications from 2000 onwards. This is reflected in the development of a wide variety of every-day life applications such as logic access control in modern laptop computers or even restricted commercial access to amusement parks (e.g. Disney World has used biometrics to identify season ticket holders since many years). The September 11th attacks only confirmed and further developed this already existing market trend.

Today the major application markets of biometric solutions include ID titles, access control to sensitive sites or areas, border control, logic access to IT network and digital devices, electronic payment and signature and even data encryption techniques[268]. Nonetheless, even if biometrics are in essence a security technology, it is progressively considered by users or operators as a way to provide additional functionalities to systems such as comfort or automation (ambient intelligence), opening the way to the development of commercial applications with large volume potential. However, although new application domains will emerge in the future due to increased biometric market acceptance, access control applications, either physical or logical, will however remain a key application sector in the future.

7.2.2 Overview of main market (customer) segments

Biometric equipment/device/solutions are being used for access control or identification purposes in the following key vertical markets:

- **Financial services**: access to Automated Teller Machines, logic/physical access to restricted areas/systems, electronic locks;
- **Gaming and hospitality**: access control to hotel rooms (electronic locks) or in casinos;
- **High-tech and telecom**: logic access in replacement of passwords or Personal Identification Numbers;
- **Industrial manufacturing**: logic/physical access to restricted areas, workers time records system;
- **Retail distribution**: for time records purpose and physical/logical access control to restricted area/systems;
- **Travel and transportation**: for identification purposes, checking procedures, etc.;
- **Healthcare**: for identification purposes in order to prove the identity of social welfare recipients;
- **Law enforcement**: for identity control purposes and forensic investigation;
- **Military**: logic/physical access to restricted areas/systems;
- **Municipal and State Government**: for civil registration purposes, access to social services, police and healthcare systems;
- **National Government**: *idem* at the national level;

[268] Techniques used to scramble data so the data becomes difficult to unscramble or decipher.

It is obvious that security requirements are different from one market to another. From a device perspective, high level security markets (public vertical markets, finance, transportation, military) may require specific biometric devices development as opposed to general purpose biometric solutions which are implemented in commercial markets (retail, gaming/hospitality, etc.).

Local biometric market characteristics may also differ depending on regional/national cultures and technical expertise, leading to some degree of specialisation from a technological perspective. Indeed, Japan invested early in vein recognition systems and has now the leadership in this domain for two reasons. First Japanese do not feel comfortable with direct-contact technologies such as fingerprints and prefer 'contactless' solutions like vein recognition systems, providing favourable local market conditions to new technological introduction. In addition, vein recognition systems are based mainly on LED and CCD cameras technologies, two domains where Japan holds a leadership position worldwide.

7.2.3 International market profile and market size estimates

Global market breakdown

Estimates from Acuity (see Figure 7.4) and from the US consultancy IBG International Biometric Group (IBG) (see Figure 7.5) indicate a similar biometric equipment/device market size and growth profile in the medium term. These data illustrate a market size for core biometric technologies/equipment of around $3 to 3.5 billion in 2009.

The regional breakdown of the biometric market reflects both the quite recent history of this industry and the type of application that biometry is addressing. The biometric market is concentrated in North America, Asia/Pacific and Europe, which together are estimated to represent close to 75% of biometric industry revenues in 2009 according the International Biometric Group (see Table 7.2). This cumulated market share is however expected to decline slightly to 70% in 2014, due to a decrease of the European market share against other regions (from 21% to 16%). In the meantime, North America and Asia Pacific will maintain their respective market shares.

Table 7.2 Biometric industry revenues by region, 2009-2014 (€ million)

	2009	2010	2011	2012	2013	2014
South and Central America	304.6	395.6	502.2	621.3	754.9	918.2
Asia / Pacific	828.2	1,035.2	1,264.8	1,505.8	1,760.8	2,061.2
Middle East / India	355.9	481	633.5	810.8	1,016.9	1,274.2
Europe	708.4	857.4	1,012	1,160.9	1,304.1	1,461.6
North America	1,030.1	1,320.1	1,654.2	2,020.4	2,424.6	2,913.7
Africa	195.1	267.5	356.9	462	585.4	740.1
TOTAL	**3,422.3**	**4,356.8**	**5,423.6**	**6,581.2**	**7,846.7**	**9,369**

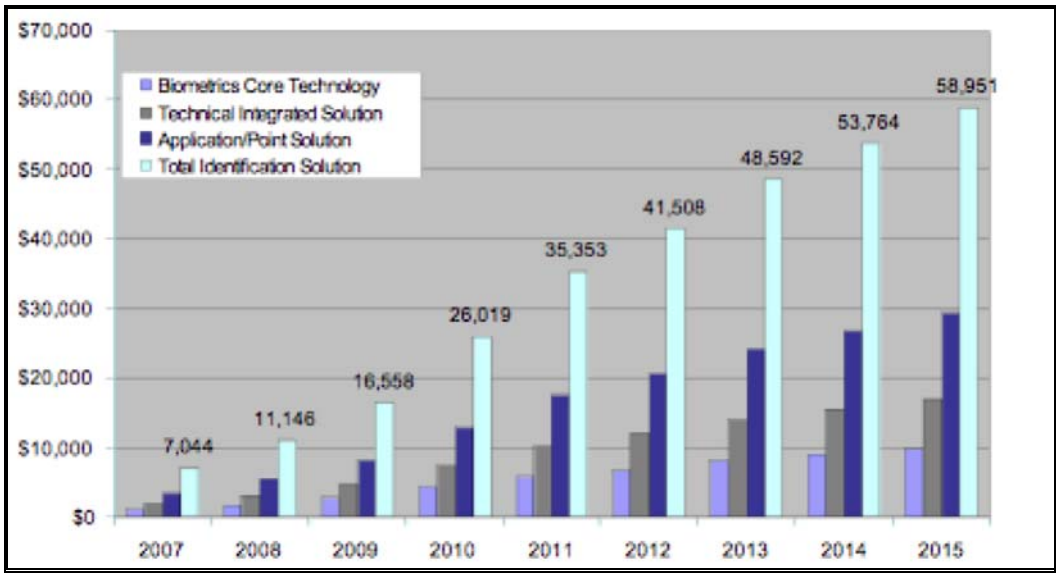
Source: International Biometric Group

Solution / value-added breakdown

Available market estimates strikingly illustrate the predominance of system integration over the device in biometric solutions added value. Figure 7.4 provides estimates of the breakdown of the identification solution market in value terms. These data – from the market research firm Acuity – suggest that the share of biometric product/equipment in total biometric solutions industry will remain limited (15 to 20% of the total industry value) in the medium term compared to application software and integration activities. The larger parts of the added value of a biometric solution consequently lie in non-specific devices like computer systems and infrastructure equipment (IT networks).

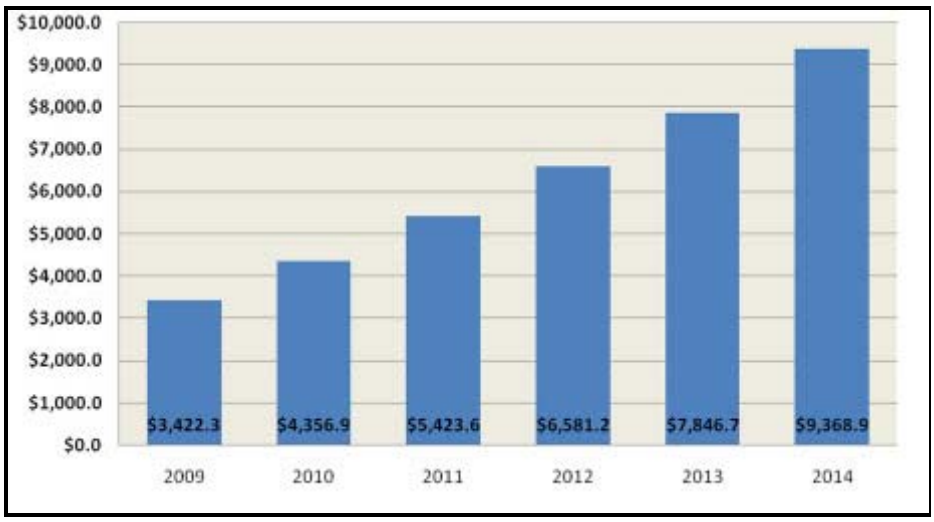
Considering the scope of the present study, it is important to consider that the key stage of added value within a biometric device does not lie in hardware equipment. Indeed, even if biometric sensors can be developed for specific security applications, they are more likely developed for general-purpose market (e.g. sensors developed for use in video cameras), and then implemented in high security level applications. On the contrary, what remains very specific and strategic for the performance of the entire biometric system, in particular in high-end security application dealing with large scale biometric databases, is the biometric characterization/comparison software as well as the encryption algorithm, which secures the very sensitive information that is stored.

Figure 7.4 Biometrics value chain: market size in million USD, 2007-2015



Source: Acuity Market Intelligence

Figure 7.5 Annual Biometric industry revenues in million USD, 2009-2014



Source: International Biometric Group

7.3 Description of the supply (value) chain

7.3.1 General description and overview

Overview of supply structure for electronic security systems

It is important to keep in mind that biometric solutions are only one of a number of technologies that can provide access control. Similarly access control equipment is only one element contributing to the added value of high security systems.

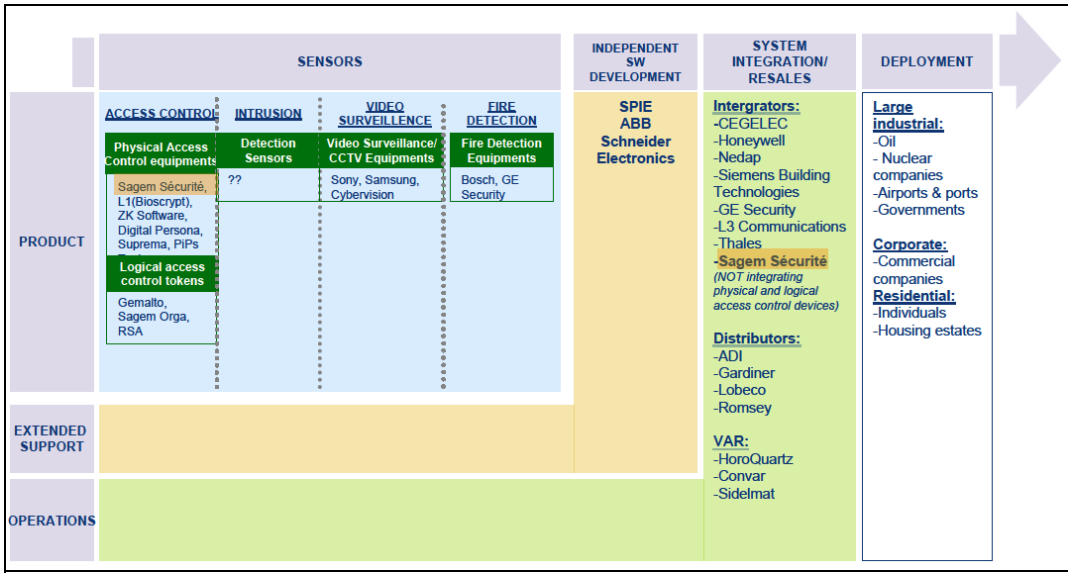
There is a wide variety of industrial players addressing the market for electronic security systems, which can be grouped along three main profiles, namely:

- Sensors manufacturers/developers, focusing on the device side;
- Independent software developers, focusing on extended support activities;
- System integrators/resellers, in charge of equipment integration and operations;

Figure 7.6 provides an indication of the main players in the general value chain for electronic security systems corresponding to each profile listed above. This indicates that products (i.e. equipment, sensors, etc.) and their related technologies only represent a part of the overall added value within the electronic security market. In fact, most of the recurring cost comes from integration tasks of security solutions within an existing information system infrastructure[269].

[269] This statement can be generalised to all types of security equipment, including biometric ones.

Figure 7.6 Electronic security system value chain



Source: Sagem Sécurité

Overview of supply structure for biometric solutions

We can distinguish several types of suppliers including:

- Industrial groups specialised in large public security markets;
- Companies that are specialised in access control systems with relatively low to medium security levels. These companies rely on large distribution networks and mainly address commercial markets;
- Integrators and IT service suppliers providing full security system solutions and dedicated application software that they either develop or customise;
- Small installation service companies using plug & play 'off the shelf' products for consumer markets or small municipalities;
- Technological SMEs specialised in sensors, image processing and complex algorithms.

These are shown in Table 7.3 and 7.4.

The general principle behind this segmentation of suppliers is that it is the large industrial groups that are the providers of large systems with high security and confidentiality of the registered information. Essentially, this type of biometric solution requires the capability to assemble (or access) and store very large biometric datasets that are use for comparison/matching processes through the application of complex biometric engine. The ability to supply this type of application requires very specific skills (encryption, biometric engine, secure IT network, training capabilities, etc.) and there are only a limited number of companies able to address this market on a worldwide basis.

Table 7.3 Typology of suppliers of biometric applications

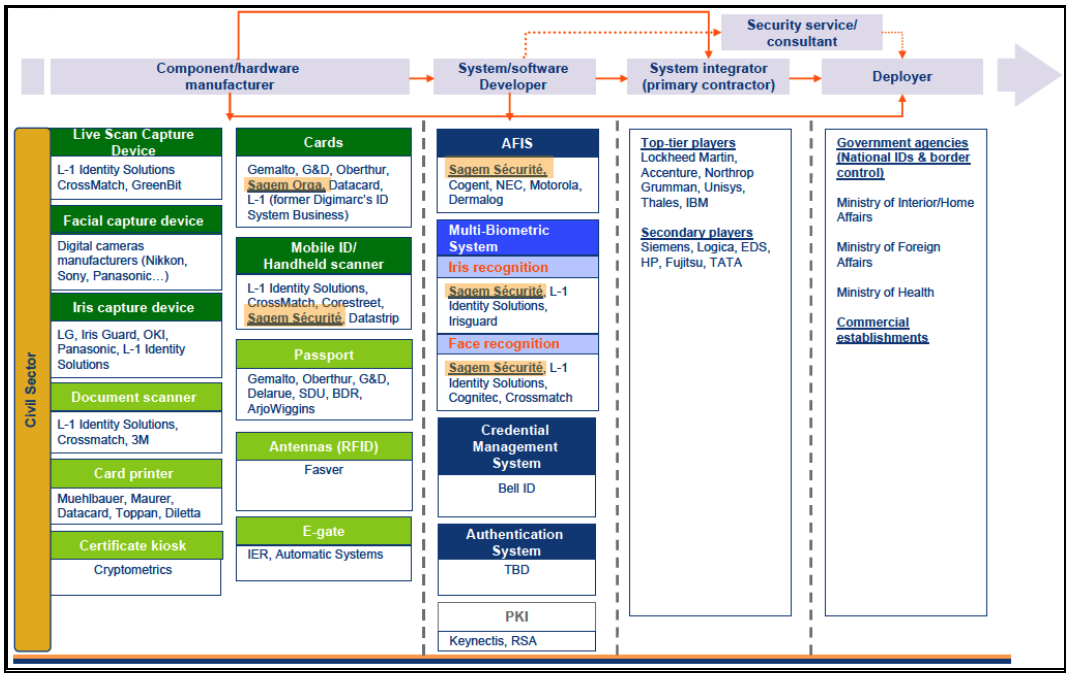
Type of supplier	Degree of specialization	Application type
Solution reseller “plug and play”	Off-the-shelf procurement	Personal application to replace keys or passwords
SMEs, service suppliers	Configuration and installation	Local and low security application
Large Groups	May engage in specific development	Large security systems, centralized

7.3.2 Overview of main market players

There is a wide variety of player profiles within the biometry industry, which ranges from ‘off-the-shelf’ product offerings to specific integrated solutions, from service or technological SMEs to large industrial groups. Table 7.4 provides a list of identified suppliers of biometric equipment including both hardware and software suppliers. Among the players identified in this list, many of them address not only the security market but also solutions for other markets such as comfort and automation. The list also highlights the dominant position of US suppliers in the biometric industry.

Figure 7.7 maps the main market players addressing large ID management systems within the supply chain segmentation

Figure 7.7 Main players in the ID management systems value chain



Source: Sagem Sécurité

Main providers of high-end biometric solutions

In terms of the main players addressing the high-end segment of the security biometric solutions (see also Figure 7.7), there are four established leaders worldwide for high-end biometric applications for public market (AFIS):

- Sagem Sécurité (France) – see Table 7.5;

- NEC (Japan) – see Table 7.6;
- Cogent (US) – see Table 7.7;
- L1 Identity Solutions (US) – see Table 7.8.

Historically, the US company Printrak was the first provider for AFIS solutions. The Japanese company NEC took the leadership at the beginning of the 1980s. The US-based Morpho Systems entered the market by the middle of the 1980s and took the leadership by the mid 1990s thanks to key contracts won within the US market (New York State identification system, FBI IAFIS) and numerous successful businesses outside the US as well.

Printrak has then been purchased by Motorola as well as Morpho by Sagem during the 1990s. The latter has recently increased its market leadership through the acquisition of its US competitor Motorola Biometrics in April 2009 to form a new division called MorphoTrak (US-based).

Geographical dimensions of the supply chain

From a regional perspective, a majority of suppliers are localised in the US, reflecting its large market size. The US is also home to the largest system integrators for security application with companies such as Lockheed Martin, Northrop Grumman, Accenture or Unisys, coming from the defence or IT industries.

The Japanese biometric supply chain demonstrates some specialisation in component/hardware manufacturing in particular cameras but is rather limited in other value chain stages with the exception of NEC who remains a key player in the AFIS market. Most of Japanese players concentrate on low-end commercial applications of biometrics.

Finally, the European supply chain has a few (but important) players in the high end segment of the biometry industry including the market leader Sagem Sécurité - with a global market share in high end segments that is somewhere in excess of 50% - as well as specialised SMEs like Dermalog (Germany), Cognitec (Germany), Iris Guard (UK) and Green Bit (Italy) as well as mid-size players like Daon (US company but Irish origin) and Automatic Systems (Belgium) and also larger players such as Thales (France); though the biometric activities of Thales are relatively limited. Contrary to the US supply chain, which addresses both low-end and high-end market segments, Europe tends to be more focused on high-end market segments.

New entrants

As mentioned previously, entry barriers are high in the high-end security application segment of the biometric industry. Most of the new entrants are penetrating the biometric market through low-end and mid-end application mostly in the commercial sector, which generates enough volumes to provide fast return on investment. New entrants generally concentrate on middle ware and purchase existing technologies to build applicative solutions for their customers. Generally, new technological development can still be performed by new entrants in the biometric industry, specifically in the domain of biometric characteristics acquisition (image acquisition process, security of acquisition against decoy, etc.)

Table 7.4 Typology of suppliers of biometric applications

Company name	Type of market	Company origin	Type of supply		
			Component	Systems	Integrator
AuthenTec	AuthenTec is the world's leading provider of fingerprint authentication sensors and solutions to the high-volume PC, wireless device, and access control markets, with more than 45 million sensors in use worldwide.	China (Shanghai)	X		
Accenture	Accenture is a system integrator of security software solutions	USA			X
Automatic Systems	Automatic Systems, subsidiary of the group IER, is a leader in physical access control and security equipment, they are specialized in the development of e-gates	Belgium	X		
Cogent Systems	Government, law enforcement, commercial	USA		X	
Cognitec Systems	Face recognition technology. The main market today is security related, but there are a variety of applications emerging related to personal use, convenience, productivity enhancement and more.	Germany	X		
CrossMatch	Cross Match Technologies, Inc. is a leading provider of high-quality interoperable biometric identity management systems, applications and services. Cross Match develops Live Scan Capture Devices, document scanners and face recognition systems.	USA		X	
Cryptometrics	CryptoMetrics is a leading provider of biometric devices and software. They develop face recognition products, fingerprint recognition products and certificate kiosks.	USA	X		
Corestreet	CoreStreet develops software security solutions, Mobile ID and Handheld scanner systems	UK	X		
Daon	Daon is a leader in software and biometric identity services. It addresses both government and commercial market as well.	USA	X	X	
Datastrip	Datastrip is a market leader in providing handheld personal identification and verification products, Mobile ID and Handheld Scanners.	USA	X		
Dermalog	Dermalog is specialized in AFIS systems for civil and criminal applications, providing both software and hardware solutions.	Germany		X	
DigitalPersona	Markets of individual, family and small business users. Fingerprint.	USA	X		
EDS	EDS, an HP company, is a leading global technology services provider and integrates security systems.	USA			X
Fujitsu	Fujitsu provides biometric solutions on top of its computer solutions. Fujitsu is in particular positioned on vein recognition (hand) and addresses a large market scope: government, finance, health.	Japan			X
GreenBit	Green Bit is a leader in the development and realization of optical dactyloscopic systems for high-security applications through fingerprint recognition. It also conceives live scan capture devices.	Italy	X		

Company name	Type of market	Company origin	Type of supply		
			Component	Systems	Integrator
Hitachi	Hitachi is present on vein recognition (finger) for both logical and physical access control solutions. Hitachi has a partnership with the UK group Easydentic for sensors development.	Japan	X		
HP	Integrates security software solutions (cf. EDS)	USA			X
IBM	IBM leader on its market, is also integrating security systems	USA			X
ImageWare Systems	Identity management, particularly in the segments of biometrics, public safety, secure credentialing and controlled access.	USA	X		
Iris Guard	IrisGuard is specialised in the deployment of Iris Recognition systems where high number of people needs to be checked in real-time.	UK	X		
L-1 Identity Solutions	L-1 Identity Solutions delivers the full range of solutions (finger ;palm, iris and facial and multimodal and services required for solving the issues associated with managing human identity	USA	X	X	
LG Electronics	Present in computer, mobile telecom, domotic, LG is also present in access control solutions related to these markets (USB key including biometrics, physical access solutions, etc.)	South Korea	X		
Logica	Logica a leader on its market and among its several activities, it also integrates security systems solutions	UK			X
Lockheed Martin	Lockheed Martin is a system integrator of first rank in the security market	USA			X
Lumidigm	Lumidigm has developed a multispectral imager that is able to collect additional information from below the surface of the skin.	USA	X		
Motorola	Motorola biometric activity (70 M$) has been acquired by Sagem Securite in 2008. This activity includes different professional solutions for governmental services.	USA	X	X	
NEC	NEC proposes biometric solutions for logic access control to computers and networks for both consumer and private companies. NEC also has a partnership with Daon for large governmental systems application (multimode border control in Japan)	Japan		X	
Nikkon	Nikkon also develops facial capture devices	Japan	X		
Northrop Grumman	Lockheed Martin is a multinational aerospace manufacturer, global security and advanced technology company. It integrates security systems.	USA			X
Nuance	Nuance specializes in application for emergency call centres (vocal synthesis).	USA	X		
OKI	OKI develops facial capture devices	Japan	X		
Panasonic	Panasonic provides facial capture devices	Japan	X		
Precise Biometrics	Fingerprint solutions, ID Cards, …	Sweden	X		
MORPHOTrak (Sagem)	Incorporated in April 2009, mainly providing fingerprint, facial and iris solutions.	USA		X	
Sagem Sécurité	Sagem sécurité is present in access control component, equipment and associated systems.	France	X	X	

Company name	Type of market	Company origin	Type of supply		
			Component	Systems	Integrator
Schlage	Schlage is present in intelligent locks for the residential and professional market. Schlage includes biometric sensors to its locks.	USA	X		
Siemens	Places itself on the security sector as system integrator for security software solutions	Germany			X
Sony	As a leader on the digital camera market, Sony develops also facial capture devices.	Japan	X		
TATA	TATA is a system integrator of security systems software solutions.	India			X
Thales	Thales is a second rank player in this sector and provides security solutions as a system integrator.	France			X
Unisys	Unisys Corporation is a provider of information technology services and programs. The company offers its system integrator services in the security field.	USA			X
UPEK	STMicroelectronics spin-off for fingerprint sensor development (TouchChip).	USA	X		
3M	Among its broad range of activities 3M is also a major player in the security field by providing document-scanning solutions.	USA	X		

Table 7.5: Sagem Sécurité: Basic company indicators

SAGEM SÉCURITÉ (FR)				
Main indicators	**SAFRAN Group**		**Sagem Sécurité**	
	2007	2008	2007	2008
Turnover	€10.2bn	€ 10.3bn	€ 670m	€ 695m
Profit	€ 406m	€ 256m	N/A	N/A
R&D budget	€ 620m	€ 439mm	N/A	N/A
Number of employees	54,224	54,493	N/A	3,500
Description of the company				
Sagem Sécurité, part of the SAFRAN Group, is the world leader in digital fingerprint biometrics and a leading player in multibiometric technologies, smartcards, secure transactions and ID management solutions. These capabilities allow it to meet the emerging security needs of individuals, companies and states. Integrated systems and equipment by Sagem Sécurité are used worldwide to ensure transport safety, as well as protect high-value infrastructures and electronic transactions. Sagem Sécurité offers products and solutions for local protection, as well as nation-wide security systems, delivered to more than 60 different countries.				
Main products and technologies				
▪ Biometric identification systems for police forces and civil agencies (in particular AFIS – Automated Fingerprint Identification System) ▪ Identification documents: national ID cards, driver licenses, e-passports and e-visas, ▪ Smartcards (SIM, bank cards, ID, health care) ▪ Healthcare, betting and gaming terminals ▪ Biometric terminals ▪ Physical and logical access control ▪ Road safety systems and equipment ▪ Automated border control solutions				

Source: http://www.sagem-securite.com and 2008 Annual Report Safran Group (http://www.safran-group.com)

Table 7.6: NEC: Basic company indicators

NEC (JP)		
Main indicators	**NEC**	
	2007	2008
Turnover	€ 28.9bn	€ 30.3bn
Profit	€ 56.6m	€148.8m
R&D budget	N/A	N/A
Number of employees	N/A	±23,500
Description of the company		
NEC is a leading global manufacturer and service provider of telecommunication, computer and electronic devices. NEC Group includes IT/Network Solutions, Mobile Personal Solutions, Semiconductor Solutions, System LSI, IC & discrete Semiconductor, Compound Semiconductor. NEC offers also biometric solutions for identification. NEC maintains a worldwide network of subsidiary companies, which includes operations in Europe where NEC performs various sales, manufacturing, and R&D functions.		
Main products and technologies		
▪ AFIS ▪ Face Recognition ▪ ID Management ▪ Fingerprint scanner ▪ Fingerprint matching		

Source: http://www.nec.com/

Table 7.7: Cogent: Basic company indicators

COGENT SYSTEMS (US)		
Main indicators	**Cogent Systems**	
	2007	2008
Turnover	€ 77.2 m	€ 85.5m
Profit	€ 20.9m	€30.7m
R&D budget	€7.3m	€ 10.1m
Number of employees	N/A	365
Description of the company		
Cogent is one of the 3 world leaders of Automated Fingerprint Identification Systems and other fingerprint biometrics solutions to governments, law enforcement agencies and other organizations worldwide. For over eighteen years, Cogent has researched, designed and developed fingerprint biometric technologies that incorporate advanced concepts in fluid dynamics, neural networks, image enhancement, data mining and massively parallel processing.		
Main products and technologies		
▪ Government : biometric identification (AFIS, PMA, Mobile Identification), Fingerprint scanners, fingerprint services, ID Management and cards ▪ Law enforcement (mobile, live scan) ▪ Commercial physical and logical access control		

Source: http://www.cogentsystems.com and 2008 Annual Report

Table 7.8: L-1 Identity Solutions: Basic company indicators

L-1 IDENTITY SOLUTIONS		
Main indicators	**L-1 Identity Solutions**	
	2007	2008
Turnover	€ 284.3m	€ 382.9m
Profit (loss)	€ 12.9m	(€ 373.3m)*
R&D budget	€ 13.5m	€ 17.2m
Number of employees	N/A	2,264
Description of the company		
L-1 Identity Solutions delivers the full range of solutions: finger, palm, iris, facial and multimodal biometric and services required for solving the issues associated with managing human identity. L-1 provides systems and solutions that empower the identification of individuals in large-scale identity management programs. In 2008, assets impairments consist of goodwill of $430.0 million and long-lived assets of $98.6 million, principally intangible assets recorded in connection with acquisitions.		
Main products and technologies		
▪ Live scan systems and services for biometric data capture ▪ Mobile solutions for on-the-spot ID ▪ Facial screening ▪ Single/dual fingerprint readers ▪ Next-generation multi-biometric identification solutions ▪ With a global network of partners such as leading system integrators, defence prime contractors and OEMs, L-1 Identity Solutions serves a broad range of markets including federal, state and local government, law enforcement, financial services, border management and travel.		
** The results (loss) have been materially impacted by acquisitions, mainly the one of Digimarc Corporation*		

Source: http://www.l1id.com and 2008 Annual Report

7.3.3 Technology aspects

From a technological perspective, most of the added-value in high-end biometric identification solutions lies in the biometric engine, providing the system with fast and reliable datasets classification and comparison capabilities over a large scale population. This 'know how' is essentially based on anthropometry and software design rather than hardware, and is specific to the biometric modality under consideration (fingerprint, vein, iris, face, etc.).

7.3.4 Component supply

From a component perspective, it is worth noting that past (i.e. before year 2000) specific hardware components (sensors, image processors, etc.) were traditionally developed specifically for biometric application. This is not the case anymore as solutions based on standard hardware have since proved their ability to reach similar and even superior performances, providing in addition safer and more reliable procurement sources over long time periods.

The key component within a biometric system remains the sensor which is in charge of capturing the biometric modality for both registration and verification purposes. Although dedicated technologies may be used for such piece of hardware (fingerprint sensors, dedicated digital cameras, etc.), standard digital cameras or sensors based on commercial

semiconductor technology are overwhelmingly used in biometric systems. Japan is at the forefront of this industry.

As these types of components are also deployed in a wide variety of consumer applications (mobile phones, audio/video equipment, etc.), there is no apparent threat from a security of supply perspective.

7.3.5 Equipment and sub-systems

Equipment and sub-systems correspond to the card readers, scanners, kiosks, etc. that are necessary in order to implement a complete biometric solution. These equipment and sub-systems are developed by equipment integrators so as to match with one specific application and in order to comply with specific operational constraints (police forces equipment, fixed kiosks in an embassy or an airport, etc.). These suppliers are also in charge of developing the biometric software, which will perform data acquisitions and comparisons within the system as well as application software.

Depending on the equipment integrator strategy, manufacturing[270] can be either delegated to sub-contractors of the electronic equipment industry, or kept internal, which is the case of the world leader Sagem Sécurité. Generally, North American suppliers tend to sub-contract their production contrary to Japan, where vertical integration is still important, European position being between these two approaches.

7.3.6 Integration and customisation

System integrators are the primary contractors for large biometric solutions programs and concentrate most of the market value (high recurring costs). However, their added value does not correspond specifically to the security industry but rather to their ability to handle large integration projects. The key stage of the biometric supply chain for large programs with high security constraints rather lies on systems/software developers or equipment/product integrators.

7.3.7 Related services

In addition to integration activities, the biometric market for security applications also generates large service activities:

- **Management of operations**: due to the recent implementation of biometric technologies in some applications, human operators are most of the time associated to identity controls in order to facilitate technology acceptance. In addition, operators play a critical role in enrolment/registration procedures, whose accuracy is essential in order to ensure the performance of the entire identification management system;
- **Computer and systems update**: identification solution are heavily relying on IT based devices and systems benefiting from constant performance upgrades that requires in turn to update the security infrastructure on a regular basis;

[270] It should be kept in mind that equipment and sub-systems only represent 15% to 20% of the entire added value of the identification solutions market.

- **Maintenance and overhaul**: as any security breach may lead to disastrous consequences in high security applications, maintenance and overhaul activities play a critical role especially when biometric solutions are being implemented to increase the degree of automation of an identity or access control procedure;
- **Training**: training activities are important not only to familiarise and increase the efficiency of operators, but also more specifically in enrolment procedures in order to increase the quality of biometric templates and therefore the overall performance of large scales authentication/identification solutions.

7.3.8 Linkages to final (end user) markets

The interconnections with the value chain are rather complex and although system integrators continue to play a critical role, we can notice that equipment and software integrators are also in direct contact with the end-user. Technology choice cannot indeed be fully delegated to the system integrator considering its importance for the performance of the complete security system. This is a key element to understand the market organisation and the biometric equipment/product suppliers' strategies (cf. Sagem Sécurité acquisitions).

7.3.9 Overall assessment of the supply chain

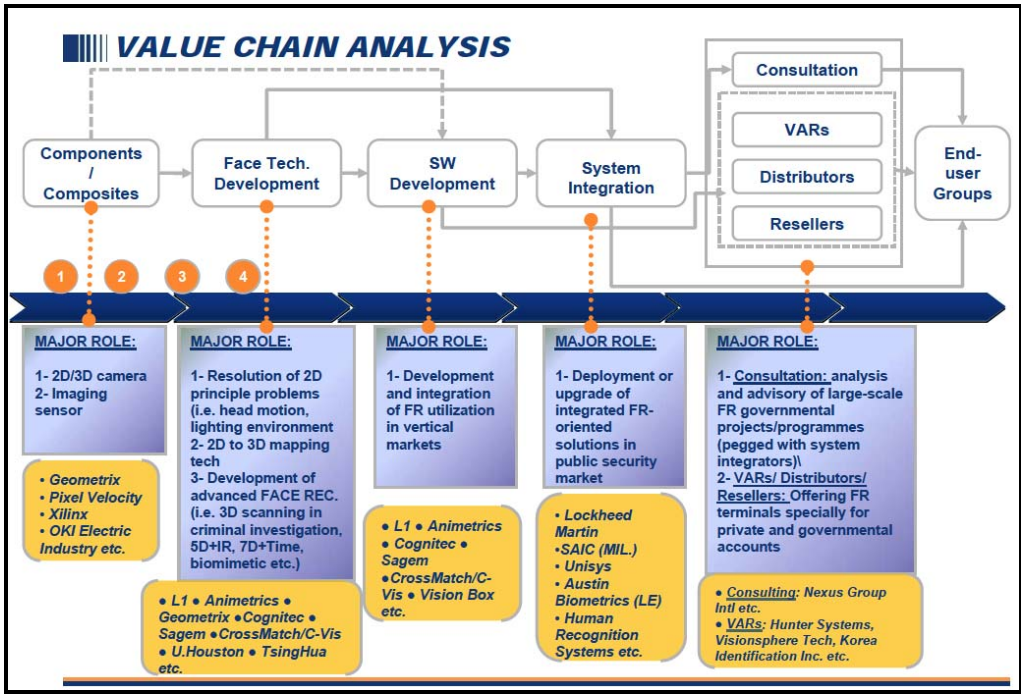
The supply chain for biometric solutions involves a lot of players with numerous interactions between them. Figure 7.8 illustrates the current value chain of facial recognition systems. It illustrates the interconnections between the various players - from the sensors/components manufacturers to the final end-user- that are required in order to integrate a new biometric technology within a larger security infrastructure.

In terms of the key characteristics of the supply chain, the following may be noted:

- From an equipment perspective, the key stage of the biometric value chain lies in the development of the registration/comparison/matching systems and algorithms, which is the responsibility of the equipment integrators (the pure biometric players).
- Application software development may be localized within equipment integrators or niche specialists of one vertical application (airport security, etc.) or biometric technology (face recognition, etc.).
- System integrators are in direct contact with the end-users, providing complete security infrastructure including biometric identification systems.

In terms of their general organisation of supply chains and the positioning of players therein, the overall situation of the supply chain(s) for biometrics solutions is seen as relatively stable. For example, the recent acquisition of GE Homeland Protection by Sagem Sécurité is not seen as indicating a strategy of Sagem that is aimed at competing with large system integrators. Rather, it points to the reinforcement of Sagem's position within the global identification market, both targeting individuals as well as goods.

Figure 7.8 Current value chain of facial recognition systems



Source: Sagem Sécurité

7.4 Main trends and developments

7.4.1 Market trends and developments

The demand for biometric equipment and solutions for security application is driven by increased security needs in both the public and the commercial markets. The major benefit of biometric based security solutions compared to other forms of people identity controls essentially lies in the level of security and trust placed on the procedure. This is notably higher for controls based on biometric solutions, which are much more difficult to counterfeit or steal. This can to some extent explain why justice, law enforcement and more broadly governmental demand have promoted biometric technology and market development since its origin. In fact, if we consider the change over time in demand for biometric equipment and solutions, this has seen a development of the use of biometric applications from 'justice' to 'police forces' and eventually to commercial applications. Thus, contrary to many other security industry branches, the development of biometry has clearly been based upon, and financed by, civil applications rather than defence ones.

Public versus Commercial applications

It is expected that the turnover generated by emerging applications (information systems access, e-commerce, telephony, physical access and surveillance) should eventually surpass traditional public sector market, but only in the longer term. According to estimates from the International Biometric Group (IBG), governmental applications (law enforcement, military, state and municipal government, national government) represent 70% of the total biometric market in 2009, and will still have an equivalent market share in 2014. Indeed, IBG estimates show that the civil ID market remains by far the leading application for biometric technologies, representing 40% of the global demand in 2009

and up to 50% in 2014 as a result of predicted massive deployment of national government ID programs across the world.

The biometric equipment/product market for public security application is influenced by two contradictory factors. On one hand, identification needs is increasing in order to fight against social fraud, terrorism and increase the control of immigration flows. But, on the other hand, biometric technologies suffer from low citizens' acceptance fearing the development of a 'Big brother' society[271]. In this respect, European countries seem particularly conservative compared to other regions and the USA, in particular.

The lack of public acceptance may partly be explained by the fact that biometry has only recently entered into the public consciousness due to the deployment of flagship large scales programmes, in particular in the US, (e.g. the US-VISIT program consisting in capturing the fingerprints of any entrants into the US). This further stimulates the development of new applications for biometric technologies, which are in turn benefiting from increased market acceptance worldwide.

Another limitation to market development is the fact that public security market is a compilation of local solutions adopted at the country level with a lack of standardization and critical size.

In the longer run, the development of the internet and e-business/commerce will further stress the need for increased 'online security' and represent long term drivers for the development of commercial biometric applications. Security is also required for e-work, data exchanges and sharing between customers and suppliers, OEMs and sub-contractors, all relying on both internal and external access to private information systems and consequently the development of new access control strategies relying on secure identification solutions. The development of mobile communication devices is also contributing to the creation of additional security needs[272].

Security is not however the only driver of commercial biometric market development. Biometric technologies can also increase user comfort in dedicated application. New concepts are currently emerging in order to use biometric screening to adapt the environment to the user (dedicated systems settings in car vehicles or customized advertisement, etc.). These new types of applications, also referred to as ambient intelligence, may stimulate market development for biometric equipment/product in the future.

Public application

The biometric equipment/product market for public security application is influenced by two contradictory factors. On one hand, identification needs is increasing in order to fight against social fraud, terrorism and increase the control of immigration flows. But, on the other hand, biometric technologies suffer from low citizens' acceptance fearing the

[271] This lack of acceptance essentially concerns public sector applications as such types of solutions, to be fully operational, rely on the development of centralised biometric databases.

[272] For example, a survey by Toshiba has indicated that 90% of top managers and CEOs in Europe are saving sensitive and even confidential pieces of information in their mobile devices. Among them, 22% state they already have lost their personal devices.

development of a 'Big brother' society[273]. In this respect, European countries seem particularly conservative compared to other regions and the USA, in particular.

The lack of public acceptance may partly be explained by the fact that biometry has only recently entered into the public consciousness due to the deployment of flagship large scales programmes, in particular in the US, (e.g. the US-VISIT program consisting in capturing the fingerprints of any entrants into the US). This further stimulates the development of new applications for biometric technologies, which are in turn benefiting from increased market acceptance worldwide.

Another limitation to market development is the fact that public security market is a compilation of local solutions adopted at the country level with a lack of standardization and critical size.

7.4.2 Technology trends and developments

Up to now, biometric equipment/solutions have not created a real breakthrough in identification control procedures, neither for control operators nor for individuals. The development of new biometric technologies is thus concentrating on these issues in order to facilitate market acceptance.

'Trace-free' technologies

Fingerprint technology has a dominant position for high-end biometry market and is expected to remain so over the medium term due to the inertia of public biometric applications. However, fingerprints leaves traces on many substrates, which could in turn present a security breach and limit future market growth for applications (except criminal applications) due to constraints from national regulatory bodies, in particular for large and centralised systems required for global ID management applications like border control. Industrial players are therefore looking to develop new 'trace-free' identification techniques like iris recognition or vein recognition technologies.

Non cooperative (transparent) controls – Facial recognition

Market acceptance also relies on the development of transparent biometric control technology, also called non-cooperative controls, allowing security operators to verify people identities without passing through a formal identification procedure (kiosks, scanners, etc.). The ability to perform identity controls 'on the go' is certainly a future market expectation.

Facial recognition is one technology that allows 'on the go' ID controls by leveraging existing video-surveillance infrastructure already in place for real time or delayed identification controls (using camera records). This technology is however still far from the level of performances reached by other biometric techniques and still requires additional development investment.

[273] This lack of acceptance essentially concerns public sector applications as such types of solutions, to be fully operational, rely on the development of centralised biometric databases.

Iris recognition is also a technology, which could allow on-the-go control as demonstrated in the US by Sarnoff Corporation (Iris on the Move).

7.4.3 Production trends and developments

Market leaders and market access

From a market perspective, the clear number one market for high-end biometric security application is the USA due to easier market acceptance and large investment programs in biometric equipment. The amplitude of current programs like US-VISIT or the modernization of FBI biometric equipment is reaching very important scales and pushing the biometric technology performances to the limit (FBI currently stores 70 million biometric profiles in its database).

National industrial policy is instrumental in biometric market development, especially in the high-end segment of the market. The US is pushing for the development of one indigenous local player, namely L1-Identity Solutions. China is adopting a similar strategy with the company Cogent (US based but Chinese ownership)[274].

National markets, although opened to international competition, heavily rely on political decision power. It is for instance very difficult for a European company to win a bid in the US without having a US partner (generally a system integrator). Similarly, the fast developing Chinese market is closed to international competition and reserved to local players like Cogent who seized this opportunity to rapidly become a world-class competitor.

Players' strategies

Biometric solutions are only one part of global security systems within large public market such as border control, criminal forces, etc. Biometric equipment/product suppliers are thus only capturing a small part of the complete value chain. As the security industry becomes more mature, some market leaders may enter into new types of growth strategies through acquisitions in order to consolidate product/solution portfolios and better address key security vertical markets with complete solutions offerings.

The recent acquisition of GE Homeland Protection (leader for CBRNE equipment) for $US 580 million by Sagem Sécurité in April 2009 tends to demonstrate this market shift. Sagem is now in a position to propose to large system integrators and end-clients complete identification solutions covering both individual and goods identification systems as well as the corresponding optimised control procedures.

7.4.4 Overall assessment of trends and developments

The high-end biometric market is characterized by long technology and market adoption cycles as well as high entry barriers. As a consequence, no major disruptions are expected in the medium term from either a technology, application, sector or geographical perspective.

[274] Although US-based, COGENT has apparently some links with the Chinese administration.

Technology and application

Fingerprints, including AFIS and Live-Scan equipment categories, are expected to remain the dominant biometric technology as they are already massively used within major public application sectors such as law enforcement and national governments. Face recognition will remain the second biometric technology as it will increasingly be used in civil ID applications as well as surveillance applications. Iris recognition should be gradually deployed for secure transaction, access control as well as identification application, due to its superior performance with respect to traditional fingerprint solutions. Finally, vein recognition is considered as a potential alternative to fingerprint for civil and commercial application where traces can represent a limit to market acceptance.

Regional market development

From a regional perspective, the US and Asia/Pacific will remain the largest end markets for biometric technologies thanks to higher market adoption. By contrast, Europes market share is expected to decline in the medium term, due to cautious national policies and public acceptance with regard to biometry. According to the International Biometric Group, European biometric market share in 2009 was estimated at 21% and is expected to decline to 16% by 2014.

Commercial vs Public applications

The growing development of commercial applications within the biometric market is not expected to have a significant impact on the high-end security segment of the market. Indeed, the critical stages of the value chain are rather different from commercial applications essentially involving 1:1 or small 1:n verification procedures compared to large scale public markets relying on large 1:n identification systems.

7.5 Regulatory conditions and development

7.5.1 International, European and national security-related regulatory conditions

EU regulation on personal data protection

The 95/46/CE Directive aimed at providing a European framework to the protection of individuals with regard to the processing of personal data and on the free movement of such data. European member states have thus translated this directive into their national legal corpus. In addition, member states are coordinating each other within the G29 group that has been established by Article 29 of Directive 95/46/EC.

G29 is an independent European advisory body on data protection and privacy. Its mission has been laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC, as summarized below:

- To provide expert opinion from member state level to the Commission on questions of data protection;
- To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities;

- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy;
- To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

European authorities thus put biometric under severe control to prevent the development of ID spoofing. Biometrics, contrary to any other ID, is not being issued to the holder nor chosen by him; it is created by the holder's body as a permanent signature, which cannot be modified in case of a security breach. As a consequence, capturing biometric data and/or registering them in a database for civil or commercial applications require exceptional measures and guarantees to protect the holder.

EU regulation on biometric passports and visas

From a regulatory perspective, the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States has harmonized biometric passport characteristics in Europe. Since August 2006, all passports delivered in Europe contain a wireless smartcard storing a digital image of the holder face (compatible with ICAO standards); these are the 1st generation of e-passport in Europe. Since June 28th 2009, 2nd generation of biometric passports are being delivered in Member States, integrating fingerprints in addition to facial image.

This European position has been driven by the regulation put in place in the USA following the September 11th attacks, requiring a biometric authentication control for any entrance of a European citizen within the USA (biometric information are stored by the USA during 75 years, building *de facto* a gigantic biometric database). The same type of control in Europe remains dependant on the position of each national authority. Currently only pilot test projects have been implemented in some European countries.

In addition Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). The European Visa Information System VIS and its biometric engine the Biometric Matching System should be operational in 2009 with the obligation for Schengen countries to connect to the system before January 2012.

European visas do not concern European citizens directly, which is a factor in their use as a first step for the diffusion of biometry for authentication and identification purposes within Europe. The Regulation includes biometric information sharing procedures between Member States and, as such, VIS deployment potentially offers the European biometric industry an opportunity to test large scale solutions in "real life" conditions[275].

[275] It is unclear whether industry will be allowed to use this database for test purpose, and current intentions seem to be that they will not be able to do so. However, VIS will provide the largest database for biometric in Europe.

Role of national authorities

In Europe the most influential national authority is the French one, represented by the CNIL (*Commission National Informatique et Liberté*). Its approach with regard to biometric systems authorizations is the following:

- Distinction between personal use which does not require any authorization, and collective use;
- Distinction between identification (1:n) and authentication (1:1);
- Each process including biometric data management is subject to prior authorization. Such authorization concerns a specific application and can only be delivered to the people/body in charge of the corresponding process implementation/operation. Therefore a solution/product authorization cannot be issued a priori;
- Some product/solution categories can however benefit from dedicated (and more simple) authorization procedures (unique authorization) like in France where only a simple conformity declaration is required in the following cases[276]:
  - Hand recognition solutions for access control application in school restaurant/self/cafeteria or in private companies for working hour/lunch break control procedures, etc.;
  - Access control systems in private companies based on fingerprints recognition, which do not involve any central database. In such systems, each employee has a specific card containing its personal biometric data for comparison purpose;
- Some dedicated measures may be taken concerning product/solutions with biometric traces like fingerprints that can easily be stolen (glasses, doors, etc.) for data spoofing purposes. Dedicated measures may also restrict the deployment of solutions including data recording procedures;
- In France, the CNIL authorizes the implementation of such systems if they comply with the following:
  - The system shall only be used for a limited set of people to control a clearly defined and restricted area, representing a serious security threat that goes beyond the direct interest of the company/organization. This may include people, goods as well as information integrity (nuclear power plant access, vaccine production plant, Seveso 2 sites, etc.)
  - Proportionality of the implemented solution with respect to the corresponding threats (application + privacy);
  - The system shall provide a high performance identification/authentication solution as well as all guarantees with respect to the protection of personal data;
  - Users shall be informed according to the law 'Informatique et libertés' and labour code if appropriate;

It is important to notice that the role of national authorities can be important in biometric solution development stages as they can be directly involved with industrial companies during the development of product/technology experimental systems. For example, the CNIL has in France given its authorisation in 2007 to engage R&D programs in the field of Facial Recognition. While in 2008, the CNIL has given its authorization in 2008 to the first deployment of finger veins and voice recognition solutions after having conducting similar technical expertise on R&D programs in order to ensure that such systems do not

[276] An on-line procedure has been implemented in France by the CNIL for such simplified authorization

contain any specific threats in terms of data protection and ID spoofing[277]. Such programmes are also a way for national authorities to further develop their understanding and expertise of new biometric technologies.

As a conclusion, we can say that European national authorities are today limiting the development of the biometric market but citizen acceptance also remains an important barrier in Europe for the biometry market development. Overcoming public acceptance issues might require more effective communication to emphasise the use of biometrics as a way to increase the efficiency and comfort of already existing security procedures rather than as brand new security processes.

7.5.2 Industry and market-based standards

Since the 1990s, the US has attempted to structure the biometric supply chain by setting up the Biometric Consortium, a grouping of all major market stakeholders under the joint presidency of NSA and NIST (National Institute for Standards and Technology).

This strategy has been further developed following September 11th attacks and the US decision to make of biometry a key 'sovereignty' technology. This has led to the development of mandatory certification processes and clearances throughout the supply chain with a similar approach to the defence industry, including industry liability containment through the Safety Act.

From a regulatory and standardisation perspective, the US has adopted an aggressive approach to identification management and controls following the September 11 attacks. As of April 2007, seventeen American national biometric standards were published as ANSI INCITS (International Committee for Information Technology Standards). These standards are being introduced in the market through new US regulations, the most important being FIPS 201 for federal and governmental security applications based on US Personal Identity Verification (PIV) product standard, and TWIC for port security

Standard bodies

The main international standardisation bodies for biometry are:

- ICAO: in particular its standard for Machine Readable Travel Documents (MRTD)[278]
- ISO SC17 and SC37: for the definition of interoperable biometric templates

In the US, the main standardisation bodies for biometry are:

- NIST: in particular for fingerprints acquisition procedures and interoperability issues;

[277] For voice finger veins recognition, the CNIL considers that such systems provide an additional level of security compared to fingerprint recognition as they are based on a 'trace-free' solution. This is in particular true for large systems including a centralized database.

[278] Since the late 1990s, ICAO has worked on the definition of biometric format standards to be integrated in next generation travel document. This work had led to the current standard adopted in June 2002 (face: mandatory, fingerprints & iris: optional). The role of ICAO in travel documents standards is important for ensuring interoperability, and this is why they have been involved in defining how to include biometry within documents. It is not a biometric standard per se, but rather a standard for implementation of biometry.

- Biometric Application Programming Interface: for the definition of biometric middleware
- ANSI INCITS

Through performing regularly competitive assessments of biometric technologies, NIST (National Institute for Standards and Technology) has become a world reference for the assessment and adoption of biometric technologies and products. The following statement in the NIST website illustrates the US approach to biometric standardisation:

> "For decades NIST has been involved with the law enforcement community in biometric testing and standardization. In the past seven years, NIST has intensified its work in other aspects of biometric standardization working with consortia & other fora. Post 9/11, NIST worked in close partnership with other U.S. government agencies and U.S. industry to help establish formal national and international biometric standards development bodies as the best environments to support deployment of standards-based solutions and to accelerate the development of the required voluntary consensus standards. Many government and commercial applications, including homeland security and the prevention of ID theft, are requiring strong personal verification and identification applications. These requirements include high performance, interoperable systems and standards-based biometric technologies that are capable of rapidly determining an individual's claimed or true identity."[279]

By contrast, Europe does not demonstrate such an aggressive strategy towards regulation (to stimulate the market demand) and standardisation (to influence technical orientation and EU suppliers' competitive advantage). From a technical perspective, some European suppliers complain that the lack of European attention to the development of biometric standards is part of a wider lack of vision and 'roadmap' in Europe with regard to the development of biometric technologies. Such a 'roadmap' could, in turn, provide suppliers with clear visibility of the future thus enhancing their ability to define long-term approaches to R&D and subsequent investments. A further issue is that, contrary to the US, Europe does not have the capability to test the performances of a biometric identification solution due to the absence of large-scale biometric databases that are absolutely necessary in order to test these types of solutions.

Europe has however more recently engaged itself in biometric passports and visas on a large scale and has apparently taken the interoperability leadership through multi-annual tests of the Brussels Interoperability Group (BIG). Current actions in Europe include Biometric Matching System (BMS) where Sagem and Accenture are collaborating to implement a global biometric engine and database allowing the storing of 70 millions biometric datasets of European and foreign citizens. The system is designed to facilitate interoperability between police, justice and immigration services and interact with existing databases like the SIS (Schengen Information System) and VIS (Visa Information System). Overall, however, the biometric market still remains limited in Europe due to conservative Member States policies towards biometry with respect to the US.

[279] Source: www.nist.gov

Biometry and airport security standards

Airport Security is currently one of the major vertical segments of the security market impacting the regulatory, standardisation and structure of the biometry supply chain. Since the late 1990s ICAO has converged towards a standardisation of the 3 formats of biometrics that have been selected since 2002 for new passports issuance: face, fingerprints and iris.

The major regulatory texts for civil aviation security, whether international (annex 17 ICAO) or regional (European regulation 2320 and 820) are anticipating the generalisation of biometry within air transportation security procedures. Similarly, the ISO 24713-2 norm, which has been adopted since Q1 2008, regulate biometric access control for professionals within airports.

Biometry within e-passports could simplify police/customs security checks and identity controls for boarder control procedures within airports. Fully automated systems are already operational in Europe (e.g. the IRIS system which has been in place since 2006 in major British airports, the French pilot test PEGASE) and provide a basis for testing technology in 'real life' implementation (300,000 flyers in the UK, 10,000 in France).

7.5.3 Overall assessment of regulatory conditions

Regulatory conditions in the high-end biometric market are essentially being driven by developments in the USA, which has put in place regulatory initiatives, certification and standard bodies that have become world references for the entire industry. On top of its proactive role in defining biometric standards and application driven regulations, the US is also home to the most advanced academic teams in the field of biometrics, which constitutes *de facto* a favourable and open environment to international players to develop new state of the art solutions in close cooperation with national authorities and end-users. By contrast, Europe is concentrating its effort on biometric passports, visas and interoperability issues as illustrated by the Biometric Matching System program. From a regulatory perspective, the air transportation vertical market segment is indeed one that is offering to high-end biometric solutions suppliers the most interesting development perspectives in the medium term. European national regulations for biometric authentication in airports should follow the biometric passport deployment but some barriers remain in Europe due to lower public acceptance as well as cautious national authorities and European positions. On top of fingerprints and face recognition, which are embedded in the new generation of biometric passports, other biometric modalities such as iris recognition are being tested by some European airports for other applications such as boarding controls, etc., which may further contribute to the lack of homogeneity of the European market.

7.6 The global competitiveness position of the EU industry

The biometric equipment market really took off during the 1980s with the first large public contracts for automated identification solutions in the US (police forces, FBI). Europe was, at that time, at the forefront of biometric technologies, due to its historic knowledge of anthropometry and its early adoption of biometry for justice and anti-criminal activities. Since the 1980s, biometry has become one of the most dynamic

segment of the security equipment industry, and the September 11th attack only accelerating an already existing demand for large identification solutions at a very large scale.

From a supply side perspective, biometric equipment and system providers have developed in close connection with their local market. In this respect, some differences can be highlighted among the main competing regions:

- Europe: focus on high security level and governmental authentication/identification applications, as well as equipment and system integration,
- North America: largest supply scope, covering both high end market segments as well as large volume (low cost) commercial applications (logic access for computers, hospitality, etc.), from sensing technologies to large system integration,
- Japan: mainly focused on commercial applications and trace-free biometric technologies like vein recognition (for cultural reasons), comprehensive equipment within the supply chain from sensing technologies to equipment integration;

Today, the biometric equipment market segments are still dominated by large governmental programs (civil and criminal ID, military, state and national government, etc.). Estimates by the International Biometric Group indicate that this segment will represent close to 70% of the total market for biometric equipment during the period 2009 to 2014. Commercial market segments of biometric equipment (retail, gaming/hospitality, high tech and telecoms, etc.), although growing faster, are note expected to modify this market breakdown, at least in the medium term.

From a technological perspective, entry barriers are rather high in the biometric market and fingerprint solutions are expected to remain the dominant technology over the years to come, followed by facial recognition systems. This is essentially linked to the characteristic of the largest market segments (governmental applications), which are resistant to frequent technology disruptions and favour interoperability and incremental technology updates.

It is worth noting that the competitiveness criteria for biometric suppliers are different from high-end governmental to commercial applications. High-end applications value added essentially relies on algorithm/software design and system integration capabilities contrary to commercial applications where the added value largely lies on device integration capabilities in order to reduce cost.

From a competitiveness perspective, Europe is home to one of the world leaders – and arguably the leader – in high-end biometric identification solutions, namely Sagem Sécurité. The development of the company's activities have, however, been largely driven by opportunities in the US market environment, from both a demand side perspective (the largest contracts are located in the US) and an industrial perspective (recent acquisitions of both Motorola biometrics division and GE Homeland Protection). Indeed, with the exception of this world leader, the European biometric industry appears quite fragmented and fragile, in particular due to the weak European market demand for high-end security products. From an equipment/device perspective, European supply is characterised by a few companies of relatively limited size offering high-end biometric products. These companies currently have neither the size nor the capability to develop

large (value added) systems and solutions. Consequently, they are generally partnering with large scale system providers, either US or European based, to develop their sales.

A major issue for the development of the biometrics security sector in Europe remains the limited size and fragmented nature of the market. One important aspect of this situation is the cautious policies of national authorities' with regard to the adoption of biometric solutions, which can be seen as a reflection of public concerns about preservation of individual rights of citizens (e.g. protection of personal information etc). This cautious approach plays a critical role in limiting the size of the market and, hence, the development of high-end biometric identification systems.[280]

The limited European biometric equipment market size is not the only challenge that European suppliers have to cope with. A closely related problem is that restrictive national policies (based on protection of personal information) hinder the ability of European companies to develop or access large scale biometric databases that are necessary in order to test new biometric technologies and equipment/systems. This is a considerable constraint on the ability of European companies to develop and validate biometric solutions, and in turn on the innovation capacity and competitiveness of the European supply chain.

7.7 Conclusions and potential policy issues

Although the competitive position of Europe within the global level playing field appears to be favourable due to the fact that Europe is home to the market leader, the future prospects for the European market environment appears less favourable - from both a market size and an R&D perspectives - when compared with the US.

From a policy perspective, regulations relating to biometric security deployment are a national responsibility. Nonetheless, at the European level, a number of potential policy initiatives can be identified that could contribute to stimulating the market for deployment of biometric authentication and identification and to strengthening the European supply chain for biometric solutions. These may include:

- **Development of a European-level approach to biometric security**. Current policy is set at a Member State level with individual national bodies having the responsibility to analyse, certify and qualify biometric solutions. A European vision (e.g. roadmap) for biometric security could support the development of more coherent and harmonised national policies. Similarly, an independent body with the ability to provide expertise to guide and evaluate biometric developments/solutions at a pan-European level could help to consolidate the supply chain and provide some kind of medium/long term guidance for the industry (as it is already the case in the US).
- **Enhance public-private dialogue**. Industry representatives have indicated that they feel that there is a lack of dialogue between national authorities and industry concerning the development of relevant public policies that affect the biometric

[280] As noted earlier, between 2009 and 2014, the International Biometric Group is anticipating that North America will continue to represent 30% the market for biometric equipment, while Europe will see its market share decline from 21% to 16% over the same time period.

security market and industry. This lack of dialogue is also true at the European level and should be addressed.

- **Support academic biometric infrastructure**. The degree of biometric expertise within the EU academic community is seen to weak when compared to the US, where clusters of academic expertise have been developed in order to support industrial R&D investments. This weakens the competitive position of the European industry.
- **Improve product liability framework**. The US SAFETY Act allows high-end security solutions - including large-scale identification systems – to benefit from a dedicated liability regulation, limiting the investment risk for the industry and thus stimulating investments within the supply chain. Adoption of a similar European initiative could stimulate investment in the European biometric security sector.

8 Secure, mobile, ad-hoc communication systems

8.1 General description of the segment

8.1.1 Segment definition

The segment under analysis in this Chapter is 'Secure, mobile, ad-hoc communication systems in case of incident, crisis or disaster events'. **Our specific segment market analysis will concentrate on large government communication systems**, which corresponds to the large security threats identified by the European Commission and the high-end Professional Mobile Radio (PMR) communications market segment.

PMR equipment and infrastructure are used in specific application market, whether they are private or public, with high levels of security requirement. This results in hardware redundancy[281] as well as specific piece of technology development compared to general purpose mobile communication equipment categories. For example, PMR equipment differs from civil mobile communication equipment by providing additional services to subscribers such as:

- Group call;
- Emergency call;
- Direct call;
- Broadcast call.

PMR communication networks also have specific features that are mandatory for some security market, in particular:

- Communication encryption, to limit the risk of intrusion within the communication network and ensure a high degree of confidentiality to the users;
- Communication robustness, to guarantee the availability of communication and protect the communication network against internal threats such as network saturation or external ones such as natural disasters.

8.1.2 Product overview

From a product perspective, the secure communication sector is similar to the global telecom industry and includes two different types of product families:

- Infrastructures: base stations, repeaters, switches, routers, etc.

[281] Correspond to the implementation of redundant electronic circuitry in order to make the equipment fault tolerant in case of a component failure

- Terminals: mobile terminals, talkie-walkie, peripherals (earphones, embedded terminals in vehicles, etc.)

The secure communication sector also includes the development of specific applications mainly based on software development like geo-localisation, bringing a high added-value to users from an operational perspective.

Product families can then be divided into either fixed communication or mobile communication products, each corresponding to different types of constraints, technology and most importantly end-market applications:

- Fixed communication products correspond mainly to critical infrastructure markets (embassies, power plant, etc.)
- Mobile communication products corresponds to civil security applications (police, fire-fighters, emergency squads, etc.) as well as specific end application market such as special events secure communications solutions or transportation networks, requiring dedicated mobile communication services.

8.1.3 Overview of technologies

Depending on application requirement and corresponding security levels, technologies used in secure communication equipment will fall into the following categories:

- Military radiocom;
- PMR (Professional Mobile Radio communications);
- Civil technology (GSM, CDMA, WiFi, WiMax, etc.).

Technological development in the telecommunications industry has historically been driven by military applications due to the very specific requirements of military forces in terms of communication, and in particular mobile communications.

Since the 1990s and the emergence of commercial cellular communication standards like CDMA in the USA and GSM in Europe, consumer markets have considerably developed further stimulating the technological development. Mobile communications are now clearly driven by commercial applications, with fast product introduction and increased data rates and performances. Despite the development of commercial low cost and high performance communication solutions, some specific security markets such as public safety, transportation, utilities, etc. require dedicated communication network with specific technologies and characteristics, living some space for the development of PMR technologies.

The basic differentiators of PMR technologies against commercial applications lie in the encryption of communications and the security of service thanks to hardware redundancy as well as dedicated network infrastructures operating in specific frequency spectrum compared to commercial communication networks.

First limited to analogue two-way radios (talkie-walkie), PMR technologies have developed in the USA and Europe during the 1980s and 1990s, in parallel with commercial mobile communications. PMR solutions evolved during that period from basic network infrastructure to comprehensive mobile digital communication networks

with high level functionalities particularly designed for public safety forces, fire fighters, transportation staff, etc. Although the development of PMR technologies is less dynamic than commercial cellular communications, it benefits from fast incremental improvements in the commercial domain and follows the same technological drivers such as IP communication, increased data traffic and interconnection capabilities.

From a technological perspective, this evolution tends to blur the boundaries between commercial and PMR core technologies, the main distinction between both markets being in the development of dedicated system designs and software development rather than in the hardware technology itself.

8.2 Market (demand-side) overview

8.2.1 Overview of main market (customer) segments

From an end client perspective, the PMR market either corresponds to the requirement of large governmental systems (police forces, etc.) or private systems (retail, logistic, etc.). Both end market categories do not require the same level of communication security and do not correspond to the same technology, neither to the same suppliers as described later on. A further distinction has then to be made between high-end and low-end PMR solutions.

From an equipment perspective, high-end PMR solutions can either be based on analog or digital communications schemes. High-end digital PMR systems represent approximately 30% of the total market in value terms with the following approximate end-application market breakdown[282]:

- Public safety: 60% to 70% of the market in value terms (around 50% in user terms);
- Mass transportation: 15% to 25% in value terms;
- Critical infrastructure: 10% (including offshore, water distribution networks, energy, stadiums, etc.);
- Defence: <5%.

8.2.2 International market profile and market size estimates

The market for large high-end PMR systems is very much influenced by the structure of governments at the national and even local level. Several profiles of end-market can be distinguished:

- Highly centralized market at the national level like France, or at the federal/province level like Spain;
- Highly decentralized market like in the USA;
- Local markets like municipalities for example, who may have their own budget line and decision power for such type of communication investment.

[282] Note: these estimates refer to the high-end digital PMR market (referred to as trunked digital PMR). A broader classification (trunked PMR) includes also analog solutions; the Defence share of this broader classification is estimated at around 10% of market demand.

According to industry estimates, the high-end PMR market value is estimated at € 6 billion[283] (including infrastructure and terminal equipment, as well as applications and services).

8.3 Description of the supply (value) chain

Although the development of the secure communications sector cannot be disassociated from the general development of the telecommunications sector (see Box 8.1), security markets have special requirements that general consumer telecom networks and devices are not generally able to provide. This has led to the development of specific network typologies and corresponding supply chains (see Table 8.1).

As far as the equipment value chain is concerned, the following key stages can be isolated, each corresponding to dedicated company activities and profiles although vertical integration degree may vary depending on players' strategies:

- Components design and manufacturing;
- Electronic board design and assembly;
- Equipment design and integration;
- System integration.

The structure of added value is very different between low-end and high-end market segments of the PMR industry:

- In low-end applications, infrastructure added value is very limited compared to the terminal added value. Most of the players' revenues are generated thanks to the 'device'.
- In high-end applications, added value is on software and systems rather than on the device. Software development can represent up to 50% of R&D cost for a high-end terminal.

Table 8.1 Supply chain discrepancy between global mobile telecom market and secure mobile communications

	Global telecom market	Secure communications
Terminal suppliers	Nokia, Samsung, LG, Sony-Ericsson, etc.	Motorola, EADS, Sepura, etc.
Infrastructure suppliers	Ericsson, Nokia-Siemens, Alcatel-Lucent, Huawei, ZTE, etc.	Motorola, EADS, Selex, HYT, etc.
System integrators	Infrastructure suppliers + IT integrators (Accenture, IBM, etc.)	Infrastructure suppliers + Defence integrators (Lockheed Martin, Raytheon, etc.
Operators	ATT, Orange, O2, China Mobile, etc.	Depending on applications and countries either private operators (Airwave), public operators or national authorities

[283] EADS market estimates

Box 8.1 General development in the telecommunications sector

Telecommunication networks play an essential role in the society, by providing a link between individuals as well as companies, in order to exchange both voice and data transparently.

The telecommunication supply chain is a rather complex one, involving several categories of suppliers with very different business models, from electronic component and equipment suppliers to service suppliers including global operators providing communication services, either fixed or mobile, on a global basis.

Telecom is subject to specific conditions that are somewhat different from other industries. Specifically, its development has been for a long period of time based on a 'closed loop model' at the national level characterised by local technology providers, incumbent operators and public R&D bodies working in close relationships to develop new network generations and facilitate market adoption, as well as maintaining return on investment for the industry thanks to national deployment programs.

Although national authorities still play a critical role in defining telecom market rules at national levels, the industry is now much more open to international competition, in particular since the telecom crisis that occurred in 2001. New technologies and devices are now increasingly being developed in the Far East, which translates into a highly competitive environment for market players.

From a supply chain perspective, a telecommunication network is basically composed of two product categories:

- Terminals & peripherals: to connect a user to the telecommunication network;
- Network infrastructure: providing the path to convey the information on either short (Local Area Network) or long distances (Wide Area Network, Metropolitan Area Network, etc.).

Since the telecommunication market globalisation, the telecoms industry is being driven from a technology perspective by the progressive penetration of communication systems around the world, predominantly for consumer and enterprise applications, as well as the increase of data exchanges backed by the generalisation of internet usage. In the more developed countries, this fast development is being further stimulated to increase the quality of service and performance of new generation networks, and in the less developed areas, to reduce cost and facilitate telecom penetration among households and business.

8.3.1 Overview of main market players

Motorola is the clear number one player on the high-end PMR market with a market share of approximately 50%, followed by EADS (20-25%). The fifth most important player, namely THALES, has only a 3% market share. Motorola has 80% market share in the US, which is representing approximately 40% of the world market[284].

From a supply chain perspective, the major European players are exclusively competing on the high-end segment of the PMR market whereas Japanese players are concentrating on the low-end segment.

Motorola is the only player addressing both dimension of the market, which provides the company with a competitive advantage due to higher production volumes. Motorola's annual production represents several millions PMR terminals whereas EADS is only

[284] Market share estimates have been collected through interviews with EADS and THALES representatives.

manufacturing 10 to 100k terminals per year. In addition, Motorola's key competitive advantages lie on an extensive and global distribution network for low-end products as well as a global brand known worldwide as the reference for PMR communication.

Europe has however good positions on the high-end market segment outside of the USA. EADS is indeed stronger than Motorola in Europe and has a similar world market share (US market excluded). Selex (Finmeccanica) is also a major supplier in the high-end PMR segment (#3 on the world market if US excluded).

In addition to the big players mentioned above, Europe also has some smaller players positioned on high-end markets such as:

- Rohill, NL
- Sepura, UK (350 employees)
- Frequentis, Austria (800 employees, 141 million euros in 2008)
- Rohde Schwarz, Germany
- Team Simoco, UK
- Teltronic, Spain

These players are either designing/integrating specific product categories (like terminals for Sepura) or complete systems for specific market segments (transportation, local systems, etc.).

Europe also has system integrators able to pilot large infrastructure deployments. These companies are mainly coming from the aerospace/defence industry (e.g. Thales, BAE, EADS, Finmeccanica/SAAB).

Table 8.2 PMR OEM ranking

	Low end	High end
1	Motorola (US)	Motorola (US)
2	Kenwood (Jap)	EADS (EU)
3	Icom (Jap)	Harris (Tyco/Macom) (US)
4		Selex (EU), HYT (CH)
5		Thales (EU)

Source: EADS

The high-end PMR market is a conservative one, which has rather high entry barriers. In Europe, some attempts have been made by players from the mid-end segment to penetrate high-end application with limited success (Siemens and Rohde Schwarz have lost a major contract in favour of more established players, namely Motorola and Alcatel).

To some extent, high entry barriers are also a result of the lack of understanding of the customers. Consequentially, commercial lobbying/marketing by suppliers can play a key role to play in helping customers define (and influence) their needs, which has a direct impact on the sales and marketing costs. Only large equipment/system integrators (e.g. GE, Lockheed, Raytheon, Northrop, Thales, Alcatel, etc.) have the financial structure to support such investment before the first product shipment. EADS has the ambition to become one of the key players for large systems integration in the future, although the

market is up to now in the hands of large defence conglomerates, mainly US-based, thanks to the market structure that is in their advantage.

Table 8.3: Motorola: Basic company indicators

MOTOROLA (US)				
Main indicators	**Motorola Inc.**		**Enterprise Mobility Solutions**	
	2007	2008	2007	2008
Turnover	€26,734m	€20,499m	€5,621m	€5,508m
Profit (loss)	(€36m)	(€2,886m)	N/A	N/A
R&D budget	€3,233m	€2,795m	N/A	N/A
Number of employees	66,000	64,000	N/A	N/A
Description of the company				
Motorola, Inc. is an American, multinational, telecommunications company based in Schaumburg, Illinois (United States). It is a manufacturer of wireless telephone handsets, and also designs and sells wireless network infrastructure equipment such as cellular transmission base stations and signal amplifiers. Its business and government customers consist mainly of wireless voice and broadband systems used to build private networks and public safety communications systems. The Enterprise Mobility Solutions of Motorola is by far the world leader in the global PMR market, with a large market coverage from low(mid)-end analogue PMR to high-end digital PMR, with large market shares across all continents and end-users profile.				
Main products and technologies				
▪ Low-end two-way radio ▪ APCO P25, ▪ TETRA, etc.				

Source: 2008 Annual Report (http://investor.motorola.com/financials.cfm)

Table 8.4: EADS Defence & Security: Basic company indicators

EADS Defence & Security				
Main indicators	**Defence & Security**		**Defence & Communication Systems**	
	2007	2008	2007	2008
Turnover	€5,392m	€5,668m	N/A	€1,400m
EBIT	€345m	€408m	N/A	N/A
R&D budget	N/A	N/A	N/A	N/A
Number of employees	N/A	N/A	N/A	5,520
Description of the company				
EADS is a global leader in aerospace, defence and related services. The division Defence & Communication Systems corresponds to the PMR activity of EADS within the EADS Defence & Security subsidiary. It is historically positioned on the secure communication business since the integration of Matra Communication within EADS at its creation. EADS consolidated its position in the PMR business thanks to the acquisition of Nokia enterprise solutions in 2005 and then Plant CML in the US in 2008. EADS Defence & Communication is the European leader for high end digital secure communication solutions				
Main products and technologies				
▪ TETRA, TETRAPOL ▪ APCO P25, (following PlantCML acquisition)				

Source: EADS 2008 Annual Report (www.eads.com) and public consultation

Table 8.5: Selex Communication: Basic company indicators

SELEX COMMUNICATION (IT)				
Main indicators	**Selex Communication**		**Professional Communications**	
	2007	2008	2007	2008
Value of Production	€ 787m	€ 755m	N/A	N/A
Profit	N/A	N/A	N/A	N/A
R&D budget	€ 47m	€ 87.4m	N/A	N/A
Number of employees	4,721	4,404	N/A	N/A
Description of the company				
SELEX Communications, a Finmeccanica Company, is a global supplier of advanced communication, navigation and identification solutions to protect communities and critical national infrastructure. The company delivers advanced, secure, integrated and interoperable networked solutions for governmental, civil and military applications. SELEX Communications develops and supplies turnkey and integrated communication solutions that combine different communication technologies including TETRA, Simulcast and last generation wireless broadband radio to realize multi-technology network solutions, as well as Air Traffic Control (ATC) and GSM-R radio communication systems. The company is headquartered in Italy with offices all around the world.				
Main products and technologies				
▪ TETRA ▪ SIMULCAST ▪ .GSM and GSM-R				

Source: www.selex-comms.com

Table 8.6: Harris Corporation: Basic company indicators

HARRIS CORPORATION (US)				
Main indicators	**Harris Corporation**		**Wireless Systems**	
	2007	2008	2007	2008
Net sales	€ 3,097m	€ 3,613m	N/A	€ 315m
Profit	€ 351.4m	€ 302.2m	N/A	€ 58m
R&D budget	€ 171.2m	€ 187m	N/A	N/A
Number of employees	16,000	16,500	N/A	1,150
Description of the company				
Harris is an international communications and information technology company serving government and commercial markets worldwide. Headquartered in Melbourne, Florida (US), the company is dedicated to developing best-in-class assured communications® products, systems, and services. Wireless Systems corresponds to the TYCO/MACOM PMR activity purchased by Harris Corporation in April 2009. Wireless Systems is entirely localized in the USA, with product development in Massachusetts and manufacturing facilities in Virginia. Principal end-markets include public safety and public service, federal government, transit and transportation, and utilities.				
Main products and technologies				
▪ APCO P25 ▪ Broadband WiMax ▪ EDACS ▪ Etc.				

Source: press release, www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2690

The role of SMEs in the PMR sector

There is a limited number of SMEs active on high-end PMR market, which is the segment that is under the scope of this analysis. SMEs are generally start-ups limited to specific technology development that may be integrated by PMR equipment suppliers in their global solution portfolio. Some SMEs from the IT sector may also be involved in the PMR market to provide specific encryption algorithm based on specific software developments. Other specialised SMEs, which are generally spin-offs of larger industrial groups, may also propose additional communication capabilities to existing systems based on innovative network architectures/solutions (BluWan, Luceor).

Start-ups may also develop to propose new services requiring secure communications capabilities but these companies are generally using standard technologies and differentiate themselves on the basis of innovative business models and service offerings rather than on equipment.

8.3.2 Component supply

PMR equipment integrates several types of electronic components including antennae, filters, amplifier, processors, converters, etc. Most of these component families rely on semiconductor technology with manufacturing capacities heavily localised in Asia, where these components are generally produced. The PMR market is only a minor contributor to the revenue of electronic component manufacturers, which is to a very large extent determined by revenues coming from consumer applications.

Although electronic components rely on commoditised technologies and production is outsourced, specific component design activities are still being kept internally by major PMR players. This is in particular the case for specific integrated circuits[285] that provide data encryption functions, which remains a key capability of PMR devices.

Degree of concentration: HIGH

8.3.3 Electronic Board Assembly

Electronic board assembly is the process by which components are being placed and interconnected within an electronic board. Electronic board assembly is to a very large extent subcontracted to dedicated players, also called EMS (Electronic Manufacturing Services). Again, PMR applications generally represent only a small portion of their revenues.

These players have production facilities localised across the World in order to find the right balance between volumes, flexibility and cost. For the PMR market, the specific requirements and low volumes are such that it remains possible to maintain board assembly activities in high cost regions like the USA or Europe.

Degree of concentration: MEDIUM

[285] An Application Specific Integrated Circuit (ASIC) is an integrated circuit developed for particular application in order to improve their performance.

8.3.4 Equipment design and integration

This is the segment of the value chain where PMR players concentrate their attention. If PMR equipment design is kept internal, the integration (production and testing) of equipment may either be kept internal in dedicated manufacturing facilities (e.g. Motorola use this approach) or outsourced to EMS/ODM specialists who may have the know-how to do so. It is worth noting that these EMS/ODM may be previous OEMs plant that have been spun-off as part of a 'de-verticalisation' process (e.g. EADS/Lagassé Communication).

The number of players in a position to operate in this market depends on the segment of the PMR market that they address:

- For low-end application with relatively low constraints on product performances and robustness, entry barriers are relatively low as well as the degree of concentration within the value chain.
- For high-end application with high constraints, entry barriers are high and thus the number of players rather limited.

8.3.5 System Integration

System integration mainly refers to the high-end segment of the PMR market serving large government systems. In these types of systems, PMR equipment is only one part of the full security solution and has to be integrated in or interconnected to an existing information system.

System integration can be performed by:

- **IT integrators**: generally providing an expertise on the client business and existing infrastructure rather than a technological expertise on PMR solutions (Accenture, IBM, etc.);
- **System integrators**: providing a technological expertise, including a PMR one for some of them. Include large system integrators from the Aero/Defence industry (Lockheed Martin, GE, Thales, etc.) but also niche market specialists (airport communication integrators);
- **PMR integrators**: providing integration services on top of PMR equipment (EADS, etc.)

The degree of concentration is rather HIGH but also depends on the security requirements of the dedicated application.

8.3.6 Related services

Related services associated with PMR communication networks include:

- Network installation and maintenance: realized by specialists players in close cooperation with the end-users and the equipment suppliers,
- Network operation: corresponding to the day-to-day management of the communication network. This task can be realized either by dedicated network operators or by the client himself in case of large governmental applications.

Of course, most of the recurring cost of the PMR value chain lies in related installation and maintenance services, which represent more than 50% of the PMR market (according to consultancy firm IDC[286])

8.3.7 Linkages to final markets

The structure of distribution channels is very different depending on end-market typologies. While low to mid-end PMR solutions are generally provided through specialist distributors, addressing a very fragmented demand (retail stores, manufacturing facilities, etc.), high-end PMR solutions for civil security forces, public transportation networks or governmental agencies are generally being directly addressed by the equipment manufacturer.

Contrary to other security industry sub-segments, PMR equipment suppliers have by nature a complete vision of the communication network. They are consequently in a better position to realize its integration although they can also work in partnership with dedicated system integrators depending on applications and customer requirements.
It is for example difficult for a European equipment manufacturer to win a contract in the USA without any partnership with a local system integrator.

8.3.8 Overall assessment of the supply chain

Overview of production organisation and location

PMR equipment production, contrary to the global telecommunication equipment industry, is still localised close to the final largest market, namely the US and Europe. This is specifically true for high-end equipment categories and application with large security requirements where nations do not want this piece of technology to be manufactured in the Far East. Some key hardware pieces also fall under the same restrictions like the encryption modules, for which design and production remain local for national security purposes.

With regard to the specific organisation of production activities, the situation depends on players' market positioning and portfolio. Although production tends to be massively subcontracted in the PMR business, some companies – such as the market leader, Motorola - continue to integrate manufacturing activities. However, Motorola has a specific position in the market thanks to its high production volumes. More importantly, perhaps, a large part of this manufacturing activity still seems to be localised in the USA, which could be considered as an asset in order to secure its leadership position in the US market when negotiating with administration and authorities (especially in the high-end segment which involves consultation with, and authorisation by, national authorities).

The situation of Motorola can be contrasted with EADS that has outsourced its production and sold its manufacturing plants in 2005 to a Canadian group named Lagassé. Production is localised in Europe mainly in France (Lagassé) and Estonia

[286] *Le marché des réseaux radio-électriques*, February 2006. Survey conducted for the French National Telecommunication Authority ARCEP

(Elcoteq, an EMS previously working with Nokia before the acquisition of Nokia's PMR business by EADS).

Industry consolidation and new entrants

Over the past 15 years with the tremendous development of mobile communications, players from the telecom industry have constantly adapted their business perimeter. Traditional telecom equipment suppliers divested PMR activities to focus on mainstream equipment business lines. The first important move was made by Philips in 1996 who disengaged from its PMR activity when it spun-off this activity to form Team Simoco. The 2001 crisis put the telecom industry under severe financial constraints, which further accentuated the consolidation of the PMR sector. The largest telecom companies serving mass-market consumer application and networks divested their PMR product lines, which have mostly been acquired by Aerospace and Defence groups; for example:

- Acquisition of Nokia PMR activity by EADS in 2005[287];
- Acquisition of Alcatel PMR activity by Thales in 2006;
- Acquisition of Tyco Wireless activity by Harris in 2009.

Recent acquisitions by major PMR suppliers also illustrate their interest in developing their market footprint abroad:

- Motorola acquired Vertex (Japan) in 2007, a specialist of two-way radio systems (low-end);
- EADS acquired Plant CML (US) in 2008, the US leader for emergency (911) and mission critical management solutions.

These acquisitions are being undertaken to secure leadership positions in key strategic segments and to face the arrival of new players within the PMR market. These new entrants have different profiles:

- **Broad-based telecom equipment suppliers** willing to reintegrate the PMR market in order to increase their margins in more protected markets compared to highly competitive consumer ones (Alcatel, Nokia). This also includes new players in the developing countries and specifically China (e.g. Huawei and ZTE). These players are however positioned on new types of services (healthcare, etc.) and do not directly address the high-end segment of the PMR market;
- **Dedicated PMR specialist players** like HYT (China) supported by local government and local market barriers in order to secure a local source in these highly strategic communication technologies; (HYT is already equivalent in size to Selex thanks to the protective measures put in place in its home market).

Business opportunities may also arise for new entrants in smaller markets (cities, small enterprise), which are not directly targeted by the large secure communication providers. In the most developed countries where large civil security networks are already deployed, these smaller markets are the most dynamic area of demand for PMR.

[287] EADS was already involved in PMR communication due to the integration of Matra Communication in the perimeter of the European Group since its creation.

8.4 Main trends and developments

The global telecommunication industry is the subject of intense competitive pressures from both a technological perspective and business model perspective. From a technological perspective, key developments include:

- Development of IP based communication in replacement of telecom-based architectures and technologies;
- In the longer run, development of Software Defined Radio solutions outside of the defence perimeter to address both the global telecom as well as the secure communication market.

And from a business model perspective:

- Development of services, driving profound modifications on the structure of the supply chain and the positions of players;

Although the PMR market is a rather protected – and somewhat 'conservative' - market compared to general purpose communications business, it is nonetheless influenced by these global forces.

8.4.1 Market trends and developments

As far as the high-end PMR solutions are concerned, the market has been very dynamic in the recent years due to the progressive deployment of next generation digital networks (TETRA, P25) in Europe and in the USA in order to update previously deployed PMR networks. From a general perspective, the market drivers in the PMR industry are historically corresponding to a 'technology push' model, (i.e. new standards and technology emergence) creating the demand of governmental agencies and civil security forces.

However, the market for PMR equipment, with the notable exception of large-scale nation wide communication networks, is highly fragmented at the regional and even local level, which is to some extent limiting the growth potential of PMR solutions due to a lack of harmonisation.

8.4.2 Technology trends and developments

Pressure to use civil technologies

Technological progress in the telecommunication industry is being driven by consumer applications, providing increased data rate and additional services to traditional mobile voice communications. Although the competition intensity is less important in the PMR market than in the consumer one, the PMR industry is facing some pressures to adopt 'consumer-based' technology in security network architecture.

The expected benefits of adopting consumer based architecture is to reduce costs, increase the security of supply through a reduced exposure to specific piece of technology and of course benefit from the latest advancements in terms of transmission data rates that are somewhat limited in traditional PMR equipment due to ageing network architectures.

One major expected evolution of security solutions in the medium and long term is indeed the development of data fusion capabilities, i.e. the ability to aggregate, filter and analyse very large data flows coming from different sources such as video-surveillance cameras or other sensor categories. The development of this capability translates into larger amount of information to be conveyed through secure communication networks, which should be adapted to support this increased data rate.

Although consumer-based networks and architectures are more robust and secure than they were in the past (3G, Long Term Evolution, WiMax), their specifications are however not compliant with the high-end security market. Therefore, attempts are being made to modify these consumer based standards and technologies in order to provide additional levels of protection; for example:

- Secured-WiFi;
- Secured-WiMax.

Such type of development is however expected to impact low-end and mid-end application sectors of the security market rather than high-end application sectors.

Another approach being developed by the industry is to use existing COTS (Commercial Off The Shelf) products like components or modules and to tune them directly in order to increase their level of security and robustness. Several approaches can be adopted in order to perform this customisation with different levels of performance:

Table 8.7 COTS levels of performance

	Type of modification	Cost associated to design modification	Players profile
Level 0	Direct COTS use	€ 0	SME
Level 1	COTS shell in more rugged package	€ 30,000	SME
Level 2	COTS with hard/soft add-ons	€ 500,000	SME / Large Players
Level 3	Internal COTS hard/soft redesign	€ 1m	SME/ Large Players
Level 4	Modified wireless standard on new platform	€ 10m	Large Players

Source: Thales

IP-based communications

The civil telecommunication industry is currently shifting on a major scale from historical telecom-based technologies and network architectures to turn to IP-based communications. IP-based communication, contrary to telecom-based technologies, is based on highly commoditized hardware and modular approach, increasing maintenance/upgrade performances and reducing total cost of ownership.

PMR telecommunication equipment is currently based on rather traditional telecom technologies and has not evolved to integrate IP-based architectures. However, some players like Thales are already offering PMR solutions using such type of technologies based on routers rather than switches. If this type of technology was to develop further, this could have a large impact on players strategy in terms of development and production.

Software Defined Radiocommunication (SDR)

The concept of Software Defined Radio-communication is the ultimate evolution of IP-based communications and corresponds to one rather simple argument. Considering the fact that there is an exponential growth in the ways and means by which people need to communicate, the need to modify radio devices and systems easily and cost-effectively, as well as increase the interoperability between different solutions, developed at different times with different architectures and technologies is becoming a critical issue for the industry.

SDR is precisely aiming at bridging this gap between the increased complexity and heterogeneity of communication networks and the ability for the supply chain to manage such a complexity. A broad definition of SDR is: 'Radio in which some or all of the physical layer functions are software defined' (Source: SDR Forum, IEEE)

The SDR concept first emerged in the Defence sector, and in particular in Europe, in the late 1980s and 1990s due to the fact that communication interoperability issues are very sensitive in this domain. Indeed, the defence industry has to implement new communication systems that are backward compatible with previous ones developed several decades ago, which are still in use on the battlefields or within defence organisations.

In fact, SDR corresponds to a group of both hardware and software technologies that are used in radio's operating functions (also referred to as the physical layer of a communication network architecture) to provide additional level of flexibility thanks to modifiable software or firmware and programmable processing technologies. It then becomes theoretically possible to implement radio hardware with large frequency spectrum capacities and tune this standardised hardware by modifying its software and programmable hardware to emulate every type of waveform whatever the frequency and communication protocol required.

The SDR concept can be even further extended to Adaptive Radio and even Cognitive Radio systems:

- Adaptive Radio, is a radio able to monitor its own performance in order to adapt its configuration and improve its performance,
- Cognitive Radio, is a radio that is not only adaptive but also able to track the local communication infrastructure environment and adapt its settings to emulate it and interoperate with it,

Considering the development of multinational defence cooperation, humanitarian missions and more generally the necessary capability to effectively project forces and infrastructures abroad in every type of situation, there is obvious interest for defence players to develop this type of technology is obvious. The development of SDR systems is, however, still in its infancy and it has not to date penetrated other application fields such as secure or civil communications. In this respect, software content within both infrastructure and terminals tends to increase much more rapidly than hardware, providing additional levels of flexibility to the systems. Nonetheless, should the SDR

concept develop further outside of the Defence perimeter, it could have a profound impact on the supply chain (see Box 8.2)

Box 8.2 Software Defined Radio transition and impact

Should the SDR concept develop further outside of the Defence perimeter, it could have a profound impact on the supply chain, in a way similar to that experienced within the data processing industry during the 1980s.

An 'ideal' SDR solution relies on two core components:

- The device side, corresponding either to an infrastructure equipment (base stations, etc.) or a terminal (mobile phone, etc.) with embedded programmable hardware (FPGA[288], DSP[289], ADC[290]) allowing to adapt the hardware to different communication protocols;
- The software side, corresponding to software defined 'waveforms', which are being downloaded within the device in order to emulate the corresponding protocol.

From a supply chain perspective, the situation is therefore very much similar to the one of the computer industry where the device (computer) added value lies on very specific pieces of hardware (microprocessors), operational systems and applicative software providing the functionality of the overall computing solution. This type of configuration led to the creation of the Wintel duopoly (Windows + Intel) and the commoditisation of almost the entire computing industry with massive subcontracting strategies and the progressive localisation of manufacturing facilities in low cost regions.

Similarly, in the longer run it could be possible to see the progressive shift of major communication equipment suppliers towards the design and supply of licensed waveform software allowing an operator to emulate any kind of communication protocol on its standardised equipment. The investment profile of equipment suppliers will then massively shift to software development rather than hardware.

From a security industry perspective, European communication equipment suppliers are in good position to transition to this new type of business model, having access to the technology, the customers and the system know-how.

As far as the component supply is concerned, the fact that most of the critical pieces of hardware are being developed and manufactured by US companies does not seem to represent a threat for European suppliers. Indeed, DSPs, ADCs and FPGAs used in SDR systems are primarily developed for consumer application and are unlikely to fall under export regulations.

8.4.3 Production trends and developments

Development of services

With regard to services development, the PMR market is no different from the civil telecommunication market and most players are increasingly concentrating attention on services on top of equipment development (see iPhone success). In the PMR domain, additional services that are delivered in addition to more traditional ones may include:

[288] Field Programmable Gate Arrays: semiconductor electronic component, which are programmed by the user in order to perform different types of functions including filtering, processing etc.
[289] Digital Signal Processors: semiconductor electronic components, which are programmed by the user to perform intensive data processing. Mostly used in telecommunication industry and real time applications.
[290] Analogue to Digital Converters: semiconductor electronic components, performing the conversion of analogue signals into digital formals (4,8,16 bits, etc.)

- Situation awareness (complementary information based on geolocalisation capabilities);
- Video streaming, video conferencing;
- High resolution images;
- CCTV;
- Satellite images & maps transfer;
- Detailed real time biometrics.

Of course, the development of these additional services heavily relies on the capacity of PMR networks to convey increased amount of data and consequently support higher data rates.

Specific types of services may also develop within equipment/system integrators in order to educate customers on equipment/systems capabilities. These services are based on simulation know-how and may be used for very large government systems in pre-commercial discussions. Players in a position to provide such type of services are mainly coming from the Aerospace & Defence industries where complex simulation is heavily used.

Network mergers and operational services

The merger of operators' networks and the delegation of network management from operators to equipment/system integrators is a major trend within the telecom industry. This is especially the case in Europe as telecom operators increasingly focus their activity on providing content and services to their subscribers rather than investing heavily in infrastructure capacities and management. Both of these trends are also true in the high-end PMR market:

- Pressure to merge national agencies' networks in order to increase interoperability and reduce cost of ownership;
  - In France for example, communication networks of national security agencies are different and will be harmonised around a common architecture so that interoperability can be further enhanced. National civil agencies will then be users of a common network (INPT: Infrastructure Nationale Partageable des Transmissions).
- Delegation of network operations to external suppliers. As far of the externalisation of national security agencies network operations is concerned, several business model profiles can be distinguished in Europe:
  - In the UK, network management has been outsourced to a private operator (Airwave: spin-off of O2 and BT). Airwave is not only in charge of network operation but also of equipment selection and procurement. Airwave has selected Motorola as its major supplier. Spain has adopted the same type of organization (with Telefónica).
  - There is currently a call for tender to do the same in Germany with, however, a more important control of the State. There is a similar situation in Belgium, where a dedicated operator has been created controlled by the State in order to manage civil security network (a call for tender has been issued for PMR equipment as well as Control and Command systems).

- In France, although civil security network are converging, the State is directly controlling the system.

The same type of business organisation is also developing outside of Europe (EADS is operating the civil security network in Qatar).

Modular approach to technology

From a technological perspective, there are specific requirements in the PMR market (encryption, security of service), which will force players to maintain specific network architectures for high security application. At the same time, the use of civil technology, in the form of functional modules, may develop in order to provide additional capabilities at reduced cost.

This phenomenon has already been experienced in the IT industry and security networks and will likely tend to be more heterogeneous than before from a technological perspective, although this trend is less important than in civil networks. As a consequence, equipment/system integrators need to develop collaborations with external solution providers in order to provide complete solutions to their customers. The telecom industry is increasingly working in multi-vendor environment and integration capabilities become a key asset in the value chain.

This new evolution may have some impact on the investment profile of major equipment integrators. EADS for example is still designing internally its own ASIC (Application Specific Integrated Circuit) and may decide to outsource this activity in the future.

Modular approach to marketing

From a marketing perspective, a similar modular approach may develop in the future. Indeed, the security industry from a global perspective and the PMR market from a specific one are characterised by the complexity of each business cases:

- Complexity and variety of technological solutions;
- Lack of understanding of major end clients who are not familiar with technology;
- Variety of contexts and needs from one business case to another;
- Etc.

Some players within the security and the PMR market are trying to develop new types of marketing tools and process, based on modular solutions and packages, each corresponding to a variety of customers' requirements. This approach aims at simplifying customers' choices and adapting technological solutions to their needs.

8.5 Regulatory conditions and developments

8.5.1 International, European and national security-related regulatory conditions

Regulations impacting the PMR market demand are falling into the perimeter of national authorities, and more particularly the regulation concerning civil security forces, which represent by far the largest end market segment for the high-end PMR solution providers. To that respect, the US adopted specific regulations in 2000 regarding Emergency call, which is stronger than European ones from a technological perspective.

Another area where regulation plays a critical role for PMR solutions suppliers is the allocation of frequency spectrum for secure communication activities, which will be dealt with in the following sub-chapters.

8.5.2 Industry and market based standards

There are different standards deployed worldwide for high-end digital PMR equipment including different functionalities from a security perspective (see Table 8.8).

Table 8.8 Standards for digital PMR solutions

	Emergency call and pre-emption	Authenti-cation	Encryption levels	Players
EDACS	Light	Light	1	Ericsson – Tyco
iDEN	Light	Light	0	Motorola
APCO P25	Yes	Light	2	Motorola, Thales, EFJohnson
TETRAPOL	Yes	Yes	2	EADS
TETRA	Yes	Yes	4	Motorola, EADS, Rohde&Shwartz, Thales, ETELM, DAMM, Rohill, Teltronic, Selex, Sepura, etc.

Source: Motorola

The two major international standards for digital high-end PMR equipment are:

- TETRA in Europe;
- APCO P25 in the USA.

These standards have a strong influence on market access. TETRA is almost available worldwide, with the exception of North America where Motorola put a barrier to its deployment by refusing to licence key patents with the objective to secure its leadership position in its homeland market. Conversely, the US P25 standard is only deployed in North America.

The European TETRA digital PMR standard

The development of the TETRA standards in Europe started in 1990 following the development of the GSM and has similarly relied on the support of the European Commission and ETSI members. This process was also undertaken with the cooperation of manufacturers, users, operators and industry experts and led to the release of the first TETRA standards in 1995, allowing equipment manufacturers to develop interoperable products.

Along with digital PMR standards, other mobile communication standards can be developed to serve specific vertical application markets. This is notably the case for the GSM-R standard addressing the railway industry. This standard has been promoted by the European telecommunication industry and is illustrative of the lack of coordination and industrial policy at the European level. Indeed, it has divided the transportation market between metro application (using TETRA) and national railway networks (using GSM-R).

Players that have abandoned the PMR segment a few years ago (e.g. Nokia) are now trying to penetrate the secure communication market by promoting the GSM-R standard (following Nokia-Siemens merger).

Standards bodies

There are two standard bodies in the World that are instrumental in telecom standardisation:

- ETSI in Europe, and
- TIA (Telecom Industry Association) in the USA.

ETSI and TIA have different approaches towards standardisation. In Europe, voting power depends on the turnover of the company while in the USA each company has the same voting power. Another difference between Europe and the USA in terms of standardisation is the influence of end-users, which is much more important in the USA.

The PSCE (Public Safety Communication Europe) Forum has been put in place in Europe within the 6th Framework Programme in order to define a consensus between the different stakeholders, standardisation being one the key points in the agenda in order to promote further interoperability between national security agencies networks.

8.5.3 Overall assessment of regulatory conditions

From a regulatory perspective, US regulations appear much more attractive to the industry as technical requirements seem to be stronger (emergency call legislation put in place in 2000) compared to those existing in Europe. In addition, each call in the US is financing the communication infrastructure contrary to the European system.

As we have already mentioned the increased data rate requirement is a major trend in the PMR market due to increased data fusion and services demand. However, PMR solutions are limited by the frequency spectrum, which is being attributed at the national level. European countries have allowed national security agencies' networks to operate in the 380-400MHz band and all players have to comply with this constraint, which is having a direct impact on network performances. Furthermore, this strategic and scarce resource does not seem to be protected at the European level, as countries are selling frequency bands in auction to the best bidder for commercial application.

The US has a more protective regulation and already has selected a higher frequency band (700MHz) for security communication networks, which can provide to local players a decisive competitive advantage for next generation security communication networks.

8.6 The global competitiveness position of the EU industry

Like in many security market segments, the mobile secure communication market is divided between general-purpose commercial applications and high security applications, both relying on different technological solutions (analogue versus digital PMR solutions).

From a supply side perspective, regional supply chains in the PMR market have specific market leaderships:

- **Europe:** leadership in high-end governmental applications through the international digital standards TETRA and TETRAPOL with global players supporting complete infrastructure solutions (EADS, Selex, Teltronic, Thales) as well as dedicated players specialised in some devices categories (Sepura, Artevea, Frequentis, etc);
- **North America:** leadership positions across both commercial and governmental applications thanks to Motorola, by far the number one player in the PMR market;
- **Japan:** focus on commercial market segments through large companies such as Icom and Kenwood.

Contrary to other security market segments, the high-end PMR market is more balanced from a demand side perspective, due to the importance of public safety applications (police forces, firefighters, etc.) in the overall revenues of the industry.

Standardization has historically played a key role in the telecommunication market development and secure communications have benefited from the development of specific standards in order to increase technical interoperability capabilities between governmental agencies, as well as to secure regional market for local suppliers.
To that respect, the development of the TETRA standards in EU has proved to be a major success and a strong contributor to the competitiveness of the overall European industry in high-end governmental applications.

Nonetheless, the secure communication industry, like the telecom industry in general, is being confronted to strong competitive pressures since the telecom crisis in 2001 and the deregulation of the communication markets. Increased competition from Asian players and more particularly Chinese players, in addition to the development of IP-based communications have profound impacts on:

- **The structure of the value chain:** commoditization of the devices, development of sub-contracting strategies,
- **The structure of the added value:** value creation through services (content, network operations, etc.)

In front of this changing business environment, European secure communication suppliers are facing the development of lower cost commercial solutions based on IP communications and integrating security network functionalities, which are capturing the low and mid-end part of the PMR market due to an acceptable level of performance coupled with an increased modularity of the communication infrastructure. In this type of communication solutions, intimately linked to the data processing industry, the US supply chain has the global leadership.

On the longer run, the development of Software Defined Radio, whose concept emerged in the European Defence industry, is also in a position to profoundly modify the value proposition of EU suppliers and the structure of the value chain, with an increased focus of large equipment integrators on communication system development and integration.

Although the European leadership in the communication industry has suffered from the development of IP-based communications, Europe remains in a good position to consolidate its competitive position in the secure communication market, thanks to its leadership in mobile and secure communications, as well as its track record and accumulated knowledge in Software Defined Radios, and based on the assumption that an adequate standardization policy and homogenisation of the national markets at the European level is being stimulated.

8.7 Conclusions and potential policy issues

The secure communication supply chain remains specific compared to the commercial one, but the border between both industries tends to blur. Secure communication suppliers have in particular to cope with the same technological trends of the commercial sector, providing higher functionalities and services to the end-user. This relies on a continuing effort in R&D to develop new solutions meeting customer requirements across the world.

Because of standards, existing infrastructure and security constraints for high-end applications, entry barriers remain high for international suppliers willing to develop their sales abroad. This translates into the fact that the local market environment should provide the conditions for local suppliers to justify R&D investments in order to remain competitive against international competition.

The assessment of the secure communications market raises a number of potential policy issues that may be highlighted:

- **Market harmonisation:** There is a factor 1000 between the PMR and the GSM market in terms of end-users. PMR suppliers therefore need some degree of harmonisation at the European level in order to reach a critical size providing the business conditions in order to invest. From a policy perspective, this means that standards will continue to play a key role for supporting the competitiveness of European suppliers on the global market place. Based on Public Safety Communication Europe[291], there is a need for increased collaboration between Member States for the adoption of common interoperability definitions, user requirements, generic models as well as generic scenarios.
- **Radio spectrum availability:** There is a recognized need, in particular for public safety application, to have access to a dedicated radio spectrum. As already mentioned, technological evolution is in addition pushing towards larger bandwidth allocation.
  The progressive shift from analogue TV broadcasting to digital TV broadcasting in the years to come will free up some important spectrum resources in the 800MHz – UHF band. This has to be considered as a major opportunity as these frequencies have very interesting characteristics in terms of propagation and range. Allocating frequencies within this UHF spectrum for public safety application (currently using minimal public spectrum around 1%), which remains the most important output of 'high-end' PMR equipment, could help to stimulate development of the market and technologies for secure applications and, in turn, contribute to enhancing the

[291] www.psc-europe.eu

competitive position of European suppliers. Protecting some of this additional spectrum resource for security application requires a coordinate action at the European level. Additional resources availability for secure communications in the 5GHz area would also contribute to stimulate the development of communication solutions for disaster relief applications and to increase communication interconnection capabilities to other device categories such as sensor networks, etc. Although a lot of actions are being undertaken at the European level by the European Commission and the European Parliament in order to define a common approach to the allocation of the digital dividend[292], no dedicated spectrum is allocated to public safety applications yet.

- **Standardisation for future applications – Software Defined Radios:** Even if Software Defined Radio applications in the security market remain confidential up to now, Europe should pay particular attention to standardisation activities in this field, as the impact on the structure of the supply chain could be very important. Although the US has a more recent experience in this field compared to Europe, industry consultations highlight the fact that they adopt an aggressive standardisation activity in this field. European standardisation activities in the communication industry have proved to be very beneficial to the competitiveness of the EU communication supply chain, eventually contributing to the emergence of the GSM standard. SDR communications will certainly impact not only the secure communication industry but more generally the entire communication industry. It is to this respect a key issue to be considered at the European level.

[292] Such as the Commission Communication COM(2007)700 final on 'Reaping the full benefits of the digital dividend in Europe: A common approach to the use of the spectrum released by the digital switchover' (November 2007) available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0700:FIN:EN:PDF; or the European Parliament ITRE Committee Report, 'Toia Report' on the Digital Dividend in Europe (July 2008), found at:: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0305+0+DOC+PDF+V0//EN.

9 Protective and intelligent textiles and clothing

9.1 General description of the segment

9.1.1 Segment Definition

Definition of personal protective equipment (PPE)

The technical textiles for intelligent personal protective clothing and equipment (protective textiles) are part of the much broader market for personal protective equipment (PPE). PPE refers to protective equipment for all kinds of hazards, like nature, heat, flames, chemicals and flying particles,[293] but also to job-related occupational safety, health purposes, sports, martial arts and combat, etc. One factor influencing the selection of this segment for study is its conclusion in the European Commissions 'lead market initiative' (see Box 9.1)

Directive 89/686/EEC[294] on personal protective equipment determines that PPE covers 'any device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards'.[295] PPE also covers:

- A unit constituted by several devices or appliances which have been integrally combined by the manufacturer for the protection of an individual against one or more potentially simultaneous risks;
- A protective device or appliance combined, separably or inseparably, with personal non-protective equipment worn or held by an individual for the execution of a specific activity;
- Interchangeable PPE components which are essential to its satisfactory functioning and used exclusively for such equipment.

The focus of the Directive is to 'lay down the conditions governing its placing on the market and free movement within the Community and the basic safety requirements which PPE must satisfy in order to ensure the health protection and safety of users'.[296] The Directive belongs to the family of directives under Article 95 of the EC Treaty.[297] It is also worth noting that the Directive is currently being revised to bring it in line with the revised New Approach Framework.[298]

[293] Mäkinen, 'Protective clothing- nowadays and vision', article for the 3rd European Conference on Protective Clothing (ECPC) and NOKOBETEF 8, may 2006.
[294] Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment.
[295] Military equipment can (given the regulatory framework) not be defined as PPE.
[296] Ibid. Footnote 186.
[297] DG Enterprise, http://ec.europa.eu/enterprise/mechan_equipment/ppe/dir89-686.htm.
[298] See: http://ec.europa.eu/enterprise/newapproach/index_en.htm

Depending on the circumstances (sports, fire, chemicals) there is personal protective equipment for nearly every part of the human body (mainly the outside, but also respiratory protection). Examples of PPE equipment are: head protection (helmets, hearing protection, masks), respiratory protection (gas masks, filter masks), body protection (suits like turnout gear, bomb disposal suits, motorcycle suits, but also body armour), arm/shoulder protection, hand protection (gloves), leg and foot protection (shoes, knee pads, hip pads).

Given the broad scope of the sector for personal protective clothing and equipment, **we will focus in this case study on the protective clothing for first responders, mainly policemen and firemen.**

Box 9.1 EU policy background

EU innovation strategy

In 2006, the European Commission published a Communication on a broad-based innovation strategy for Europe.[299] This Communication was a follow-up of the October 2005 Communication on 'More Research and Innovation', which sets out a programme of 19 fields of action[300] and the recommendations in the report 'Creating an Innovative Europe'.[301]

One of the proposals in the Communication on a broad-based innovation strategy for Europe was facilitating the creation and marketing of new innovative products and services in promising areas (lead-markets). The Commission considered that the removal of barriers would essentially contribute to the competitive process and lead to the emergence of new markets. The facilitation should focus on (i) supply measures (e.g. research support by the FP7), and (ii) actions aimed at understanding and stimulating competitive market demand for innovative products and services (examination of the regulatory environment, the setting of standards, better use of the opportunities provided by procurement rules, improvement of the overall market environment for innovation). According to the Commission, such an initiative will help to create dynamic virtuous circles of growing demand and innovation by facilitating early movers, without 'picking winners' or pushing specific technologies.[302]

The lead market initiative (LMI)

In December 2007, the Commission adopted a Communication pertaining to a lead market initiative. For the identification of the lead markets five main criteria were used: (i) demand driven instead of technology push (strong market potential), (ii) broad market segment (range of interconnected products and services), (iii) strategic societal and economic interest, (iv) added value of prospective, concerted and targeted, but flexible policy instruments (combination of different public measures and incentives are needed), and (v) no 'picking of the winners'.[303]

[299] Commission Communication COM (2006) 502 on 'Putting knowledge into practice: A broad-based innovation strategy for the EU.

[300] Commission Communication COM(2005) 488 (12.10.2005) on 'More Research and Innovation – Investing for growth and employment: A Common Approach'

[301] 'Creating an Innovative Europe'; report of the independent expert group on R&D and innovation appointed following the Hampton Court Summit and chaired by Mr Esko Aho.

[302] Commission Communication COM (2006) 502 on 'Putting knowledge into practice: A broad-based innovation strategy for the EU.

[303] Commission Communication COM (2007) 860 on 'A lead market initiative for Europe';

Based on these criteria, the Commission selected six promising lead markets. One of these is the market for **'technical textile for intelligent personal protective clothing and equipment'** (protective textiles).[304]

In order to facilitate the emergence of the lead markets, specific action plans have been developed. These action plans focus on six main policy instruments, namely (a) legislation, (b) public procurement, (c) standardisation, labelling and certification, and (d) complementary instruments (like business and innovation support services, training and communication; financial support and incentives).

9.1.2 Product overview

Protective clothing for first responders

Pertaining the protective clothing for fire fighters the personal protective equipment mainly consists of the following equipment. A difference can be made between products made of textile (turnout gear, clothing), products which contain textiles (gloves, shoes) and other equipment (helmets).[305]

- **Turnout gear** (protective clothing): this includes fire suits, turnout trousers and turnout coats or tunics. Main goal of the turnout gear is to protect against heat and flames during fire fighting (e.g. thermal stress);
- **(Protective) gloves**: Gloves worn by fire-fighters provide protection and prevent injuries to the hands during fire fighting activities. Any small hand injury can prevent a fire-fighter from performing the job correctly or performing the job at all;
- **Boots** (protective footwear): protecting feet, ankles and lower legs from fire hazards. Fire boots are critically important as they are always in contact with a heat source: the ground. This requires that boots protect against a variety of burning materials and other hazards, such as protruding nails and electrical wires;
- **Fire helmets** (protective headgear): this includes head protection against hazards that wearers may come into contact with. Fire helmets need to be able to provide protection at greatly increased temperature levels;

For policemen the personal protective equipment is more limited, and refers mainly to high-visibility vests and safety shoes. Policemen may also need safety vests (basic protection against knives and bullets), tactical vest (bullet-proof vests for high risk situations), riot-gear, chemical/gas suits and motor suits, but this differs per situation and per Member State.

In our analysis, we will focus on the textile-based equipment, like the turnout gear and protective gloves. These textile-based equipment (and mainly the fire-resistant clothing and gloves) form the main type of protective clothing.

[304] The other lead markets are: (i) eHealth, (ii) construction, (iii) bio-based products, (iv) recycling, and (v) renewable energy.

[305] Frost & Sullivan, 'Fire fighter PPE - the challenge and importance of winning and keeping contracts', August 2008. Also mentioned are Self Contained Breathing Apparatus (SCBA):– the breathing system worn by fire-fighters to supply them with breathable air when fighting fires, during rescue operations and in any atmosphere that is oxygen deficient in the course of their work.

9.1.3 Overview of technologies for protective/intelligent clothing and textiles

Protective clothing and textiles

In general, there are five types of different hazards related to work place safety. These are chemical, thermal, mechanical (e.g. ballistic threats), nuclear (radiation) and biological hazards. Protective clothing often combines protection against several hazards. Several technologies can be identified which are (directly) linked to the before mentioned hazards.[306] The scope of this case study does not allow us to go into the (technical) details of these technologies. However, technologies from European companies are strongly involved. As an example, we focus here on thermal protection.

For first responders (and especially fire-fighters), one of the most important characteristics of there protective equipment should be that it is heat protective and flame retardent (often called 'heat and flame resistant'). According to Raheel *et al* there are three alternative methods for imparting flame resistance to textile goods:[307]

- Topical treatment in which fabric is treated with a flame-retardant agent;
- Built-in method in which a flame-retardant agent is added to the fibre-forming polymer in the manufacturing process of manmade fibres;
- Use of inherently heat- and fire-resistant fibres (FR-fibres).

The latter is the most common technology for fire-fighter suits. There exist a variety of heat protective and fire retardant fibres, which (according to Raheel *et al*) each has its own characteristics, niche and set of problems. The most well-known fibres are the 'aramid fibres' (like Kevlar, Nomex and Twaron), which were developed primarily for their inherent heat protective and fire retardant characteristics and high strengths. Other fibres are for example the modacryl fibres, viscose fibres (e.g. Lenzing) and polybenzimidazole fibers (e.g. PBI).[308]

However, it also should be mentioned that fibres are not essential anymore for reaching a high level of thermal protection. Strong technical innovation has made it possible that the current finishing technology can largely adapt fiber characteristics at the fabric level. So, fiber characteristics can be altered afterwards at fabric or garment level.[309]

Intelligent or smart clothing and textiles

Smart or intelligent textiles form a technological trend that is at very preliminary level of development. One definition of smart textiles is that these textiles '*are able to sense stimuli from the environment, to react to them and adapt to them by integration of functionalities in the textile structure. The stimulus as well as the response can have an electrical, thermal, chemical, magnetic or other origin*'. Advanced materials, such as breathing, fire-resistant or ultrastrong fabrics may be high-tech materials, but according to this definition they are not 'intelligent or smart'.[310]

---

[306] For technical details, see: Raheel, 'Protective Clothing Systems and Materials', New York, 1993.

[307] Raheel, Perenich, Kim, 'Heat- and fire-resistant fibers for protective clothing', in: Raheel, Protective Clothing Systems and Materials, p. 197 and further.

[308] ESF indicated to the study team that the difference between aramid-fibres and for example polybenzimidazole fiber (PBI) is not so crucial in the type of applications described in this study.

[309] Based on information provided by interviewees.

[310] Kiekens e.a. 'smart clothing: a new life', Ghent University, see: http://www.iafnet.com/files/iaf_03_presentations/Smart%20Clothing-%20a%20new%20life.pdf.

Kiekens identified three levels of 'intelligence':[311]

- passive smart textiles can only sense the environment, they are sensors;
- active smart textiles can sense the stimuli from the environment and also react to them, besides the sensor function, they also have an actuator function. Examples are shape memory, chameleonic, water-resistant and vapour, heat storage, thermo regulated, vapour absorbing, heat evolving fabric and electrically heated suits;
- very (or ultra) smart textiles take a step further, having the gift to adapt their behaviour to the circumstances.'A very smart or intelligent textile essentially consists of a unit, which works like the brain, with cognition, reasoning and activating capacities'.

There are several types of smart materials which are used in smart textiles, like phase changing materials (PCM) for thermoregulation (PCM absorbs a much higher amount of heat compared to normal material) and shape memory materials (potential to assume different shapes at certain temperatures).[312]

9.2 Market (demand-side) overview

9.2.1 Overview of main market (customer) segments

Personal protective equipment

As a consequence of the variety of risks (e.g. nature, heat, flames, chemicals) and situations in which they occur, the demand-side of the PPE-market is very fragmented. Broadly speaking, from the wide variety of government services and corporate companies that require certain types of protective clothing, the principal industry users of PPE are[313]:

- Engineering and manufacturing;
- Chemicals;
- Pharmaceuticals and food;
- Oil, gas and petrochemicals;
- Construction;
- Utilities; and
- Emergency services.

Protective clothing for first responders

The end-users of the protective clothing for first responders are rather clear:[314]

- Police forces (national, regional of local); and
- Fire brigades (mainly local and related to municipalities; there are also private fire brigades, for example for industrial companies and airports)

[311] Ibid, see footnote 310; see also the Mateo-project (part of the EC framework of the Interreg IIIC), 'State of the art in smart textiles and interactive fabrics', July 2006, see: www.mateo.ntc.zcu.cz/doc/State.doc.

[312] The Mateo-project.

[313] Textiles Intelligence, Editorial: Europe's Research Roadmap for new PPE, May 2009.

[314] First responders also include ambulance personnel, but these are not mentioned explicitly in this case study. The scope of the case study was limited to policemen and firemen.

In fulfilling their jobs, first responders (especially firemen) often have to deal with some of the more extreme hazards like heat, flames, chemicals and gases. In addition to the requirements that these hazards create for heat and flame resistant material (e.g. aramid fibres), there can also be additional requirements such as cut-proof material and high-visibility material.

As with the broader market for PPE, the market for first responders is also highly fragmented. While the police forces in the different Member States often are part of a national organisation which may organise collective purchasing of clothing and equipment, fire brigades more often act as local entities[315]. An example of this differing organisation of purchasing can be found in the Netherlands. The Dutch police have a central logistics division (KLPD Divisie Logistiek, now part of the vtsPN) which supplies (in principle) every policeman with the same equipment. By contrast, Dutch fire brigades are local or regional entities (often related to cities or municipalities) and, though there is some steering from the Ministry of Home Affairs, local fire brigades buy their own equipment. This is also the situation in France. In the UK, some initiatives have been taken to bundle the procurement process and in 2006, the non-departmental public body Firebuy was established to deliver English Fire and Rescue Service (FRS) procurement at national level.[316]

Box 9.2 Findings from interviews

From the interviews we carried out it became clear that there exist very 'mixed feelings' about the Firebuy initiative. Some interviewees expect that the bundling of demand will have a very strong impact on SME's which do not win the tender(s). One of the interviewees indicated that in the UK the Firebuy initiative has caused some resentment amongst various departments and some departments continue to source their own protective ensembles. There are many negatives associated with centralized buying and some positives, according to this interviewee. The centralized sourcing of garments would suggest that "one size fits all" when a rural fire department may experience very different daily activities than the fire department in a large industrial city. For centralized buys, the bidders usually need to have substantial financial assets and this would exclude many smaller suppliers that have equal or better solutions. Of course the benefit, is to drive the per unit price down due to volume buys.

Overall, the fire-fighter PPE market is seen as a stable market, with limited (demand) growth. This is related to the fact that it is primarily a 'replacement market' with a stable number of policemen and fire-fighter, with a limited amount of new end-users.[317] One of the interviewees however mentions that within Europe there is a tendency to professionalize the emergency services (especially fire fighters), which is related to the decreasing number of volunteers. The effect of this trend on the total market size is uncertain, as professional fire fighters might be equipped with more expensive gear.

[315] In addition to the high fragmentation of demand, local fire services often publish their requirements only in their own language, which can be a limiting factor for non-local suppliers..
[316] See http://www.firebuy.gov.uk/about_firebuy/firebuy/index.php.
[317] Frost & Sullivan, 'Firefighter PPE- the challenge and importance of winning and keeping contracts', August 2008.

9.2.2 International market profile and market size estimates

There are no (publicly available) estimations for the size of the European market for protective clothing.[318] Data on the global and European market for personal protection equipment (PPE) as well as for protective textiles is scarce, also.[319]

Textiles Intelligence estimated in 2009 that the global turnover for PPE is over €10 billion ($13 billion) per year[320, 321]. This turnover refers to four PPE-categories:

- Above-the-neck-protection (headwear, ear and eye protection);
- Protective clothing;
- Protective gloves;
- Footwear.

Both Euratex and the European Safety Federation (ESF) estimate the turnover of the European PPE-market at €10 billion[322]. This estimation is based on a previous calculation related to the Lead Market Initiative[323]. Of this total, Euratex estimate that protective textiles represent 50-60% of total turnover, while footwear (partly textile-based) adds another 20%. Six areas represent 80% of the turnover, namely (i) foul weather clothing (mainly leisure and active wear), (ii) fire resistant clothing, (iii) medical (non-woven) protection, (iv) high visibility, (v) ballistic & cut protection, (vi) disposable chemical protection[324].

The estimate of €10 billion turnover can be compared to earlier figures from Frost & Sullivan (2005)[325] that estimated that the total PPE-turnover in Western-Europe was €4.2 billion in 2003 (see Table 9.1). There analysis indicated that the segments for protective clothing and gloves are the 'predominant textile-based sectors' of the PPE market in

[318] When asked, Euratex, Promptex and the European Safety Federation (ESF) were not able to make an assessment on the size of the market; (a) Euratex is the European apparel and textile organisation. "EURATEX's main objective is to promote the interests of its members (apparel and textile industry) while taking into account the European Union's institutional framework and its international obligations". See: < http://www.euratex.org/content/about.html >; (b) the European Safety Federation (ESF) represents manufacturers and suppliers of PPE. One of their mission goals is "to create and promote health and safety management in the workplace". See: < http://www.european-safety-federation.org/functions/content.asp?Pag=6&pnav=;25 >; (c) Promptex is the 'European Federation for the Promotion of Procurement Contracts in Textiles and Leather', members are for example fabric and garment producers.

[319] Differences in definitions of PPE and approaches to measuring the size of the sector/market also have an important influence on estimates of size.

[320] Textiles Intelligence, Editorial: Europe's Research Roadmap for new PPE, May 2009.

[321] Initial and partial assessment made by the study team would suggest that this figure underestimates the size of the sector.

[322] Interview with Euratex and ESF.

[323] In the report of the 'Taskforce on protective textiles', composed in preparation of the Lead Market Communication, the size of the total European market for PPE (in relation to textiles) was estimated at € 8 billion, of which 85% is covered by the EU15. The Report uses a definition of PPE that covers 'clothing and other often textile-based systems and accessories whose main function it is to protect the user'. This definition is broader than the legal definition given in Article 1 of Directive 89/686/EEC. Euratex indicated to the study team that, for example, medical clothing and clean room textiles were included in the report, while these do not fall under the PPE-Directive. Further the Taskforce Report estimated (based on Euratex and Eurostat data) that in 2006 the EU-25 market for textile industrial applications was approximately € 39.4 billion, of which protective textiles was one of the largest segments (20%). The Report also estimated that 200,000 jobs are directly or indirectly linked to the PPE industry. The service operations related to PPE (work wear and healthcare segments) account for € 1.5 – 2 billion turnover and 35.000- 40.000 employees.

[324] European Commission, Report of the Taskforce on Protective Textiles: 'Accelerating the development of the protective textiles market in Europe', composed in preparation with COM (2007) 860 on 'A Lead Market Initiative for Europe'.

[325] Frost & Sullivan, 'Personal Protective Equipment in Western Europe provides Growth opportunities for technical textiles', press release June 2005.

Western Europe. In 2003, the turnover of protective textiles and gloves accounted for approximately €2.5 billion (60% of the total PPE-market in Western Europe).

Based on estimates of the average cost of equipping first responders, Table 9.2 provides a very rough estimation of the market value of protective clothing for first responders. Given a three-year depreciation period, the estimated annual market size is approximately €525 million to €875 million.

Table 9.1 Turnover for Personal Protective Equipment (PPE) in Western-Europe (€ million)

	Turnover 2003	Turnover 2008 (estimated)
Protective clothing	€ 1,400	€ 1,900
Protective gloves	€ 992	€ 1,114
Sub-total	€ 2,392	€ 3,014
Head protection & footwear	€ 1,775	€ 1,847
Total	**€ 4,167**	**€ 4,861**

Source: Frost & Sullivan (2005)[326]

Table 9.2 Estimated market value protective/ intelligent textiles for (professional) first responders

EU-27	Price [3]	Market value
Fire-fighters - number		
1.483.804 [1]	€ 550 (low) € 1,000 (high)	€ 816 million € 1.484 million
Policemen - number		
1.518.012 [2]	€ 500 (low) € 750 (high)	€ 759 million € 1.139 million
Total (low price scenario)		**€ 1.575 million**
Total (high price scenario)		**€ 2.622 million**

Notes:

[1] Based on the number of fire-fighters in 19 Member States (related to population) an estimate is made for the EU-27 (use of Eurostat data).

[2] Based on the number of policemen in 25 Member States (related to population) an estimate is made for the EU-27 (use of Eurostat data).

[3] One interviewee estimated the price of a full equipped fire-fighter at approximately € 750 to € 1,000 (without SBCA), the price for a policeman is lower, but > 50% compared to a fire-fighter. Another interviewee thought it would be more realistic to use €550,- as a minimum for fire-fighters.

An important assumption here is that all police and firemen are fully equipped, which might not always be the case. Another assumption is that the Eurostat data refers to professional fire-fighters and not to volunteers (that's not clear from the data set). Several stakeholders refer to the fact that only Germany has approximately 1.5 million fire-fighters, most of them being members of voluntary fire brigades.

9.2.3 European production profile

Based on Eurostat (Prodcom) data it is possible to provide an overview of the value of production sold of certain PPE related products. Table 9.3 shows that the total EU-27 production value of protective gloves in 2008 was approximately € 33 million, with Italy

[326] Ibid. Footnote 210.

and the UK being the biggest producers. Italy is also the biggest producer of safety headgear, while Germany is the main supplier of breathing appliances and gasmasks.

Data was not available for fire-resistant and protective safety clothing.[327]

Table 9.3 EU production value of manufactured goods (in €)

	Protective gloves		Safety headgear		Breathing appliances and gas masks	
	2007	2008	2007	2008	2007	2008
Bulgaria	N/A	114,000	133,000	N/A	36,000	N/A
Czech Rep	N/A	222,000	N/A	N/A	N/A	N/A
Denmark	718,000	N/A	1,521,000	N/A	N/A	N/A
Germany	1,573,000	1,489,000	84,863,000	81,253,000	271,715,000	289,875,000
Spain	2,961,000	N/A	23,082,000	25,333,000	5,022,000	3,462,000
France	N/A	N/A	26,498,000	45,364,000	74,784,000	51,015,000
Italy	486,000	5,870,000	237,119,000	212,675,000	N/A	218,000
Hungary	571,000	449,000	N/A	N/A	N/A	N/A
Poland	1,813,000	2,627,000	6,876,000	N/A	N/A	N/A
Portugal	N/A	N/A	16,628,000	N/A	N/A	N/A
Romania	1,476,000	1,084,000	N/A	N/A	N/A	N/A
Slovenia	N/A	862,000	N/A	N/A	N/A	N/A
Finland	N/A	N/A	1,371,000	358,000	1,6991,000	16,844,000
Sweden	N/A	N/A	N/A	N/A	40,945,000	40,562,000
UK	3,555,000	3,961,000	93,186,000	80,048,000	140,345,000	125,531,000
EU-27	**33,247,000**	**32,827,000**	**584,838,000**	**569,169,000**	**550,567,000**	**530,205,000**

Source: Eurostat (Prodcom)[328]

Notes:

- Protective gloves: Protective gloves, mittens and mitts for all trades, of leather or composition leather (NACE 3299.1130);
- Safety headgear: safety headgear (NACE 3299.1150);
- Breathing appliances and gas masks: Breathing appliances and gas masks, excluding therapeutic respiration apparatus and protective masks having neither mechanical parts nor replaceable filters (NACE 3299 5910).

[327] The manufacturing of protective safety equipment (which includes (i) the manufacturing of fire-resistant and protective clothing and (ii) the manufacturing of fire-fighting protection suits) is covered in NACE Rev. 2 number 32.99 (other manufacturing n.e.c.). The Eurostat / Prodcom database did not cover these subcategories on a 6 or 8 digit level.

[328] Prodcom data: http://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_NOM_DTL&StrNom=PRD_2009&StrLanguageCode=EN&IntPcKey=23060748&StrLayoutCode=&CFID=537825&CFTOKEN=cbc18aa3a3b6590b-A9262B34-9858-D7B4-35101E0EC8AF753A&jsessionid=f900627cf766636c451e

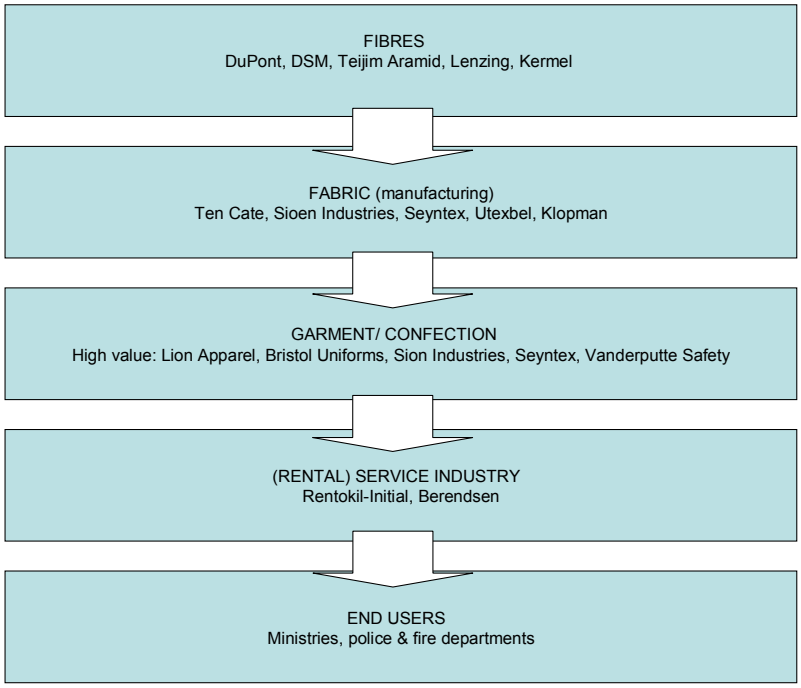
9.3 Description of the supply (value) chain

9.3.1 General description and overview

The supply side of the PPE-market is characterised by the presence of a large number of market players[329]. The PPE-market is very broad and the PPE-industry is serving a diverse range of different industries and services. All these industries and services have to provide a certain level of working protection to their employees, but working conditions, risks and the level of needed protection differ per sector and company. Many of the PPE providing companies focus on certain niche markets.

The supply chain for protective clothing for first responders is illustrated in Figure 9.1. The first part of the supply chain (fibres and fabric) is dominated by a group of global market players. Further downwards in the chain, the supply-side gets less concentrated and is dominated by smaller firms or SMEs (garment, textile rental), which often focus on certain niche markets or only serve local (or regional) clients. Frost & Sullivan confirms that the (downstream) Western-European market for fire-fighter PPE is 'extremely' fragmented and state that 'there are many small manufactures in each country that have established ties with local fires services'[330].

Figure 9.1 Overview of the supply chain for protective clothing for first responders



Source: ECORYS

Note: The mentioned companies are examples; this is not an exhaustive list.

[329] Koncept Analystics, 'PPE market: an analysis', April 2009.

[330] Frost & Sullivan, 'Firefighter PPE- the challenge and importance of winning and keeping contracts', August 2008. One of the interviewees indicated that for non-textile related PPE like helmets, respiratory protection and eye protection the market is rather concentrated.

9.3.2 Overview of main market players

Main fibre developers

Pertaining to the protective clothing for first responders the fibres are an important technology. As mentioned before, current finishing technology is such that fibre characteristics can also be adapted at the fabric level.

Fibres have their own characteristics and are for example heat protective and fire-retardant, very strong or entirely waterproof. The development of these fibres requires very specific technical expertise and very high investments. Therefore, this part of the supply chain is dominated by important (global) players like:

- DuPont (Kevlar and Nomex) - Table 9.4;
- Teijin Aramid (Twaron) - Table 9.5;
- DSM (Dyneema) - Table 9.6
- Lenzing (Lenzing FR) - Table 9.7
- Others, like Kermel[331] and PBI[332]

The market shares of the different main players are uncertain, but DuPont and Teijin Aramid are believed to have the highest market share. The DSM-fibre is characterised by its strong cut protection (bullet-resistant vests), while the other fibres (mainly) have heat protective and fire- retardant characteristics.

The origin of most of the big (global) fibre producers is in the chemicals industry and they have very broad product portfolios, which go beyond the fibre-market. At the same time, the big chemical companies like DuPont and DSM, are currently focussed on the high-end market and over the last ten to fifteen years they have divested their low-end activities, which were often sold to Turkish and Asian companies.

Recently, the trend is more towards blending of fibres, as blends enable a better combination of performance and protection. One interviewee indicated that Lenzing and Tejin Aramid are better positioned herein, while Dupont prefers to sell 100% Nomex. Finishing blends demand more expertise on behalf of textile firms.

[331] Kermel, a French company which focuses on four end-markets: (i) technical uses (gas filtration, (ii) industry (workwear), (iii) military and public order (pilot jackets, tank crew coveralls, fire resistant NBC suits and anti-riot garments), and (iv) fire-fighters (fire suits, gloves). The Kermel fibre is an aramid fibre and is characterised by its non-flammability. Specific company figures (employment, turnover) are not available.

[332] PBI Performance Products Inc. produces the polybenzimidazole (PBI) fibre. Specific company figures (employment, turnover) are not available.

Table 9.4 DuPont: Basic company indicators

DUPONT (US)				
Main indicators	**DuPont**		**Safety and Protection Division**	
	2007	2008	2007	2008
Turnover	€ 21,436m	€ 20,757m	€ 4,116m	€ 3,895m
Profit	€ 2,731m	€ 1,626m	N/A	N/A
R&D budget	€ 976m	€ 947m	N/A	N/A
Number of employees	60,000	60,000	N/A	N/A
Description of the company				
DuPont is (mainly) a chemical company, which provides a broad range of 'science-based solutions' related to (for example) health care, safety and security and electronics. The Safety & Protection division (one of the main five) covers a broad range of safety products for all kinds of industries, like construction, transportation, communications, industrial chemicals, oil and gas, electric utilities, automotive, manufacturing, defense, homeland security and safety consulting. Pertaining to the major demanding industries, the textile/apparel industry represents 23% of the total division sales (€ 976 million or $ 1.3 billion). Approximately € 976 million ($1.3 billion) of division turnover is realized in 'Europe' (which includes the Middle-East and Africa).				
Main products and technologies				
▪ One of the main product groups of the Safety & Protection division is related to aramid fibers. The aramid products represent 27% of the total division sales (€ 1 billion or $ 1.5 billion). Nomex and Kevlar are the most common fibers pertaining to personal protection, for example for the military, law enforcement personnel, workers in the oil and gas industry, firefighters and other first responders. ▪ Nomex is a high temperature resistant aramid fibre with an inherent and permanent flame and heat protection (engineered into the molecular structure of the fiber instead of chemical treatment). Nomex is used for example for fire-fighters turnout gear. The Kevlar fiber is, according to the DuPont website, characterized by its high resistance to cuts, abrasion and high temperatures. Kevlar is for example used in protective gloves.				

Source: DuPont website (www.dupont.com) and *Annual Report 2008*

Table 9.5 Teijin Aramid: Basic company indicators

TEIJIN ARAMID (JP)		
Main indicators	**Teijin Aramid**	
	2007	2008
Turnover	€ 5,827m	€ 5,814m
Profit	€ 476m	€ 432m
R&D budget	€ 194m	€ 202m (fibers: 5%)
Number of employees	18,819	19,053
Description of the company		
Teijin Aramid is part of Teijin Limited, the (Japanese) holding company of the Teijin Group. The holding company encloses approximately 150 companies in more than 10 countries which mainly focus on chemical materials and solutions. There are five main fields of operation: (i) synthetic fibers, (ii) films and plastics, (iii) pharmaceuticals and home health care, (iv) trading and retail, and (v) IT and new products. The Teijin Group bought the company Aramid (with the Twaron fiber) in 2000, which was part of the Dutch chemical company Akzo-Nobel. The fiber business group (including polyester fibers and high performance fibers like the aramid fibers) contributed in 2007 approximately 29% to the net sales.		
Main products and technologies		
▪ Teijn Aramid owns now three types of aramid-fibres, which are Twaron, Teijinconex and Technora. These fibres are used for a wide variety of products, for example products for heat-, cut- and ballistic-protection, tires, communication cables, ropes and cables. Friction material (33%) and protective clothing (22%) are the main applications for para-aramid fibers. Twaron and Teijnconex are the most important ones pertaining to heat protection solutions. ▪ Twaron is a very strong, light para-aramid fiber, which has a high modulus, is thermally stable, and is highly impact and chemical resistant. One of the applications of this fibre are heat-protection products, for example brigade uniforms, fire extinguishing blankets, fire-blocking layers in airplane seats, and applications in the metal-processing and glass industries. Teijinconex is a meta-aramid fiber which is also used for heat-resistant material, like fireproof clothing.		

Source: Teijin Aramid Annual Report 2007, Teijin Aramid website (www.teijinaramid.com)

Table 9.6 DSM: Basic company indicators

DSM (NL)				
Main indicators	**DSM**		**Performance Materials Cluster**	
	2007	2008	2007	2008
Turnover	€ 8,921m	€ 9,439m	€ 2,390m (€ 259m related to DSM Dyneema)	€ 2,297m (€ 305m related to DSM Dyneema)
Profit	€ 823m	€ 903m	N/A	N/A
R&D budget	€ 372m	€ 394m	€ 113m	€ 127m
Number of employees	23,254	23,591	4,978	4,592
Description of the company				
Royal DSM is a Dutch chemical company with a wide range of product applications. There are five main clusters: (i) nutrition, (ii) pharma, (iii) performance materials, (iv) polymer intermediates, and (v) base chemicals and materials. The cluster 'performance materials' includes the business group DSM Dyneema-fiber (besides DSM engineering plastics and DSM Resins). Types of end-use markets for this business line are: the automotive industry, the aviation industry, the electrics & electronics industry, the sports and leisure industries, the coatings industry and the construction industry.				
Main products and technologies				
The main product in relation to protective clothing is the DSM Dyneema fiber. This is a 'superstrong polyethylene fiber that offers maximum strength combined with minimum weight'. It can be used for different solutions, for example related to personal protection (bullet-resistant vests, helmets), but also textiles (protective gloves, protective sportswear, industrial textiles).				

Source: DSM website (www.dsm.com) and *Annual Report 2008*

Table 9.7 Lenzing: Basic company indicators

LENZING (AT)				
Main indicators	**Lenzing**		**Fibres Business Units**	
	2007	2008	2007	2008
Turnover	€ 1,261m	€ 1,329m	€ 1,069m	€ 1,108m
Profit	€ 151m	€ 114m	N/A	N/A
R&D budget	€ 18,2m	€ 18,8m	N/A	N/A
Number of employees	5,918 *	5,945 (EU: 3,745)	N/A	N/A
Description of the company				
The Lenzing Group consists of several companies (headquarter in Austria) which are active in fibers and plastics. They 'provide the global textile and nonwovens industry with high-quality cellulose fibers'. Fibers are the main business field of Lenzing, besides plastics and engineering. In 2008, the turnover was € 1.3 billion; 82% of this turnover was related to fibers (€ 1.1 billion). The two main business units related to fibers are (i) fibers for textile applications and (ii) fibers for the nonwovens industry. Approximately 39% of total turnover was realized in Europe and 52% in Asia. 4				
Main products and technologies				
The Lenzing Group owns four fibres, Tencel, Lenzing Modal, Lenzing Viscose and Lenzing FR. The latter protects against heat and flames. The Lenzing FR fibre is a 'specialty viscose fiber', and offers protection from heat and flame. According to the website, the Lenzing FR fiber is used in a wide range of applications, for example protection from fire, radiant heat, electric arcs, molten metals and flash fires. It is used by fire brigades, as well as police forces. In 2007, Lenzing started cooperation with TenCate. Together, they developed a new production line of flame retardant uniforms for the US Armed Forces (TenCate Defender M).				
*Note: * excluding staff of discontinued operations*				

Source: Lenzing Annual Report 2008, Lenzing website (www.lenzing.com)

Main manufactures (fabric)

The next level of the supply chain consists of the manufacturing of the protective clothing fabrics. As mentioned before, the fabric companies are currently able to add fibre characteristics to the fabrics with their current finishing technology. One interviewee indicates that since the variety of inherently flame-retardant fibers are limited, the fabric manufacturers must create unique blends based on specific performance requirements. This also functions as a method for differentiation. There are several (global) manufactures, such as:

- TenCate - Table 9.8;
- Ibena Textilwerke - Table 9.9;
- Utexbel - Table 9.9;
- Seyntex - Table 9.9;
- Klopman -.Table 9.9.

Although market shares are unknown, TenCate (NL) is seen as the global market leader for manufacturing fabrics for protective clothing. Seyntex is also active on the garment level.

Table 9.8 TenCate: Basic company indicators

ROYAL TENCATE (NL)				
Main indicators	**Royal TenCate**		**Advanced Textiles and Composites**	
	2007	2008	2007	2008
Turnover	€ 886m	€ 1,033m	€ 350.3m	€ 481m
Profit	€ 58.1m	€ 46.2m	N/A	N/A
R&D budget	€ 8.2m	€ 7.9m	N/A	N/A
Number of employees	4,020	4,437	N/A	N/A
Description of the company				
Royal TenCate is a Dutch company that manufactures 'advanced materials'. These materials are for example used for protective clothing, in the aerospace industry, in antiballistics, for civil engineering projects, in horticulture, in fish farming, for the manufacture of tents and awnings and in the installation of artificial grass pitches. Ten Cate is divided into three sectors: Technical Components, Geosynthetics & Grass and Advanced Textiles & Composites. The latter division consists of four market groups, namely (i) TenCate Protective Fabrics, (ii) TenCate Outdoor Fabrics, (iii) TenCate Space & Aerospace Composites and (iv) TenCate Armour Composites. In 2004, TenCate acquired Southern Mills (US) for approximately € 29 million ($ 36 million). At that time, Southern Mills was (one of) the US market leaders in flame- and heat retardant fabric.				
Main products and technologies				
TenCate Protective Fabrics claims to be the market leader in America and Europe in the field of protective fabrics, as well as the world's leading manufacturer of fire protective clothing fabrics. There are four main collections of protective fabrics: Tecasafe, Tecashield, Tecapro and Defender M. The Protective Fabrics division is active on four main markets: industrial safety, military, services and industry and emergency response. Emergency responders mainly use the Teceshield collection. The TenCate Tecashield® collection is a range of inherently flame- & heat-resistant fabrics. The multiple of fabric solutions within this collection is enormity and can be subdivided in two marktsegments: industrial safety and emergency response. TenCate Defender M is an inherently heat- and flame-resistant military fabric (with Lenzing FR).				

Source: Ten Cate Annual Report 2008, TenCate website (www.tencate.com)

Table 9.9 Ibena, Utexbel, Seyntex, Klopman: Basic company indicators

Company	Description
IBENA	Ibena Textilwerke is a large German textile company which is active in weaving, finishing and sewing. They have production facilities in Germany, the Czech Republic and China. They have two main operating divisions, (i) home textiles and (ii) technical textiles (TECHTEX). The latter division produces fabrics for flame retardant textiles (product group 'Ibena Protect'), automotive textiles, technical decoration fabrics, etc. Ibena offers, inter alia, fabrics based on DuPont fibers (they are a official 'Nomex quality partner'). Annual turnover of the Ibena Group is over € 100 mn and they employ approximately 400 people worldwide.[333]
UTEXBEL	Utexbel is a Belgian company which is mainly active in spinning (three mills), weaving (two mills), dyeing (2 units), coating and printing. They have two divisions, a yarns division and a fabrics division. The latter produces fabrics for garments (work, protection and career wear, sportswear, casual wear) and technical and industrial applications. Utexbel has an annual turnover of € 105 million (80% export) and employs 990 people.[334]
SEYNTEX	Seyntex is based in Belgium and is active in weaving, knitting, dyeing, finishing, coating, textile printing and manufacturing of textiles. Currently, they employ 1,200 people (global) and produce (amongst others) fire-fighter suits, police and military products.[335] In 2007, their turnover was approximately € 115 million.
KLOPMAN INTERNATIONAL	Klopman International started in the 1960, with the production of polyester/cotton blended fabric in Italy. They supply both protective clothing (for example for agriculture, cleaning, healthcare, police military and emergency service) as well as casual clothing. Besides the workwear (main focus) they have also developed various kinds of PPE-fabric, like fire-retardent, antistatic and chemical resistant textiles. In 2008, Klopman was acquired by MW Unitexx S.A., a subsidiary of MW Corp of Mumbai (India).[336] In 2008 their turnover was around € 135 million.
OTHERS	Some other companies were mentioned by the interviewees. However, the information on their websites was too limited to present it here in more detail. • BE: Cordia • ES: Teijdos Estambril, Textil Santanderina, Sati Grupo Textil[337] • DE: Theodolf Fritsche GmbH & Co[338] • FR: Europrotect, TDV[339] • IT: Tessitura Majocchi, Mextex[340] • UK: Carrington Career & Workwear, TBA Textiles, Eagle Technical Textiles (also garment)[341]

[333] < http://www.ibena.de/english/Ibena/ibena.html >.
[334] < http://www.utexbel.com/aboutEN.html >.
[335] < http://www.seyntex.com/companyinfo.aspx?lang=english >.
[336] < http://www.klopman.com/pages/industryselector/index.asp?sectionID=9 >.
[337] See: < http://www.estambril.com/index.php?option=com_content&task=view&id=1&Itemid=2 > (The Estambril Group produces, inter alia, fire-retardant fabrics (fire-fighters), but also fabrics for police forces), < http://www.techs.es/index_eng.htm > and < http://www.textilsantanderina.com/textil_santanderina_eng.html (Textil Santanderina produces technical textiles, inter alia, fire-retardant fabrics (fire-fighters), < http://www.sati.es/ >.
[338] See: < http://www.tfritsche.de/firmeninfo.htm > or < http://www.techtextil.net/ >.
[339] See: < http://www.europrotect.fr/flash/index.html >, < http://www.tdv-industries.fr >.
[340] See: < http://www.mectex.it/eng/phtl2.htm >.
[341] See: < http://www.carrington.uk.com/index.asp >, < http://www.tbatextiles.co.uk/index.php > (specialised in first responder PPE, turnover in 2008 was approximately € 31 mn), < http://www.eagletechnicalfabrics.com/index.html > (turnover in 2008 was approximately € 31 mn).

Main suppliers (garment)

At garment level the market the concentration level is very low, both for high-end and low-end quality protective clothing. Often, (local) fire and police departments buy their products from local (or regional) garment companies. There are some bigger companies active on the market, like:

- Seyntex, - Table 9.9 (above);
- Sioen Industries - Table 9.10
- Lion Apparel - Table 9.11;
- Bristol Uniforms - Table 9.11;
- Remploy Frontline - Table 9.11;
- Cosalt - Table 9.11;
- Arlen - Table 9.11;
- Vandeputte Safety - Table 9.12 (they do not produce garments itself).

Table 9.10 Sioen Industries: Basic company indicators

SIOEN INDUSTRIES (BE)		
Main indicators	**Sioen Industries**	
	2007	2008
Turnover	€ 380m	€ 350m
Profit	€ 30m	€ 6.5m
R&D budget	N/A	N/A
Number of employees	N/A	4,676
Description of the company		
Sioen Industries is a Belgian company which is active both at fabric and garment level. Sioen employed in 2008 4,676 people, but only 1,619 were employed in the EU (BE: 899, DE: 6, FR: 291, IE: 33, NL: 27, PL: 338, PT: 25). In Indonesia 2,222 people work for Sioen and in Tunisia 757 people. Nearly 70% of the total number of employees works for the apparel division, but a lot of those people work outside the EU.		
Main products and technologies		
They have four main divisions, namely (i) coating, (ii) industrial applications, (iii) chemicals and (iv) apparel. The latter also designs and produces protective clothing.		

Source: Sioen Industries website (www.sioen.com) and *Sioen Industries Annual Report 2008.*

Table 9.11 Summary table: Other market players

Company	Description
LION APPAREL	Lion Apparel is a US based firm (Ohio) and claims to be a 'global leader in the production and distribution of apparel for fire-fighters, police, emergency services, government agencies and military organizations'. They have several subsidiaries in Europe, like in France, UK and Germany. Further, they employ approximately 800 people (global). Lion's main three markets are the emergency services, military and civilian agency uniform, and the personal equipment markets. Lion Apparel has several partners, like DuPont, Kermel and W. L. Gore (Gore-tex membrane). Lion apparel is also active in the support services. In 1998 they started with the TotalCare service program for the London Fire Brigade. This service program provides a couple of services, like advanced inspection, cleaning and decontamination, repairs, documentation and tracking. They claim that there service program for PPE covers over 40,000 fire fighters around the world.[342]
BRISTOL UNIFORMS	Bristol Uniforms is a UK based company which designs and manufactures protective equipment for firefighters (fire service, airport, marine, industry and wildland). An after care service is provided by 'Bristol Care' for all types of protective clothing worn by police forces. Bristol Uniforms cooperates with DuPont, W.L. Gore (Gore-tex membrane) and 3M (high visibility solutions).[343]
REMPLOY FRONTLINE	Remploy Frontline is part of Remploy Group (UK based). They are strong in CBRNE and marine protective solutions, but also provide protection for first responders. The annual turnover of the Remploy Group is approximately € 207 mn.[344]
COSALT (BALLYCLARE)	Cosalt is specialized in marine and off-shore safety, but also provides fire-fighting equipment like suits and breathing apparatus (Ballyclare division). In 2008, the Cosalt Group realized a turnover of approximately € 125 mn.[345]
ARLEN	Arlen is a Polish garment supplier of PPE and produces (inter alia) fire-retardant garments, as well as anti-static, chemical and high-visibility garments. The Arlen Textile Group employs over 1,000 people.
Others	The interviewees mentioned some more companies, but the information available (mainly on their websites) was too limited to present here in more detail. • DE: Alwit GMBH, Fuchshuber Techno-Tex, HF Sicherheitskleidung[346] • ES: Fabrica Española de Confecciones, Confecciones Oroel[347] • IT: Italy Grassi, Siggi Group, Tacconi, Ariete Group[348] • NL: Van de Mark and Safety Masters[349] • UK: Bennett Safetywaer[350]

[342] < http://www.lionapparel.com >.
[343] < http://www.bristoluniforms.com >.
[344] < http://www.remployfrontline.co.uk/index.php?option=com_frontpage&Itemid=1 >
[345] < http://www.cosalt.com/ >
[346] < http://www.alwit.de/uk/index.php?option=com_frontpage&Itemid=1 > (ALWIT GmbH is a German company and specialized in manufacturing heat protective clothing and gloves. Their fire-fighters PPE covers fire-fighting suits, fire hoods, neck curtains and gloves. They employ approximately 20 people, there is no indication of their turnover); < http://www.fttex.com/index_en.html >, < http://www.hf-sicherheitskleidung.de/Seite1_ie.htm >.
[347] See: < http://www.fecsa.net/es/ >, < http://www.oroel.com/web/empresal.asp >.
[348] See: < http://www.grassi.it/index.htm >, < http://www.tacconi-spa.it/ >, < http://www.ariete-group.it/sito2008/index.php?lang=eng >.
[349] See: < http://www.willemvandermark.nl >, < http://www.safetymasters.nl/website/TLL/sm1.php >. In October 2008, Safety Masters took over the fire-fighter division of Carhartt (http://www.carhartt.com).
[350] See: < http://www.bennettsafetywear.co.uk/ > (annual turnover approximately € 25 mn).

Table 9.12 Vandeputte International: Basic company indicators

VANDEPUTTE INTERNATIONAL (BE)				
Main indicators	**Vandeputte International**		**Related to PPE**	
	2007	2008	2007	2008
Turnover	€ 73m	€ 80m	€ 35m	€ 39m
Profit	€ 1.7m	€ 2.8m	N/A	€ 0.5m
R&D budget	N/A	N/A	N/A	N/A
Number of employees	186 (BE: 138)	193 (BE: 147)	N/A	N/A
Description of the company				
The (Belgian) Vandeputte Group ('Vandeputte International') is mainly active in Belgium, France, the Netherlands and Germany. They consists of three divisions: (i) Vandeputte Safety, which focuses on the development and distribution of a complete range of high-quality personal protective equipment, (ii) Artelli provides a specific support service for resellers and wholesale distributors, and (iii) Samurai@Work offers a complete package of services in fields of activity such as safety, ergonomics, industrial hygiene, embellishment of the workplace and environment.[351] They also offer a 'Concept for Safety' (C4S) which provides solutions pertaining to consultancy, e-bussiness, logistics, but also repair and maintenance.				

Source: VandePutte website (www.vdp.com)

Support services

There are several companies who provide additional 'support services', which can vary from a first risk assessment (which clothing does an end-user actually need?) to logistics, cleaning and replacements of the protective textiles. The market for additional support services is very fragmented and a lot of the services are provided by (local) SMEs, but full service is offered by companies like Bristol Uniforms (Bristol Care), Lion Apparel (TotalCare) and Vandeputte Safety (C4S). Further, there are also a number of 'textile rental firms'[352], like:

- Rentokil-Initial - Table 9.13
- Davis Service Group (Berendsen) - Table 9.14
- Others, like Alsco (DE/IT), Bardusch (DE), Elis (FR), Mewa (DE), Johnson Service Group (UK) – details are not shown in this study.

[351] < http://www.vdp.com >.

[352] These textile rental firms are organised in the European Textile Services Association (ETSA) with 13 active members.

Table 9.13 Rentokill-Initial: Basic company indicators

RENTOKIL-INITIAL (UK)				
Main indicators	**Rentokil-Initial**		**Textiles and Washroom Services Division**	
	2007	2008	2007	2008
Turnover	€ 3,219m	€ 3,014m	€ 881m	€ 769m
Profit	€ 310m	€ 103m	N/A	N/A
R&D budget	N/A	N/A	N/A	N/A
Number of employees	> 78,000	78,000	9,682	9,772
Description of the company				
Rentokil-Initial was originally based in the UK and started as a pesticide provider and insect killer. Currently, Rentokil-Initial provides all types of services, like cleaning services, courier services, E-security, facilities services, washroom services, and linen, garment and floorcare rental. They claim to be one of the largest 'business services companies' in the world. In Europe, they have specialized in the supply and laundering of workwear, uniforms, clean room uniforms and protective equipment. The 'Textiles and Washroom Services' division covers washroom, linen hire, garment rental, and floorcare activities in (specially) the UK and continental Europe.				

Source: Rentokil-Initial website (www.rentokil-initial.com) and *Annual Report 2008.*

Table 9.14 Davis Service Group: Basic company indicators

DAVIS SERVICE GROUP Plc				
Main indicators	**Davis Service Group**		**Workwear**	
	2007	2008	2007	2008
Turnover	€ 1,201m	€ 1,198m *	N/A	€ 396m
Profit	€ 156m	€ 147m	N/A	N/A
R&D budget	N/A	N/A	N/A	N/A
Number of employees	N/A	17,300 **	N/A	N/A
Description of the company				
Berendsen was originally founded in Denmark and is currently owned by the Davis Service Group Plc. which focuses on textile rental services and textile maintenance. Berendsen 'rents, launders and maintains all kinds of workwear for companies'. Berendsen offers a wide range of hard-wearing, functional workwear for industry, workshops and service companies'. The Berendsen Group consists of an international network of local companies in nine European countries (Nordic countries and continental Europe). In the UK and Ireland the Davis Service Group is active under the name of Sunlight Service Group and Spring Grove Services (Ireland) Limited.				
** €411 million in the Nordic countries,€284 million in continental Europe and €504 million in the UK and Ireland;* *** 7,500 employees for the Berendsen Group and 9,800 for Sunlight Service Group and Spring Grove Services.*				

Source: Davis Service Group website (www.dsgplc.com) and *Annual Report 2008.*

9.3.3 Technology aspects

Technology aspects have been discussed before (see section 9.1.3 and 9.3.2). Main point which is made is that fibres are an important technology, but technology now allows also manufacturing companies to add 'fibre characteristics' to the fabric.

9.3.4 Fibres and fabric supply

Production of fibres

At the fibre level (aramid) the market is dominated by DuPont (US) and Teijin Aramid (NL/Jap). The main fibre producers have been described in section 9.3.2. For big chemical companies like DuPont, Teijn Aramid and DSM the production of fibres is only one of their activities. Despite the number of European companies, this cannot be seen as a European specialisation.

Production of fabrics

There are several European companies active in the manufacturing of the protective clothing fabrics (e.g. TenCate, Ibena and Seyntex). Although the structure of the fabric market is less concentrated than the fibre market, in the past there has been a strong consolidation trend. There are also companies in the new European Member States that are supplying fabrics, but these are mainly SMEs with strong ties to their local (or regional) market.

European companies have focussed on fabrics for high-end quality protective clothing (e.g. fire-fighter suits), where market entry barriers are high (given the necessary technical and market knowledge as well as large investments) and Europe is (still) able to remain competitive. However, the (large) differences in wages and production costs mean that low-end quality fabrics are mainly produced in the Far East.

9.3.5 Confection / garment production

Some of the European producers of protective garment have been described in section 9.3.2. Low-end products are mainly produced in the Far East, while high-end products like fire suits are (still) produced in Europe. There are however some exceptions, with companies producing their (high-quality) garment in the Far East, but based on very strict technical specifications. In eastern-Europe both low-end and high-end products are produced (often by outsourcing).

9.3.6 Related 'support' services

Both the end-users and suppliers of protective clothing for first responders are becoming increasingly aware of the necessity of additional 'support services'. The range of these offered services is very broad and can vary from a first risk assessment (which clothing does an end-user actually need?) to logistics, cleaning and replacements of the protective textiles. One of the interviewees indicates that this awareness should be reflected in adequate procurement strategies in which the demand is created for PPE products that provides the best value for money in terms of full life cycle management. This will raise the bar for all PPE producers and optimize the quality of PPE in relation to the requirements of end users in practice.

Cleaning services

Given the fact that a dirty fire suit may limit the effectiveness of the protective elements (like the heat and flame retardant layers) and increase hazards (dirt can burn), attention for clean equipment is very important. Several interviewees paid attention the issue

stating, for example, that fire brigades (professional, but also voluntary) use washing machines programmed on the special need for fire-fighter PPE. However, interviewees also pointed out that the importance of clean textiles is sometimes (still) very low.[353]

Sometimes end-users wash their protective equipment at home, without certain expertise or attention for washing instructions.[354] ETSA has indicated that this is, for example, a problem with high-visibility textiles. Washing without following the instructions might influence the performance of the high-visibility textiles in a negative way, to the extent that they may even below the minimum CE- requirements. This issue is also related to the liability of employers, who are responsible for the safety of their employees. Employers seem to be more and more aware of this.

The market for washing and cleaning of clothing services is very fragmented. A lot will be done by (local) SMEs, but full service is offered by companies like Bristol Uniforms (Bristol Care), Lion Apparel (TotalCare) and Vandeputte Safety (C4S).

Clothing/textile rental services

There are also a number of 'textile rental firms', who offer end-users a broad range of solutions. The total size of the market for textile rental is € 9.9 billion (2007).[355] Approximately 35% (€ 3.5 billion) of this turnover is related to 'workwear'.[356] Regarding the total workwear turnover, Germany/Austria/Switzerland represent the largest geographical market (€ 1.2 billion), followed by France/Italy/Spain/Portugal/Greece (€ 970 million), UK/Ireland (€ 565 million), Scandinavia/Finland/Benelux (€ 621 million) and the new Member States (€ 150 million).

These textile services cover a 'timely and cost-effective provision of textiles, usually on a rental contract basis, to professional end-users'.[357] The end-users rent (or lease) certain protective equipment from these companies, while they offer a 'full service' which may include (i) investment in the stock of textile goods, (ii) management of the stock according to the evolution of the customer's needs, (iii) pick-up of soiled items, (iv) delivery of professionally cleaned, repaired and quality-checked textiles, (v) access to professional expertise in logistics, textile purchasing, textile maintenance and processing for an optimized service for each customer, (vi) wide range of products and (vii) product and service solutions tailored to the individual needs of companies and each member of staff.[358]

Examples of these textile rental firms are big players like Rentokil-Initial and Berendsen. Given the fact that a complete fire suit (without SCBA) costs approximately € 750- 1,000 per fire fighter, this needs quite a lot of investments. One of the interviewees indicated that currently (due to economic pressure on costs and investments) more companies who

[353] We heard some example of fire suits which were only washed once or twice a year and often not by professional services.
[354] It is not always necessary to hire a specialised company for washing. In some procurement processes the possibility to wash 'at home' (or in the station itself of course) is an important item.
[355] ETSA, 'Textile Rental Market Survey 2007, published in June 2008.
[356] Workwear refers in this survey to textile-related PPE (it excludes: garments worn in healthcare and nursing homes, garment worn by hotel and restaurant and kitchen staff, as well as non-textile PPE like helmets, shoes, etc.).
[357] These textile rental services are organised within the European Textile Services Association (ETSA), see www.etsa-europe.org/homefs.htm and www.etsa-europe.org/Etsa-Europe.org/members/pdf/ETSAMemberslist.pdf.
[358] Further information at http://www.etsa-europe.org/Etsa-Europe.org/members/pdf/ETSAMemberslist.pdf.

use workwear/PPE consider full outsourcing (including rental services) instead of investing in new workwear.

9.3.7 Linkages to final (end-user) markets

Often the end-users have (via their public procurement process) direct contact with the garment companies and there hardly seem to be any wholesale/distribution market in between. Further, the (rental) service companies also play a role in distribution, as they take care of the whole process from buying, leasing, cleaning, but also replacement.

9.3.8 Overall assessment of the supply chain

As mentioned before the supply chain for protective clothing for first responders is characterised by the presence of a number of large global players in the upstream market, mainly related to fibres and fabric. The downstream market (garment, but also additional support services) is less concentrated and dominated by SMEs. A large number of the SMEs focus on certain niche markets or only serve local (or regional) clients. High quality fabrics and garment (for fire suits) are still produced in western European countries, despite the cost disadvantages compared to low cost countries, for example in the Far East.

An important trend within the supply chain is the downstream movement of some of the big players (e.g. DuPont) that players seek to have more control of downstream activities, for example at the garment level. Further, there is some level of vertical cooperation within the supply chain. Within the Nomex Quality Programme, DuPont (which reduced its end user marketing considerably, according to an interviewee) has developed (vertical) cooperation with companies like Lion Apparel, Bristol Uniforms and Sioen.[359] Lenzing and TenCate developed together one of their production lines (Defender M). Lion Apparel also cooperates with TenCate.

Within the supply chain, there are certain levels of European specialisation, but these are mainly related to high quality fabrics and garment. The strong attention for comfort and ergonomics may be a typical area of European specialisation.

9.4 Main trends and developments

Several factors have been identified that shape market developments. Often, these factors are in fact a trade-off between the supply and demand sides. Typical supply side factors are the constant attention for further improvement of the material pertaining to the weight, comfort and ergonomics of the protection equipment. Despite certain improvements, the suits (especially for fire-fighters) are still very uncomfortable, especially in certain circumstances (e.g. assistance by accident in sunny weather).

[359] < http://www.dpp-europe.com/-Programme-.html?lang=en >.

9.4.1 Market trends and developments

Differences between Member States

Within the EU, important differences in demand exist between Member States that are associated with factors such as climatic circumstances, as well as the landscape, type of buildings, architecture and density (rural versus urban). Also the risk for forest fires (higher in southern Europe) and the presence of Sevesco sites (risk for chemical hazards) are relevant. Further, there are national differences in the way fire-fighter operate. For example, in Germany only certain fire-fighters will enter the building, while in the Netherlands (nearly) all fire-fighters are trained to do this. In the US, the fire-fighters almost immediately enter the building, while in Europe they rather fight the fire from outside; although procedures differ across countries.

Development of demand

Since the year 2000, the average growth rate of the global market for personal protection textiles has been estimated at approximately 3.5%, and it is expected that for the coming 10-15 years this growth rate will remain.[360] Overall, the PPE market for first responders is a relatively stable market, with limited (demand) growth. This is related to the fact that it is mainly a 'replacement market', which corresponds to a stable number of policemen and fire-fighter and with a limited amount of new end-users.[361]

Increasing attention for well-being first responders

In general, fire-fighters wear their standard turnout gear in all circumstances (fire-fighting, but also in case of traffic accidents); only in special situations will they use chemical and gas suits. There is, however, increasing attention being paid to the well-being of the fire-fighters with regard the range and properties of protective clothing available. For example, one question that is being raised is whether it is possible to wear protective clothing that is designed for the specific situation (e.g. turnout gear in case of fire, lighter equipment in case of a car accident). This however might result in higher expenditures (several suits per fire-fighter) and logistical problems.

Illegal copying of (European) technical solutions

A problem related to technological development and global competition is the (illegal) copying of technical solutions. Interviewees mention the fact that more and more (R&D intensive) technical solutions developed by European companies are quickly reproduced in the Far East. European companies spend a lot of their R&D budgets on research and a few months after the market release, the first (low quality) copies emerge on the market. Thus, the intellectual property rights regime – due to lack of enforcement – is seen as having little relevance for the sector.

[360] European Commission, 'Accelerating the development of the protective textiles market in Europe', COM (2007), 860.

[361] Frost & Sullivan, 'Firefighter PPE- the challenge and importance of winning and keeping contracts', August 2008. However, see also our previous remark that there is however a trend to professionalize the fire-fighting services, which might result in less volunteers and more professionals (with possibly more expensive equipment).

9.4.2 Technology trends and developments

Technology development along the supply chain

As we mentioned before, fibres are one of the main technologies d for protection against heat, flames, gases and chemicals. Most of the main types of fibres have already existed for several decades (e.g. DuPont's Nomex was developed in the 1960's and 1970's as well as AKZO's Twaron and the Lenzing FR-fibre). Fibres techniques are still improving, but mainly in the field of blending fibres. Blending leads to a better combination of performance and protection then the 'traditional' fibres do. At the same time, technical development and innovation are not only the result of improvement in the fire-resistant fibres but also from improvements in spinning, weaving, dyeing and finishing. As said earlier, recent technical innovation had made it possible that the current finishing technologies add 'fiber characteristics' at the fabric level.[362]

A trend which is related to this is the promising use of nanotechnology-based materials. Nanotechnology for protective clothing is still in a preliminary development phase. 'Recently, there is a growing interest in the use of fine fibres such as micro- and nanofibres for specialist applications. The protective clothing made up of these fibres and their composites give high performance, functionality, comfort, and larger life span with less weight, size, maintenance and cost'. Nanostructures and nanocomposites are for example used for lightweight protective clothing, flexible antiballistic textiles, chemical and biological warfare protection and microsensors into a smart suit or smart helmet (body and brain sensing, environmental and situational awareness).[363] Avila observes that also cotton fabrics coated with nanotubes (that are modified with enzymes capable of detecting and detoxifying chemical warfare) market players could offer a new line of comfortable chemical protective clothing for the military and civilian first responders.[364]

Smart or intelligent textiles

This technology has been described in section 9.1.3. Currently, smart textiles are primarily used at garment level and not at fabric level. In the previously mentioned Mateo-project it was said that 'the production of very smart textiles (the third generation) is now a reality after a successful marriage of traditional textiles and clothing technology with other branches of science like material science, structural mechanics, sensor and actuator technology, advance processing technology, communication, artificial intelligence, biology etc.[365] Interviewees indicate that, although they are still in a preliminary development phase, smart solutions are seen as having a (very) high potential for the future. The further development of intelligent solutions for PPE textile may bring the European sector to a next level in PPE in the future, for example within the European Framework Programmes.

[362] Based on information provided by interviewees.
[363] Thilagavathi, G. et al, 'Nanotechnology and protective clothing for defence personnel', Defence Science Journal, volume 58, issue 4, July 2008, p. 451-459.
[364] Avila, A.G., Hinestroza, J.P., 'Smart textiles: Tough cotton', Nature Nanotechnology, volume 3 (2008), p. 458 – 459.
[365] Ibid, see footnote 311.

Box 9.3 EU Framework Programme 7 (FP7)

Within the European Framework Programmes 7 (FP7), 'Nanosciences, Nanotechnologies, Materials and new Production Technologies' (NMP) is one of the themes within the 'industry and industrial technology' cluster. Seven projects related to PPE for first responders are funded with European budgets (all starting second half 2009), like ProfiTex[366] (€ 4 mn, research to support fire-fighters with a system that supplies mission relevant information), iProtec (€ 2.7 mn, development of intelligent PPE system that will ensure active protection and information support) and SafeProTex (€ 3.1 mn, research for development and application of specific functionalizing [protective] materials)[367] Within the FP6, the Proetex-project is carried out. This project is developing 'textile and fibre based integrated smart wearables for emergency disaster intervention personnel'[368].

An example of these intelligent solutions is provided by the Danish company Viking, who have integrated 'Thermal Sensor Technology' in the traditional turnout gear. Thermal sensors monitor the outer temperature near the fire-fighter and on the inside of the coat close to the body. Two LED displays (sleeve and back) indicate critical heat levels to the fire-fighter (and his colleagues). Another example is the German company ALWIT which is developing 'wireless supply of vital data including temperature and location data' in fire-fighters PPE.

Increased attention for comfort and ergonomics

In general terms the main trends underlying the supply of materials (i.e. fibres and fabrics) and garments relate to their broader application and to improvements in terms of comfort and ergonomics. The latter is influenced by EU regulation, but also being driven by demand requirements; for example, one interviewees mentioned that in their procurement process they currently demand that fire suits only cause 10% extra 'burden' (in terms of motion and ergonomics) compared to a ordinary jogging suit. This attention for chronic low-intensity exposure is part of a broader trend which focuses on improvement of effectiveness, safety and health of first responders, according to one of the interviewees.

Some interviewees indicate that the attention for ergonomics and comfort is stronger in Europe than for example in the US. This is probably partly a reflection of differences in cultures but, also, partly due to (EU) regulations.

Increased attention for incorporated technical solutions

Another trend some of the interviewees observed is the incorporation of several types of protection in a single solution (i.e. suit) against several hazards (e.g. fire and heat but also chemicals). The need for combined protection technologies into one system might increase as the threats are becoming more complex and diverse.

[366] See for example, < http://www.wearable.ethz.ch/research/groups/health/ProFiTex/index >.
[367] Interview with Euratex, see also:
http://ec.europa.eu/enterprise/newsroom/cf/document.cfm?action=display&doc_id=4117&userservice_id=1&request.id=0
[368] < http://www.proetex.org/index.htm >.

9.4.3 Production trends and developments

Contrary to other many other textile production segments, for which production largely takes place in the Far East, the production of high-end quality protective textiles (e.g. fire-fighter suits) is still possible in Europe. For example, at the fabric and garment level, there are still companies which employ most of their people in the European Union (e.g. Utexbel and Vandeputte). However, some interviewees indicate that there is a (still weak) trend towards outsourcing of production of high-end quality textiles to low-income countries, also.

With regard to the outsourcing of the production of high-end quality textiles, two of the interviewees expressed their concerns whether the minimum (CE) safety requirements can be guaranteed in the future. This concern was prompted by the lack of quality control in low-income countries and illegal use of the CE marks and insufficient market surveillance within the EU.

9.4.4 Overall assessment of trends and developments

The market for protective/intelligent textiles for first responders is a relatively stable market, due to the fact that the number of end-users is rather stable and the bulk of their demand relates to equipment/garment replacement.

From a technological perspective, the main focus of attention - throughout all levels of the supply chain - is for further improvement of materials in relation to weight, comfort and ergonomics of the protection equipment is the main driver for demand. The demand for protection for several hazards concentrated in one suit is also a driver for demand. However, in most cases there is a (negative) trade-off between protection and comfort. Intelligent textiles (for example by providing vital data) look very promising, but are still a preliminary trend.

9.5 Regulatory conditions and development

9.5.1 International, European and national security-related regulatory conditions

PPE-directive 89/686/EEC

For both PPE and protective textiles, the PPE-directive (89/686/EEC of 21 December 1989) lays down the regulatory framework. This Directive was created in order to create an internal European market for PPE. The significant differences in PPE-provisions were seen as a barrier to trade and harmonisation should ensure free movement of these products[369].

In this Directive some basic requirements are mentioned pertaining to (a large number of) PPE-products, certification procedures, EC type examination, quality control, CE marking, etc. The Directive determines that PPE-products must satisfy basic health and safety requirements which focus on protection, comfort, ergonomics, efficiency and

[369] Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment. As previously mentioned, this Directive is currently being revised in order to bring it in line with the revised New Approach framework (see: http://ec.europa.eu/enterprise/newapproach/index_en.htm).

product information (annex II). Further, the Directive looks at eliminating trade barriers, for example by determining that Member States may not prohibit, restrict or hinder the placing on the market of PPE, which comply with the European provisions.

A factor that influences the development of the PPE and protective textiles market is the public procurement system (laid down in Directive 2004/18/EC as amended). In theory, the public procurement system should facilitate in a 'perfect match' between supply and demand. In practice however, end-users often lack the (technical) knowledge to develop and use an updated bid book, creating inefficiencies between supply and demand.

9.5.2 Industry and market-based standards

Harmonised technical EN- standards

While Directive 89/686/EEC sets out the broad regulatory framework, the European Committee for Standardization (CEN) developed harmonized standards fir some of the risks identified in the PPE-Directive. These harmonised technical standards and specifications for PPE- products were laid down in a number of EN-norms. There are at least 120 EU standards related to PPE-requirements and testing methods.[370] Examples of PPE regulation related to a safe work environment are:

- EN 340: 2003 Protective clothing: general requirements;
- EN 471: 2003 High visibility warning clothing;
- EN 343: 2003 Protective clothing: protection against rain;
- EN 342: 2004 Protective clothing: protection against cold;
- EN (ISO) 11612: 2008 Protective clothing for workers exposed to heat.

These EN-norms have been implemented in national jurisdictions and therefore have a national counterpart.[371] Member States (or for example fire brigades) have the possibility to require additional performance (or a higher level of performance) than indicated in the EN-standard. Higher requirements are in most cases related to their own risk analysis in relation to their safety situation and based on Directive 89/656/EC (PPE use) rather than 89/686/EC (PPE manufacturing)[372]. Interviewees indicated that additional performance requirements are often required, for example in Germany and the UK.

Minimum requirements for fire-fighters

For fire fighters the minimum requirements for their protective clothing are laid down in EN 469. Other relevant standards are EN 1486 (protective clothing for specialised fire fighting), EN 15614 (wild land) and EN 659 (protection gloves for fire fighters). Some of these standards have an ISO-counterpart, like ISO 11613 and ISO 15538.

EN 469 specifies test methods and minimum requirements for clothing to be worn during fire fighting operations and associated activities where there is a risk of heat and/or flame. It covers the general clothing design and the minimum performance levels. The required performance levels may be achieved by the use of one or more garments. It does not cover protection for the head, hands and feet or protection against hazards, e.g.

[370] See for example: http://www.newapproach.org/ProductFamilies/Default.asp
[371] See for example: http://www.cen.eu/esearch/CatWeb.aspx?id=1040005
[372] See also the Commission's PPE Guidelines (p. 3), see: http://ec.europa.eu/enterprise/mechan_equipment/ppe/ppe_guidelines.pdf

chemical, biological, radiation and electrical hazards. These aspects may be dealt with in other standards.[373]

End-users demand that their protective equipments is CE certified. Suppliers of protective clothing are only allowed to use the particular CE trademark when their products are tested and fulfil the requirements of Directive 89/686/EEC.

9.5.3 Overall assessment of regulatory conditions

EN standardisation

Some interviewees mention that the focus of the current EN standardisation norms and the formulation of the product requirements in public procurement is too narrow. Companies with innovative solutions seem to have problems with these strict EN norms, and seem incapable to 'break through' these strict EN-norms. It was also indicated that the standardisation/certification process is very costly for SME's.

Inefficient usage of the public procurement framework

The current usage of the EN norms and the public procurement framework by (especially) the end-users results in some problems and is seen as an important obstacle for further innovation. The people who are involved in the development of the public procurement process and the bid books often lack technical knowledge and are often unaware of new technical and market developments. This creates an information asymmetry between the end-users and suppliers, which hinders the innovation and further technical development (usage of old bid books, wrong product specifications). Especially private (or semi-governmental) buyers use the public procurement mechanisms without good 'terms of references' and proper selection and appeal procedures.

Box 9.4 Findings from interviews

> One of the interviewees stated that sometimes technology is better than the international standards and the demand requirements in the bid books. Often this is also related to the fact that users normally are content to wear a suit that they are accustomed to, even though the protection is limited. Several products are on the market now that have excellent strength before and after exposure to heat and flames, where as traditional products tend to 'fall apart' even though they are considered protective.

Additional national requirements create trade barriers

Member States have the possibility to add extra safety requirements. Several interviewees stated that the existence of these extra safety and test requirements creates trade barriers, results in a fragmented market and hinders the development of the internal market. Within the scope of this study it was not possible for us to determine exactly the heights and effects of these barriers.

[373] EN 469: 2006 Protective clothing for fire fighters.

9.6 The global competitiveness position of the EU industry

Given the lack of 'traditional' trade and competitiveness data, it is very difficult to provide an assessment the EU competitive performance, for example by benchmarking with other countries like the US and Japan. Assessments of productivity performance, international trade performance, investment and FDI performance could not be done.

Key players in EU and global market

The final market for protective textiles for first responders is definitely not a global market, but has a more European or even national dimension. Table 9.15 provides an overview of the main EU and non-EU companies active on the European market for protective textiles for first responders. None of the market players is active throughout the whole chain. The position of European companies differs per level of the supply chain.

Table 9.15 Overview market players active at the European market

Level	EU companies	Non-EU companies	Remarks
Fibres	DSM (cut-proof), Lenzing (heat & fire)	DuPont (US), Teijin Aramid (Jap)	DuPont and Teijin Aramid are the world leaders. DSM is not producing real FR fibres and the position of Lenzing is growing. The Teijin Group bought the company Aramid (with the Twaron fiber) in 2000, which was part of the Dutch chemical company Akzo-Nobel.
Fabric	TenCate, Ibena, Utexbel, Seyntex, Klopman	-	TenCate is active at the US (military) security market with their Defender M production line (US Army). EU companies are active outside the EU (e.g. Russia, Middle-East, North-Afria), but the size of these activities is relatively small.
Garment	Sioen, Seyntex, Bristol Uniforms, Remploy, Cosalt, Arlen, Frontline, Vandeputte	Lion Apparel (US)	EU companies are active outside the EU (e.g. Russia, Middle-East, North-Africa), but the size of these activities seems to be relatively small (compared to European activities).
Support services	Bristol Uniforms, Vandeputte, Rentokill-Initial, Davis Service Group	Lion Apparel (US)	

Assessment of position of EU and non EU companies

Within the supply chain, the fibre level is the only segment in which global competition really exists. DuPont (US) and Teijin Aramid (Japan, the fibre was invented by the Dutch Akzo Nobel) are the global leaders, complemented by DSM and Lenzing (both EU). However, most of them (except Lenzing) are global chemical companies with a broad range of products and technologies.

The fabric and garment market are substantially less concentrated and 'global' competition limited. In the (high-end) European fabric and garment market the position of European companies is strong. Lion Apparel is the only large non EU company which is active in the European market. Asian companies are not present at all, despite the competitive disadvantage of Europe compared to these low-income countries.

The limited presence of non EU companies is likely to be caused by market entry barriers, like the lack of harmonisation of standards (these are some ISO standards, but these do not cover the whole segment), the very scattered presence of end-users and differences in the regulatory regimes between Member States (like additional national safety requirements). At the same time, this is also a problem for European companies. It seems difficult for both EU and non-EU companies to expand their activities throughout Europe We observe in this respect a dominance of SMEs, particularly in the garment market. Most of the European companies at fabric and garment level only have a good market position in their home country and some neighbouring countries. There are hardly any companies which are active outside their home market (and some neighbouring countries) and gain a stronger position on the European market.

At the same time, European fabric and garment companies hardly gain a significant market position outside Europe. There are European companies who are active in Russia, the Middle East and Africa, but the size of these activities seems to be relatively small. Probably, the reason for this are entry barriers, like the lack of harmonisation of standards between the EU and US[374]. Companies have to make large investments to fulfil the US safety requirements, which differ from the EU standards. TenCate seems to be an exception. They managed as a European fabric company to gain a position on the US market (in this case: protective fabric for military equipment) and are also active in many non-EU countries, including the Middle-East and Africa. In order to gain access to the US they purchased Southern Mills, the largest US supplier of inherently fire-resistant fabrics.

Innovation

In general, the feeling of our interviewees is that European companies (also at fabric and garment) level are innovative. TenCate was mentioned several times as a successful entrant to the US (military) security market, with innovative products.

Other industry interviewees indicate that they see the US SME's as more innovative, especially in defence-related products. This is related to the entrepreneurial US culture, the scattered European market versus one US market and the existence of huge R&D budgets (US Defence Ministry). This perception is debatable, as one of the interviewees indicated that the R&D for the US Homeland Security market is as fragmented as the EU. The funding in textile research in by the EC and EU Member States is manifold bigger then in the US. The US has hardly any policy towards fibre and textile research, while also company R&D in fibres has dropped drastically, according to this interviewee.

The position of the European high-end quality companies might be threatened in the future by illegal copying of European inventions by companies in the Far East. Currently it is mainly a problem in low-end products.

[374] One interviewee indicated that although US delegates are working on ISO standardisation committees, the US has not introduced these standards but instead keeps using their NFPA (or ASTM) standards.

Macroeconomic conditions and R&D

Due to the current macroeconomic conditions, the risk exists that companies reduce their R&D budgets. This may relate to the companies at fibre level, but especially to the fabric and garment companies. Often protective clothing for first responders is only one of their fields of activity. When companies, due to poor economic macro conditions, limit their PPE spending, it results in lower turnover and in probably lower R&D budgets.

Within the scope of this study, it is not possible to determine how this influences the market for protective/intelligent textiles for first responders. In general, this market is seen as a stable market. The protection of fire fighters and policemen is constantly important and not directly dependent from macroeconomic conditions.

9.7 Conclusions and potential policy issues

Our assessment of the segment raised a number of policy issues which might be worth to be addressed in the (near) future.

Public procurement process and end-users behaviour

The current public procurement process in combination with the behaviour of the end-users is one of the main problems raised by the interviewees. This practice around public procurement is currently seen as an important obstacle for further innovation. Issues are for example:

- **Formulation of the product requirements in public procurement, and especially the EN-norms**. Currently, companies with innovative solutions seem to encounter problems with the strict EN-norms, and do not seem capable to 'break through' these.
- **Public procurement should focus more on innovation and quality**. Public procurement is seen as a break on innovation, but the behaviour of the end-users (governments, fire and police departments) as the main problem. The bid books that are used are very rigid and often based on the bid book used in the previous procurement process (sometimes the bid books are even written by the current supplier). Further there is often a (too) strong focus on the price component in the decision process (often main criteria) and offers for alternative solutions are often impossible or not considered seriously.
- **Lack of technical knowledge.** Following from the previous point, people who are involved in the development of the bid books are often unaware of new technical and market developments. Also mentioned, was the fact that local (fire) stations often do not have enough technical knowledge compared to (representatives of) companies who sell them equipment. This information asymmetry may result in safety risks for the first responders.

Possible suggested solutions include:

- **Greater focus on 'functional requirements'** (does it work?) instead of 'technical requirements' (at fibre/yarn-level). With a stronger focus on 'functionality' there will be more room for innovation, while the safety standards can remain high.
- **Centralisation of preparatory public procurement procedures**. The people who are dealing with public procurement on local (or regional) level should receive more guidance in the technical part of the PP procedure. Technical research and testing

can, for example, be undertaken at national level, while local and regional fire and police departments can use these results.

- **Increase expertise of public purchasers**. Following from the previous point, the expertise of public purchasers could be increased, for example by creation of national (or European) network or platform for protective clothing procurement for exchange of information and best practices.
- **Bundling of demand for 'solutions'.** Either the Government or a group of end-users could ask for a 'solution' for a certain problem, instead of determining ex-ante the suitable product for their problem. Suppliers will (likely) come up with state of the art solutions. It might also occur that more room for research is available and that a final new product may be developed in joined cooperation (like in Firebuy: joint development of new suit).

It should be noted that these suggested solutions might have a different impact on SMEs than on large firms. Whether this is a desired direction is outside the scope of this study.

Reducing market fragmentation

The existence of extra safety and test requirements (often on national level) is seen by the interviewees as an entry barrier in public procurement and hinders the further development of an internal market. Further standardisation of safety requirements may be helpful here. However, further standardisation might also influence the (innovative) position of SMEs in a negative way. Currently it is already very costly for SMEs to access the standardisation/certification process.

Given the fact that the end-users are very fragmented and hardly have any purchasing power, the bundling of demand at (regional or) national level might have a positive effect at levels of innovation and safety. An example of demand bundling is 'Firebuy' in the UK. However, one of the effects of demand bundling might be that SMEs would be excluded and would have to leave the market. Currently, these SMEs have strong ties with several local fire and police departments. When demand will be bundled into one (or several) national public procurement process(es), it is likely that SMEs would not have the possibility to tender (financial and personal capacity, too high risks). After the tender procedure, the (national) market is locked for five to six years. [375]

IPR and enforcement

The illegal copying of (European) security solutions by companies in the Far East is seen by interviewees as a problem. Violation of the intellectual property rights (IPR) and free riding on investments made by others will increase the (entrepreneurial) market uncertainty and reduce the willingness to invest in innovation and R&D.

Related to this is the inadequate enforcement of correct product quality (conform CE-standards), which might increase safety risks. CE-labelled products do not always fulfil the CE-norms (e.g. very cheap high-visibility vest which can be bought in petrol stations) and influence the market position of companies who strictly follow the requirements. Correct enforcement is very costly and seems to have low priority.

[375] During consultation, industry representative organisations expressed a rather negative opinion about the effects of the Firebuy case.

Workers safety

Industry interviewees point out that from a policy perspective there is not enough attention for personal protective equipment. DG Employment, Social Affairs and Equal opportunities focuses on prevention of hazards and collective protection, but 'forgets' the role PPE can play in the protection of employees. Especially for first responders, PPE is a crucial element for their protection. According to the safety regulations, a higher number of workers should wear PPE. However, PPE is often perceived as uncomfortable or as a hindrance. Further innovation of PPE may improve that situation, as well as more attention for enforcement and information provision.

ANNEX I: Glossary and list of acronyms

Acronym or Word / Concept		Description
3G	**Third Generation**	3G correspond to 3rd generation commercial cellular networks differentiating themselves through high data rates allowing seamless data communication on top of voice and additional services (video conferencing, etc.).
ACI-Europe	**Airport Council International - Europe**	
ADC	**Analogue to Digital Converter**	Semiconductor electronic components, performing the conversion of analogue signals into digital formats (4, 8, 16 bits, etc).
AEA	**Association of European Airlines**	
AFIS	**Automated Fingerprint Identification System**	A system originally developed for use by law enforcement agencies, which compares a single fingerprint with a database of fingerprint images. Subsequent developments have seen its use in commercial applications, where a client or customer has their finger image compared with existing personal data by placing a finger on a scanner, or by the scanning of inked paper impressions.
AIS	**Automatic Identification Systems**	
APCO P25	**APCO Project 25**	Refers to a suite of digital radio communication standards for use by federal, state/province and local public safety agencies in North America. Direct competitor to the European TETRA standard.
ASSA-I	**Aviation Security Services Association - International**	
AT x-ray	**Advanced x-ray technologies**	
ATSA	**Aviation and Transportation Security Act**	US law signed in November 2001 establishing measures to protect air transportation and securing the air travel system. One of the pillars of the new legislation was the establishment of the Transportation Security Administration (TSA), within the Department of Transportation.
Authentication		The process of establishing the validity of the user attempting to gain access to a system. Primary authentication methods are: 1) Access passwords (something the user knows); 2) Access tokens (something the user owns); 3) Biometrics; 4) Geography (a workstation, for example).
Base station		Equipment of a mobile communication network acting as a relay between the central communication network (wired) and the neighbouring cellular terminals.
CBP	**Customs and Border Protection (US)**	
CBRNE	**Chemical, Biological, Radiological, Nuclear or Explosive**	
CCSF	**Certified Cargo Screening Facilities**	Facility that directly tenders cargo to a freight forwarder or air carrier.
CCSP	**Certified Cargo Screening Program**	Procedure to receive the validation as a Certified Cargo Screening Facility.
CCTV	**Closed-Circuit Television**	

Acronym or Word / Concept		Description
CDMA	**Code Division Multiple Access**	2nd generation US cellular communication standard competitor of the European GSM standard.
CEN	**European Committee for Standardisation**	
CENELEC	**European Committee for Electrotechnical Standardisation**	
CLECAT	**European Association for forwarding, transport, logistics and customs services**	
Contact / Contactless		In regard to chip cards: whether the card is read by direct contact with a reader or has a transmitter/receiver system which allows it to be read using radio frequency technology (up to a certain distance).
CSI	**Container Security Initiative (US)**	
CT	**Computed Tomography**	Computed tomography is an imaging method employing tomography. Digital geometry processing is used to generate a three-dimensional image of the inside of an object from a large series of two-dimensional X-ray images taken around a single axis of rotation.
DHS	**Department of Homeland Security (US)**	
DSP	**Digital Signal Processors**	Semiconductor electronic components, which are programmed by the user to perform intensive data processing. Mostly used in telecommunication industry and real time applications.
EC	**European Communities**	
ECAC	**European Civil Aviation Conference**	
EDACS	**Enhanced Digital Access Communication System**	Digital radio communication protocol invented by General Electric Corp. in the mid 1980s. This system has been used in public safety and public transport applications, mostly in the USA.
EDS / EDDS	**Explosive Detection Systems/ Explosive Device Detection System**	
EMS	**Electronic Manufacturing Services**	Sub-contractors of the electronics industry which are specialised in mounting components on electronic boards in order to build dedicated functional devices or sub-systems.
Encryption		Capability of a secure communication system to secure the transmitted information through an algorithm so that unauthorized users cannot access to the information. Data encryption is done by the use of an algorithm and a key. The key is used by the algorithm to scramble and unscramble the data.
Enrolment		The initial process of collecting biometric data from a user and then storing it in a template for later comparison.
ESRIF	**European Security Research and Innovation Forum**	An independent advisory body on security research set up in 2007.
ETD	**Explosive Trace Detector (or detection)**	Explosives trace detectors (ETD) are security equipment able to detect explosives of small magnitude. The detection can be done by sniffing vapours as in an Explosive Vapour Detector or by sampling traces of particulates or by utilising both methods depending on the scenario.
ETSI	**European Telecommunications Standards Institute**	
EU	**European Union**	
FDI	**Foreign Direct Investment**	
Feature extraction		The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template.

Acronym or Word / Concept		Description
First responders		A generic term referring to the first medically trained responder to arrive on scene (police, fire, EMS).
FP6 / FP7	**Framework Programme 6 / 7**	
FPGA	**Field Programmable Gate Arrays**	Semiconductor electronic component, which are programmed by the user in order to perform different types of functions including filtering, processing etc.
FR fibre	**Fire resistant fibre**	
FSR	**Freight Security Requirements**	Conditions to ensure the safe and secure in-transit storage and warehousing of assets through the world.
GC-MS	**Gas chromatography-mass spectrometry**	A method that combines the features of gas-liquid chromatography and mass spectrometry to identify different substances within a test sample. Applications of GC-MS include drug detection, fire investigation, environmental analysis, explosives investigation, and identification of unknown samples. GC/MS can also be used in airport security to detect substances in luggage or on human beings.
GE	**General Electric**	
GPS	**Global Positioning System**	
GSD	**Hand-held gamma detector**	
GSM	**Global System for Mobile Communication**	The European based cellular communication standard originated in the 1990s and having today the largest deployment worldwide in terms of both covered countries as well as number of users.
HPLC	**High performance (or pressure) liquid chromatography**	A form of column chromatography used frequently in biochemistry and analytical chemistry to separate, identify, and quantify compounds. Retention time varies depending on the interactions between the stationary phase, molecules being analyzed, and solvent(s) used.
IAC	**Indirect Air Carrier**	
IATA	**International Air Transport Association**	
ICAO	**International Civil Aviation Organisation**	
ICE	**Immigration Customs Enforcement (US)**	
iDEN	**Integrated Digital Enhanced Network**	Digital radio communication protocol developed by Motorola, covering in particular all major airports in the USA.
Identification		The process by which the biometric system identifies a person by performing a one-to-many (1:n) search against the entire enrolled population.
IMO	**International Maritime Organisation**	
IMS	**Ion mobility spectrometry**	A spectrometry technique capable of detecting and identifying very low concentrations of chemicals based upon the differential migration of gas phase ions through a homogeneous electric field.
IPR	**Intellectual Property Rights**	
IPS	**International Port Security Program**	
ISO	**International Organisation for Standardisation**	
ISPS	**International Ship and Port Facility Security code**	
KGB	**USSR National Security Agency**	
Known consignor		The originator of property for transportation by air for his own account and who has established business with a regulated agent or air carrier.
LMI	**Lead Market Initiative**	
LRIT	**Long-range identification and tracking systems**	

Acronym or Word / Concept		Description
LTE	**Long Term Evolution**	Correspond to the next generation of commercial cellular networks, further increasing data rates.
Minutiae Points		Local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.
NII	**Non Intrusive Inspection equipment**	
NOA	**Port of impending entry**	
NSD	**Neutron search detector**	
ODM	**Original Design Manufacturers**	ODMs are manufacturers integrating design services on top of production activities.
OEM	**Original Equipment Manufacturers**	OEMs are the major electronic brands and can either sub-contract their production and design or keep it internally depending on their strategy and market positioning.
One-stop security		Concept of screening people for prohibited items once, at the beginning of their journey only.
PCR	**Polymerase Chain Reaction**	A technique to amplify a single or few copies of a piece of DNA across several orders of magnitude, generating millions or more copies of a particular DNA sequence.
PPB	**Parts per billion**	
PPE	**Personal Protective Equipment**	
PPM	**Parts per million**	
PRD	**Personal radiation detector**	Radiation detector approximately the size of a telecommunications pager, which can be worn by front line officers or security personnel. PRDs can provide a flashing light, tone, vibration or numerical display that corresponds to the level of radiation present.
R&D	**Research and Development**	
RASCO	**Remote Air Sampling for Canine Olfaction**	Detection system containing a polythene probe some eighteen inches in length, which is inserted under the curtain side or through the rubber seals of a container door, and by means of a vacuum, air is extracted from the container onto a sample tube or filter. That sample tube is then taken to a discrete analysis area where it is placed on a stand among other sample tubes. A suitably trained dog then examines the tubes and if the target material is present, the dog will indicate passively.
Regulated agent		An agent, freight forwarder or other entity that conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo.
Repeaters		Equipment in charge of amplifying a communication signal in order to extend its coverage.
RFID	**Radio Frequency identification equipment**	
RID	**Radionuclide identification device**	
RN	**Radioactive and Nuclear materials**	
RPM	**Radiation Portal Monitor**	Pass-through type monitors typically consisting of two pillars containing gamma radiation detectors and usually neutron detectors, and monitored from a display panel. Portal monitors are used for personnel, vehicles, packages and other cargo in a variety of venues.
SAW	**Surface acoustic wave**	An acoustic wave traveling along the surface of a material exhibiting elasticity, with an amplitude that typically decays exponentially with depth into the substrate.
SCBA	**Self Contained Breathing Apparatus**	The breathing system worn by fire-fighters to supply them with breathable air when fighting fires, during rescue operations and in any atmosphere that is oxygen deficient in the course of their work.
SMEs	**Small and medium-sized enterprises**	

Acronym or Word / Concept		Description
SOLAS	**International Convention for the Safety of Life at Sea**	
SSAS	**Ship Security Alert Systems**	
Switches / routers		Equipment in charge of addressing the communication signal to the ad-hoc receiver.
TAPA	**Technology Asset Protection Association**	Association of security professionals and related business partners from high technology and high value companies who have organised for the purpose of addressing the emerging security threats that are common to the high value industry supply chain.
Template		A mathematical representation of biometric data. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.
Threshold		A predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match.
TETRA	**Terrestrial Trunked Radio**	Formerly known as Trans European Trunked Radio, TETRA is a specialist PMR specifically designed for use by government agencies, emergency services, rail transportation staff and military. The standard was published by ETSI in 1995.
TETRAPOL		French digital communication protocol developed by Matra Communication (today part of EADS Group) to serve similar market segments to P25 and TETRA. TETRAPOL is essentially deployed in France (police forces, public safety, fire fighters, Paris transportation network, etc).
TIP	**Threat Image Projection**	Software to monitor (and train) screeners aimed specifically at enhancing the performance of screeners, and to assist in ensuring they are to effectively interpret the screening images and information provided.
TSA	**Transportation Security Administration (US)**	
UK	**United Kingdom**	
ULD	**Unit Load Devices**	Type of containerized cargo generally with the following dimensions: 4ft by 4ft by 8 ft
US/USA	**United States of America**	
USCG	**US Coast Guard**	
Verification		The process of establishing the validity of a claimed identity by comparing a verification template to an enrolment template. Verification requires that an identity be claimed, after which the individual's enrolment template is located and compared with the verification template. Verification answers the question, "Am I who I claim to be?" Verification systems may perform 1:1 matches, 1:few matches (very small database of enrolees) and 1:N matches (more than 500 records).
VHF	**Very high frequency radio**	
WCO	**World Customs Organization**	
WiMax	**Worldwide Interoperability for Microwave Access**	Wireless communication standard families, providing enough data rates to provide wireless broadband internet access. Some standard development are aiming at providing mobile WiMax functionalities to compete with traditional 3G and even 4G cellular networks.
WMD	**Weapons of Mass Destruction**	
WTO	**World Trade Organisation**	
WW	**World War**	

ANNEX II: List of interviewees

Name	Company / Organisation	Position
Albert Veenstra	Erasmus University	Professors on Maritime Economics
Alexandra Guerin-François	Commission National Informatique et Liberté (CNIL)	Lawyer (CNIL Legal Department)
Alvise Grammatica	EUROPOL	Information, Management & Technology Coordination Unit
	ESRIF member	
Benoit Papillault	Luceor	CTO
Bernard Didier	Sagem Sécurité	Senior Vice-President
		Director R&T Business Development
Cédric Demeure	Thales	Expert on Software Defined Radio
Christian Weiss	Sagem Sécurité	Airport Program Manager
Cinzia Missiroli	European Committee for Standardisation (CEN)	Programme Manager, Standards Development – Industry & Technology
Dana Aussems	Europe Container Terminals (ECT)	Security Manager
Eckard Seebohm	European Commission (DG TREN)	Head of Unit, Aviation Security
Emiel den Hartog	TNO	Senior Scientist Physical Protection, Biological and Chemical Protection
Emmanuelle Villot	PPSL	Program Manager
Erik Berglund	FRONTEX	Director of Capacity Building
	ESRIF member	
Evert Wijdeveld	Deltalinqs (Rotterdam Port and Industries Association)	Environmental and Safety Affairs
François Murgadella	French Defence Procurement Agency and National Research Agency	Security Program Manager
François Neumann	THALES	Technical Strategy Director
F. Westervoorde	Rotterdam-Rijnmond Safety Region	
Gert Runde	AeroSpace and Defence Industries Association (ASD)	Director Security and Defence
Gerwin Zomer	TNO	Senior consultant, Mobility and Logistics
Hansjuerg Mahler	EURALARM	President
	Siemens Building Technologies	
Henk Vanhoutte	European Safety Federation (ESF)	Secretary General
Hilde de Clerk	Confederation of European Security Services (COESS)	Secretary General
	Aviation Security Services Association - International (ASSA-I)	Secretary General
Hugo Rosemont	SBAC	Policy Adviser, Security and Resilience
Jan Dietz	TNO	Expert on Secure Communications

Name	Company / Organisation	Position
Jean-Marc Suchier	Sagem Sécurité	VP, Director European Programs
John Ketchell	European Committee for Standardisation (CEN)	Director, Innovation and Business Development
Jos van Kampen	EURALARM	Chairman of Executive Committee Security Section
	ASB Security BV	Director
Karim Jawad	IBM	Sales Leader, SW Europe Sensor Solutions
Laurent Baratier	MARTEC	Public Market Manager
Leen Van Sand	Confederation of European Security Services (COESS)	Communication Officer
Luigi Rebuffi	European Organisation for Security (EOS)	Chief Executive Officer
	AeroSpace and Defence Industries Association (ASD)	Deputy Director for Security
Lutz Walter	EURATEX	Head of R&D, Innovation and Projects Department
Magnus Ovilius	Smiths Detection	Vice-President, Government Relations
Marco Sorgetti	CLECAT (European Association for Forwarding, Transport, Logistic and Customs Services)	Director-General
Marco Taccani Gilardoni	Gilardoni	Managing Director
Marie-Caroline Laurent	Association of European Airlines (AEA)	Manager Security and Cargo
Michiel Scheffer	Noeton BV	Expert on textile industry
Mike Allen	Royal TenCate	Market Manager – Emergency response
M.J. van de Laar	International Association of Ports and Harbours (IAHP)	Managing Director Europe
Nathalie Herbelles	International Air Transport Association (IATA)	Manager Security and Facilitation
Nick Fox	3DX-RAY	CTO
Niels Beuck	CLECAT (European Association for Forwarding, Transport, Logistic and Customs Services)	Policy adviser in charge of security
Philippe Devos	EADS	Operation Marketing Manager
Réne Besselink	Secure Logistics	Director
Robert Long	European Textile Service Association (ETSA)	Secretary General
Robert Missen	European Commission (DG TREN)	Deputy Head of Unit, Aviation Security
Roxanne Vande Zande	Aviation Security Services International (ASSA-I)	Legal Advisor
Stephane Eloy	EADS	Strategic Marketing Manager
Tim Rayner	Rapiscan Systems	Director of Advanced Technology
Vlad Olteanu	Airport Council International - Europe	Policy Manager for Secuirty
Yvan De Mesmaeker	European Corporate Security Association (ECSA)	Secretary General

ANNEX III: List of references

ACI Europe, 'Airport Traffic Report - May 2009'.

AEA Cargo Policy Statements: 'Securing cargo while facilitating trade'.

“Airport Security: Are advanced technology deployments enough to grow the market?”. Presentation by David Fishering (Frost & Sullivan), 28 August 2008. Available at: http://www.slideshare.net/FrostandSullivan/frost-sullivan-airport-security-analyst-briefing-presentation

Alain Breuer, Chair AEA Cargo Security Working Group, “The future EU and U.S. air cargo security requirements: What are the challenges for the industry?”, Presentation at ECBS09 17-18 February 2009, Prague Aviation Master Class. Available at: http://files.aea.be/Speeches/ECBS09_18-02-09.pdf

Avila, A.G., Hinestroza, J.P., ‘Smart textiles: Tough cotton’, Nature Nanotechnology, volume 3 (2008), p. 458 – 459.

Business Monitor International, ‘Israel Defence & Security Report Q3 2009’, p. 39.

Calvin Biesecker. “Rapiscan To Market Brijot’s Stand-Off Millimeter Wave Body Scanner”, Defense Daily, October 31, 2007.

Carafano, J.J., ‘Fighting terrorism, addressing liability: a global proposal’, in: Backgrounder, no. 2138, May 2008.

Carluer, Frederic (2008). 'Global Logistic Chain Security, Economic Impacts of the US 100% Container Scanning Law'. Paris, France: Editions EMS.

Chopra, Sunil and Meindl, Peter (2007). 'Supply Chain Management, Strategy Planning & Operation'. New Jersey: Pearson Prentice Hall.

Christian Serra (Thales Land & Joint Systems), 'State of the Art on Software Radio Frameworks', ENSTA Conference, Paris, November 23 2005.

Civitas, ‘The Homeland Security Market- essential dynamics and trends’, November 2006.

Commission Communication COM (2004) 590 of 9.9.2004, *Security Research: The Next Steps*.

Commission Communication COM (2004) 72 of 3.2.2004, *Towards a programme to advance European security through Research and Technology*.

Commission Communication COM (2005) 429 Final of 22.09.2005, *Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security*.

Commission Communication COM (2005) 488 of 12.10.2005, *More Research and Innovation – Investing for growth and employment: A Common Approach*.

Commission Communication COM (2006) 502 Final of 13.9.2006, *Putting knowledge into practice: A broad-based innovation strategy for the EU*.

Commission Communication COM (2007) 496 final of 7.9.2007 final, *e-skills for the 21st century: Fostering competitiveness, growth and jobs*.

Commission Communication COM (2007) 799 Final of 14.12.07, *Pre-commercial Procurement: Driving Innovation to ensure sustainable high quality public services in Europe*.

Commission Communication COM (2007) 860 of 21.12.2007, *Accelerating the development of the protective textiles market in Europe*.

Commission Communication COM (2007) 860 of 21.12.2007, *A lead market initiative for Europe*.

Commission Communication COM (2007) 374 of 4.7.2007, *Mid-term review of industrial policy*.

Commission Communication COM (2007) 700 final of 13.11.2007, *Reaping the full benefits of the digital dividend in Europe: A common approach to the use of the spectrum released by the digital switchover*.

Commission Communication COM (2008) 133 final of 11.3.2008, *Towards and increased contribution from standardisation to innovation in Europe*.

Commission Communication SEC (2007) 1668 of 14.12.2007, *Pre-commercial procurement*.

Congressional Budget Office. H.R. 1 - Implementing the 9/11 Commission Recommendations Act of 2007, February 2, 2007.

Congressional Research Centre "Air Cargo Security" Updated July 30, 2007. Available at: http://www.fas.org/sgp/crs/homesec/RL32022.pdf

Congressional Research Centre "Aviation Security: Background and Policy Options for Screening and Securing Air Cargo" February 25, 2008 (available at http://www.fas.org/sgp/crs/homesec/RL34390.pdf).

Congressional Research Centre "Aviation Security: Background and Policy Options for Screening and Securing Air Cargo" Updated February 25, 2008; page 35. Available at: http://fas.org/sgp/crs/homesec/RL34390.pdf.

Council Decision 2006/971/EC of 19 December 2006 concerning the Specific Programme Cooperation implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013), Official Journal, L 400, 30 December 2006, p. 86.

Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment.

Department of Homeland Security (2007). Strategy to Enhance International Supply Chain Security. Obtained on July 30, 2008 from http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf.

Eberhardt, J., Liu, Y., Rainey, S., Roach, G., Stevens, R., Sowerby, B. and Tickner, J. (2006) "Air cargo sceening using a fast neutron and gamma-ray radiography scanner", paper presented at the 15th Pacific Basin Nuclear Conference. Available at: http://www.pacificnuclear.org/pnc/2006-Proceedings/pdf/0610015final00111.pdf.

"European Aviation Security Market Overview" Presentation by Marc Pissens, President of ASSA-I (Aviation Security Services Association – International) in May 2007 available at: http://www.easa-security.org/news.htm

EOS, *Priorities for a future European Security Framework*, August 2009.

ESRAB (2006) Report, *Meeting the Challenge: the European Security Research Agenda*.

ESRIF Intermediate Report (September 2008*), European Security Research and Innovation in support of European Security Policies*.

ESRIF Intermediate Report, September 2008. Available at: http://www.esrif.eu/documents/intermediate_report.pdf.

ESRIF Working Group 9 – Innovation Report (draft version of June 2009 provided by TNO).

ETSA, 'Textile Rental Market Survey 2007', published in June 2008.

European Biometrics Portal: Biometrics in Europe 2007, Trend Report (Unisys).

European Commission, Report of the Taskforce on Protective Textiles: 'Accelerating the development of the protective textiles market in Europe', composed in preparation with COM (2007) 860 on 'A Lead Market Initiative for Europe'.

European Defence Agency document at: http://www.eda.europa.eu/WebUtils/downloadfile.aspx?fileid=43.

European Parliament ITRE Committee Report, 'Toia Report' on the Digital Dividend in Europe (July 2008), found at: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0305+0+DOC+PDF+V0//EN

European Parliament resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection (non-binding resolution adopted on 23.10.08).

European Security Strategy – presented by Javier Solana, EU High Representative for CFSP, adopted by the Heads of State and Government at the European Council on 12 December 2003.

European Security Strategy: A secure Europe in a better world (December 2003).

Frost & Sullivan, 'Fire fighter PPE - the challenge and importance of winning and keeping contracts', August 2008.

Frost & Sullivan, 'Personal Protective Equipment in Western Europe provides Growth opportunities for technical textiles', press release June 2005.

Frost&Sullivan "The European Airport Security Equipment Market: A Growth Story in the Making" published in June 2007.

GAO (2009), MARITIME SAFETY: Vessel tracking systems provide key information, but the need for duplicate data should be reviewed, GAO-09-337 March 17, Report to the Committee on US Homeland Security, House of Representatives.

Gordon, N., 'The political economy of Israel's Homeland Security/Surveillance Industry', Working paper III, April 2009.

Homeland Security Research Corporation (HSRC), 'Global Homeland Security, Homeland Defense & Intelligence Markets Outlook 2009-2018'. Published in 2008.

HWWI and Berenberg Bank, *Sicherheits-Industrie (Strategie 2030)*, Juli 2008.

Implementing Recommendations of the 9/11 Commission Act of 2007.

IMS Research, 'The World Market for Explosives, Weapons & Contraband Detection Equipment', 2007 Edition.

IPR Enforcement – Expert Group Report: Making IPR work for SMEs: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/ipr_conference_27_04_2009/report_making_ipr_work_for_sme.pdf

Irish Aviation Authority and Avia Solutions (2004) "Civil Aviation Security financing Study" Background Report, Chapters 1 and 2, prepared for DG Transport. Available at: http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_1.pdf and http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_2.pdf.

K. Harald Drager (President of the International Emergency Management Society), *Developing A Common Voice For Public Safety Across the European Union*, Networked Public Safety London, 22, 23 January 2008.

Koncept Analystics, 'PPE market: an analysis', April 2009.

Le marché des réseaux radio-électriques, February 2006. Survey conducted for the French National Telecommunication Authority ARCEP.

Mäkinen, 'Protective clothing- nowadays and vision', article for the 3rd European Conference on Protective Clothing (ECPC) and NOKOBETEF 8, may 2006.

National Board of Trade Sweden (2008) "Supply chain security initiatives: a trade facilitation perspective", Kommerskollegium 2008:1. Available at: http://www.kommers.se/upload/Analysarkiv/In%20English/Trade%20facilitation/Report%20Supply%20Chain%20Security%20Initiatives.pdf.

NTSC Subcommittee on Biometrics and Identity Management reports: www.biometrics.gov/ReferenceRoom/Introduction.aspx.

"Opportunities to create value" presentation made at Smith's Detection Investor Day, 27 January 2009, available at: http://www.smiths-group.com/presentations.aspx

Papaioannou, K.; Reno, K; and Wyman, K. (2006?), *Market overview of safety and security*.

Raheel, 'Protective Clothing Systems and Materials', New York, 1993.

Raheel, Perenich, Kim, 'Heat- and fire-resistant fibers for protective clothing', in: Raheel, Protective Clothing Systems and Materials, p. 197 and further.

RASCargO – Fast, Cost Effective Screening for Air-Cargo", Homeland Security Europe, available at: http://www.homelandsecurityeu.com/pastissue/article.asp?art=268388&issue=176
Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security.

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Regulation (EC) No 831/2006 of 2 June 2006 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security.

Report of the 11th International Liability Forum; available at http://www.munichre.com/publications/302-05501_en.pdf.

Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research (2004).

"Review of developments in testing, implementation and operational deployment of advanced security screening technologies". Information submitted by the United States to 28th APEC Transportation Working Group Meeting, Vancouver, Canada, 5-8 September 2006. Available at: http://www.apec-tptwg.org.cn/new/Archives/tpt-wg28/Aviation/2006_TPT-WG-28_AEG-SEC_013.doc

STACCATO (2007), Preparatory Action on the enhancement of the European industrial potential in the field of Security Research – STACCATO Final Taxonomy.

Statement for Record, Mr. James Tuttle, Division Head, Explosives Division, Science and Technology Directorate U.S. Department of Homeland Security. Before the House Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection. July 15, 2008.

Statement of James C. May, President and CEO, Air Transport Association of America, Inc. before the Subcommittee on Transportation Security and Infrastructure Protection of the House Committee on Homeland Security, March 18, 2009. Available at: http://www.airlines.org/government/testimony/2009/ATA+Testifies+on+Air+Cargo+Screening.htm.

Stephen Phipsen – President, Smiths Detection. Source: Smiths Detection Investor Day (January 2009) transcript, available at: http://www.smiths-group.com/presentations.aspx.

(US) Support Anti-terrorism by Fostering Effective Technologies Act (2002).

Textiles Intelligence, Editorial: *Europe's Research Roadmap for new PPE*, May 2009.

The US Security Industry Association, 'US Security market report and economic impacts study 2008', January 2009.

Thilagavathi, G. et al, 'Nanotechnology and protective clothing for defence personnel', Defence Science Journal, volume 58, issue 4, July 2008, p. 451-459.

Transport Security Administration "Planning Guidelines and Design Standards for Checked Baggage Inspection Systems" January 30, 2009.

U.S. General Accounting Office "Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach". GAO-03-22, January 2003.

United States Department of Homeland Security, Transport Security Administration, statement of Edward Kelly, General Manager, Air Cargo before the Subcommittee on Transportation Security and Infrastructure Protect Committee on Homeland Security, United States House of Representatives (March 18, 2009), available at: http://www.tsa.gov/press/speeches/031809_kelly_air_cargo.shtm.

US Commerical Service (various country fiches).

VDI/VDE, Der Markt für Sicherheitstechnologien in Deutschland und Europa - Wachstumsperspektiven und Marktchancen für deutsche Unternehmen.

White Paper on defence and national security of the French government, 2008 (English abridged version).

William Reed (2007) "X-ray cargo screening systems: the technology behind image quality", Port Technology International, September 2007.

William Reed (2007), "Energy driven", Cargo Security International, June / July 2007.