

Study on Civil Security R&D in major third countries (SER3CO)

Final Report, within the Framework Contract of Security Studies – ENTR/09/050

Client: European Commission DG Enterprise and Industry

Rotterdam, October 2013



Study on Civil Security R&D in major third countries (SER3CO)

Final Report, within the Framework Contract of Security Studies –
ENTR/09/050

Client: European Commission DG Enterprise and Industry



DECISION
Etudes Conseil

TNO innovation
for life

In collaboration with:

The Hague Centre of Strategic Studies
FOI, Swedish Defence Research Agency
PlanConsult Holding GmbH

Rotterdam, October 2013

About Ecorys

At Ecorys we aim to deliver real benefit to society through the work we do. We offer research, consultancy and project management, specialising in economic, social and spatial development. Focusing on complex market, policy and management issues we provide our clients in the public, private and not-for-profit sectors worldwide with a unique perspective and high-value solutions. Ecorys' remarkable history spans more than 80 years. Our expertise covers economy and competitiveness; regions, cities and real estate; energy and water; transport and mobility; social policy, education, health and governance. We value our independence, integrity and partnerships. Our staff comprises dedicated experts from academia and consultancy, who share best practices both within our company and with our partners internationally.

Ecorys Netherlands has an active CSR policy and is ISO14001 certified (the international standard for environmental management systems). Our sustainability goals translate into our company policy and practical measures for people, planet and profit, such as using a 100% green electricity tariff, purchasing carbon offsets for all our flights, incentivising staff to use public transport and printing on FSC or PEFC certified paper. Our actions have reduced our carbon footprint by an estimated 80% since 2007.

ECORYS Nederland BV
Watermanweg 44
3067 GG Rotterdam

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com
Registration no. 24316726

W www.ecorys.nl

Executive Summary

Background

Policy attention to the security industry increased substantially after the terrorist attacks in the U.S. on September 11th, 2001. With an increased demand for security, the global security market grew a tenfold to around €100 billion in 2011¹. Many studies expect that growth of the worldwide security market will continue to exceed the growth rate of world GDP.

In summer 2012 the European Commission launched an action plan for an innovative and competitive security industry² to enhance growth and increase employment in the EU's security industry. Better understanding of the main competitive strengths and weaknesses of the security industries in the EU and in major other countries should facilitate the development of policy measures to generate a business environment that enables the EU security industry to keep its leading position.

One of the main problems in the EU security market identified by the Commission is its fragmentation along national and sometimes even regional boundaries. One of the first steps to address this problem the Commission proposes is to set up an EU-wide certification system for airport screening (detection) equipment and for alarm systems³. Insight in costs and benefits of harmonized certification schemes will provide essential information for establishing such schemes at the EU level.

A further important ingredient for competitive success of the EU security industry is research and development (R&D) investment. Many western countries set up national research programmes focusing on security issues. In the EU this led to the creation of the FP7 Security Research Theme; the FP7 budget represents roughly 50% to 60% of the overall EU budget for security research. Some countries outside the EU have comparatively large civil security research programmes. Their experience could provide important information for the EU research efforts. A systematic comparison of such programmes could provide best practices and lessons for the EU research efforts in the civil security field. And also enable the Commission to facilitate future cooperation with these countries and improve competitiveness of the EU industry, in particular with regard to alarm systems and airport screening equipment.

In this light, the main objectives of this Study on Civil Security R&D in major third countries (SER3CO) are:

- first to provide an overview of the competitiveness of the security industries in the EU and in major third countries with a large security industrial base. These countries include Brazil, China, Israel, Japan, South Korea, Russia and the United States of America;
- to perform a cost-benefit analysis for establishing harmonised certification schemes for alarm systems and airport screening equipment in the EU for some suggested policy options; and
- to identify successful practices and measures in the national security research programmes of the major third countries and to develop a series of recommendations for the EU security research programme.

¹ European Commission Communication, Security Industrial Policy - Action Plan for an innovative and competitive Security Industry - COM (2012) 417 final. In Chapter 2 of this report, we provide some alternative and updated numbers for the size of the global and EU security market.

² Ibid.

³ Ibid.

Approach

The study has been executed by a team of specialists from the framework consortium partners ECORYS, DECISION and TNO, in collaboration with associated partners FOI (Sweden), HCSS (the Netherlands) and PLANCONSULT (Austria). The latter were invited for their access to sources and contacts in respective countries.

The approach the study team followed to achieve above stated objectives, was first to collect relevant information within respective countries. To collect relevant information desk research and interviews with local stakeholders have been applied; to some extent, also commercially available databases were explored. For some countries national support provided access to sources that otherwise had remained closed for the project team. Interviews with representatives from European Industries complemented the search for information and to get a European perspective, especially for the certification elements. The detailed results from these Country investigations are summarised the main report of the SER3CO study.

The information collected in the Country investigations then served as a basis for overall synthesis and analysis of the competitiveness of EU industries in comparison to selected countries. Here, the security markets are described both from a generic perspective and with a focus on Airport Security Equipment and on Alarm Systems.

Both for airport security systems and for alarm systems the customer provided a set of policy options that aim for harmonized certification schemes in Europe. For the cost benefit analysis the study team collected qualitative and quantitative information from European and non-European industries. Results from public consultations in both areas that the European Commission set out were input for the SER3CO study as were the results from the ERNCIP-AVSEC working group on "Inventory of procedures for approval employed in the EU for aviation security detection equipment".

In practice, the processes of information collection and analysis went in parallel as the lead time to find and collect data took longer than anticipated; language, yes/no access to parties, different regimes with respect to offering open (Internet) information, complex national organizational structures, interwoven defence and security, and - not the least - security policies presented barriers that we could but only partially tackle.

In the sequel here the results of the SER3CO study are summarised, starting with a comparative overview of the EU and third country security industries, followed by a synthesis of the assessment on harmonisation policy options for alarm systems and airport security systems. Finally the overview of security programming for respective countries is presented with some lessons for future EU R&D programming.

I Comparative overview of the EU and third country security industries

One of the main aims of this study is to contribute to a better understanding of the main competitive strengths and weaknesses of the security industries in the EU and in selected other countries, including those that are actually or potentially important competitors for the EU. The study complements previous work addressing the competitiveness of the EU security industry and can be set in the context of the action plan, launched by the European Commission in summer 2012, for an innovative and competitive security industry⁴. This action plan notes that many EU companies are

⁴ European Commission Communication, Security Industrial Policy - Action Plan for an innovative and competitive Security Industry - COM (2012) 417 final.

among the world leaders in the security industry. However, industry forecasts and independent studies predict that the market share of the EU companies in the world security market could drop from around 25% in 2010 to 20% in 2020.⁵

In assessing the position of the EU security industry in global markets it needs to be recognised that there exists a lack of comprehensive and widely agreed data on the size and composition of global security markets and corresponding industrial base. The security sector is poorly covered by official statistics and information from commercial market analysts and data providers also reveal substantial differences in the estimated size of the global security markets and segments, therein. Among the factors that appear to underlie difference in market size estimates are:

- The definition of the security market, in particular whether a relatively narrow definition is used that is focussed on 'homeland' security (i.e. security against high-level threats such as terrorism and organised crime) or a broader definition that includes security products employed to address a wider range of 'threat' categories and covering broader market segments including ordinary businesses and private households;
- The relative weight attached to public and private sector segments of overall; the weight of public sector is important, since it thought to account for as much 60% and 80% of security market demand;
- The size and scope of security service activities included in the overall estimates of markets size. It is also important to recognise that revenues from the sale of security products (e.g. equipment and systems) represent a relatively small part of the overall value of the security market.

Against this background, we estimate the size of the global security market in 2012 to have a value of approximately €137 billion, of which the EU security market amounted to about €35 billion or slightly above a quarter of the global market. The global share of the EU appears to have decreased somewhat compared to the Ecorys (2009) estimate for the year 2008. This reduction is the result of higher growth in emerging markets over the past years, as well as adjustment of some of the segment estimates based on new information. In general terms, both EU suppliers and their US counterparts, who together dominate the security industry as a whole, have experienced faster growth in market revenues in emerging markets than in the more mature 'domestic' EU and North America markets. Although, growth in these mature markets has arguably been better than might have been expected given the impact of the economic crisis.

Broadly speaking, Europe and the USA continue to be the global leaders in the security industry and generally occupy a position of technological frontrunners in high-end security equipment. However, the global supply-side situation differs across market segments, as is illustrated by the two segments assessed in more detail for this report. In the case of screening equipment for the aviation sector – and more broadly for other market segments such as maritime – the supply of main categories of equipment (passenger screening, carry-on and checked baggage, and cargo screening) is dominated by a handful of main global players, mainly from the EU and US. By contrast, the segment of security alarms – and, more broadly, 'electronic security' including access control and video surveillance – is far more fragmented. Leading European and American suppliers of alarm systems (e.g. Tyco, UTC, Honeywell, Siemens, Bosch, Stanley, etc.) probably account for no more than 25% of the global market. And a multitude of smaller local and regional players are active both as suppliers of products and, even more importantly, in installation and maintenance of equipment.

Looking beyond Europe and the USA, Israeli and Japanese companies occupy strong positions in some – typically high-end – niche market segments, notably for IT and communication systems.

⁵ Ibid.

Neither country has a significant position in the main categories of aviation security screening equipment, though Israel has a number of innovative technological solutions on offer. Both countries are, however, relatively important players in the electronic security field – specifically in video surveillance in the case of Israel – where they are able to offer sophisticated products and systems that are competitive with those from the EU and US. The two countries provide an interesting contrast in terms of the origins and development of the security industry. The Israeli security industry is closely linked to the defence industry (through which it also maintains strong connections with the USA) and its competitive position is based on the development of innovative technologies with proven operational effectiveness. In contrast, the Japanese security industry is more closely rooted to the country's traditional strengths in consumer electronics and engineering. This is reflected in a focus on networked solutions, intelligent performance and component miniaturisation.

Presently, the bulk of the Chinese security industry is positioned in low to medium-end equipment segments, specifically in relation to products such as alarm systems, access control and video surveillance equipment. The relatively fragmented nature of the domestic electronic security sector (compared to screening technologies, see below) is one of the factors that has allowed foreign players to develop a significant position in the Chinese market, particularly for higher-end products and more complex systems and solutions. However, although foreign companies are expected to benefit from the fast growing Chinese market – driven by factors such as urbanisation, major infrastructure development etc. – their overall share of the market is expected to diminish over time. With respect to the security screening segment, a small number of Chinese companies are active in the market. Most notable is Nuctech, a spin-off from National Tsinghua University in Beijing, which claims to be the leading global supplier of high-energy (cargo) security inspection systems. The case of Nuctech serves as a pointer towards the ambitions of China to establish its position in the security market, with the assistance of institutional support and funding for technology development.⁶ Equally, it shows that the Chinese approach to the security market encompasses an important component of commercial diplomacy.

Turning to the remaining three countries analysed in the report, none of them appear as major competitors for the EU security industry, at least with respect to the specific segments that are the focus for this study:

- Drawing on engineering and technological capabilities that have sometimes been inherited from the Soviet era, there are probably a handful of Russian companies that have the potential to be internationally competitive in some niche market segments but, on the whole, it is fair to say that this potential is some distance away from being fully exploited;
- South Korea is home to a number of highly export orientated companies that possess capabilities in the supply of electronic security related hardware and components (e.g. video cameras and digital video recorders (DVR)). However, the hardware specialisation of Korean companies and an apparent weakness in areas such as systems integration suggests that they are not an immediate threat to the competitive position of the EU (and US) security industry;
- Brazil's indigenous security industry is fragmented and currently does not occupy a significant position in the global marketplace. With respect to screening technologies and electronic security systems (alarm systems), it is unlikely that Brazil's weak competitive position will change any time soon, but the possibility for a stronger regional position cannot be ruled out.

⁶ The company has already been able to make significant inroads into the EU market, with contracts to supply products to, among others: Belgium, Denmark, Finland, Hungary, Ireland, Lithuania, Latvia, Malta, Netherlands, Poland and Slovenia. The company has, however, been embroiled in controversy, and has been subject to allegations of corruption and illegal and unfair business practices. In 2009, the EU imposed anti-dumping duties on the company's products, resulting in tit-for-tat anti-dumping duties being imposed by China in 2011. The Chinese duties were ruled to be in breach of WTO anti-dumping rules in February 2013. It seems unlikely, however, that the WTO decision will do much to actually open up the rapidly growing Chinese market for foreign screening equipment suppliers.

Equally, drawing on capabilities in aerospace and defence, the desire to provide 'home grown' solutions in fields such as wide-area border and maritime surveillance.

From the perspective of market demand and potential attractiveness for European suppliers, it is evident the US remains the largest single security market. At the same time, although the US security industry is presented as Europe's main competitor, it is also the case that several of the EU's leading companies have a strong market (and production) presence in the USA. This presence reflects both the continuing importance of the US market, both in terms of its overall size and its strategic importance from a global perspective (e.g. product approval and US market position act as a reference in the global security market). At the same time, when applicable to 'dual use' technologies, US International Traffic in Arms Regulation (ITAR) can be a constraint on companies wishing to supply products to the US market, since they may effectively limit the possibility to export technologies to other markets.

In terms of medium term growth prospects, it is evident that large and fast growing markets (e.g. Brazil, China and Russia) are all attractive in terms of their market potential. However, there may be significant market access barriers for EU suppliers, notably in the case of the Chinese aviation screening equipment market which appears to be largely closed to foreign competition with all major Chinese procurements being directed to local companies. Moreover, although China already provides component supplies and production facilities for less sophisticated electronic security equipment, concerns relating to intellectual property protection may somewhat reduce the attractiveness of the Chinese market for high-end and innovative security technologies. For both Brazil and Russia, the local security industries are not considered as major competitors for the EU. Nonetheless, preference for local suppliers combined with a willingness to opt for lower-cost and less sophisticated foreign solutions may mean that EU suppliers face considerable competition in these markets.

For a combination of historical and geopolitical reasons, which have resulted in strong defence ties to the US, Europe's position in security markets in Japan, Korea and Israel has traditionally fallen behind that of the USA. It does not appear, however, that this has particularly disadvantaged EU suppliers of aviation screening equipment. For electronic security products the situation is more complex, since all three countries have comparatively significant domestic capabilities (and exports). Nonetheless, in addition to their inherent market potential, these countries also appear to offer opportunities for sharing and development of technology and possible investments in production activities.

II Alarm systems and airport screening equipment: certification and conformity assessment

Alarm systems sector

Comparison of certification and conformity assessment schemes around the world

The certification and conformity assessment scheme for alarm systems differs significantly among countries studied. A common scheme for certification and conformity assessment is lacking in Europe, although there is a range of EN standards for alarm systems. Many countries outside Europe have standards for various categories of alarm systems. However, the coverage of these standards does address different categories of alarm systems. In some countries certificates are issued, but do standards not exist. It is also observed that in the majority of countries outside Europe that were studied, certification bodies are active in the area of alarm systems. There does

not seem to be any mutual recognition of certificates or test results from other nations to be applied in these countries outside Europe.

Cost-benefit analysis of harmonization of the EU certification scheme

In this study a cost-benefit analysis (CBA) of the harmonization of the certification scheme of security alarm systems in Europe has been carried out.

The baseline

There exist some European standards for security alarm systems. By nature of the EN standard, after its publication, such standard must be given the status of national standard in all CEN member countries (including all EU member states), which also have the obligation to withdraw any national standards that would conflict with it. Some certification bodies however, add additional regulation regarding quality of products on top of the EU standards. This forces manufacturers to manufacture country-specific configurations of their products which adds costs. There is at present no common EU certification scheme for security alarm systems, nor is there any mutual recognition of national certificates of security alarm systems. This means that when a manufacturer wants to sell its products on the European market, he must obtain national certificates in each of the member states to demonstrate that its product meet either a European Standard or a national standards. Industry initiatives such as the CERTALARM scheme and the cooperation between certification bodies and testing laboratories in the European Fire and Security Group (EFSG) have not solved the problems as indicated above.

The current certification process for alarm system affects the various stakeholders involved in different ways. Some stakeholders incur negative impacts, while others clearly benefit from the current situation:

- The manufacturing industry of alarm systems is generally negatively impacted by the existing certification process in Europe. It incurs **additional costs** to obtain different certificates in the EU member states, which asks for duplication of product testing. The current certification process impacts **the time to market** of products in Europe. The current certification process also forces manufacturers to develop local variants of products to comply with additional requirement on top of the EN standards. This increases the **costs of production**. Finally, the current certification process **hampers innovation** of alarm systems;
- Certification bodies and testing laboratories: under the current situation, manufacturers of alarm systems need to apply for certification locally. This means that for each national certificate the manufacturer will pay the certification body a fee for certifying its product. As such, the certification bodies **generate revenues** from the certification of alarm systems. The same applies for testing laboratories;
- Users: Users buy (either directly or indirectly) and use the alarm systems. In many cases one is mandated to buy alarm systems with a national certificate. This mandate can be done by insurers or for example by tenderers for construction work that demand in their tender dossier that an alarm system with a national certificate is installed. As the current system adds costs for manufacturers, the consequence is that **users pay more** for the alarm systems, as one may assume that the costs increase is included in the final sales price of the system.

The baseline costs for the certification and conformity assessment of alarm systems in Europe is estimated at €17– 60 million per year. More substantial costs are incurred by manufacturers resulting from a delayed time to market. This implies that they are hampered to implement cost reduction processes in their production stemming from a new product line. From our interview programme, it was made clear that this could be conservatively estimated as around €660K per new product. We conservatively estimate this as around €60-80 million for the entire market.

Policy options

The Commission has developed a set of alternative policy options in addition to the baseline option as detailed above. These are:

- 2. *"Recommendation"* – The Commission would issue a recommendation to Member States to mutually accept each other's national certification systems or to rely on the industry-led certification mechanism, provided that EU laboratories undertaking performance testing respect certain requirements. The aim of this recommendation would be to enable a producer of an alarm system to have his product certified only once in a single Member State in order to sell it in all Member States;
- 3. *"Legislation"* - The Commission would propose legislation on System/product certification and compliance testing principles. It would also specify areas/products/... for which standards need to be developed. The legislation would be elaborated jointly with regulators, industry representatives and certifiers alike. The aim of this legislation would be the same as for the recommendation, but implemented through a legally binding act of EU legislation. Two different variations of this legislation would be considered:
 - 3.1. *The "directive-based approach"*, is characterised by a set of detailed specifications which are laid out in the directive itself. This approach is based on the so called "old approach", which usually targets specific technologies and not general areas. Automotive, chemicals and pharmaceuticals are examples of fields in which it is applied. Within this approach, certification would be based on certification by a governmental authority;
 - 3.2. *The "standards-based approach"* is not based on specifications as detailed as under the directive-based approach. This approach is based on the so called "new approach", which focuses on essential requirements written in general terms. Product legislation is restricted to the requirements necessary to protect the public goals of health, safety and security. The technical specifications under the standards-based approach are elaborated by the responsible European Standardisation Organisations (CEN/CENELEC and ETSI). Within this approach, certification would be based either on a third party certification or on a self-certification.

Costs of the policy options

The costs for implementing the policy options have been assessed as follows.

Option 2: The costs for implementing option 2 is considered fairly limited compared to the baseline. The only costs that would be incurred from the Recommendation are the costs for assessing whether the testing laboratories in the EU undertake performance testing according to requirements. This would be a one-off cost to develop the assessment methodology, and annual recurrent costs to verify whether the laboratories worth according to the requirements.

Option 3.1: The costs for implementing option 3.1 would stem from the establishment of certification capacity in the governmental authority that would become responsible for certification under this option. However, the major advantage of this option is that approval and certification now needs only to be done once for the entire EU-28, while in the current situation it is clear that in at least 10 countries different approval and certification procedures are undertaken. On a balance it may thus be expected that this option 3.1 results in a cost reduction for authorities. In addition, the option would also lead to an avoidance of duplication of testing of alarm system products. Again, there would under this option be the necessity to test once if the product is conform the specifications in the directive. This implies reduced revenues for testing houses.

Option 3.2 The costs for implementing option 3.2 would stem from additional standards development by the European Standardisation Organisations (compared to their effort in the baseline). For firms, also the alternative – an equivalent standard – could be costly, since the burden of proof for equivalence to the EU standard falls on the firm. Furthermore, the costs would

be in establishing assessment capacity at European level that needs to verify whether the third party certification or the self certification processes are working according to the requirements. These costs would also accrue to firms in the end. As there are already experienced third party certifiers that certify alarm systems, the additional costs incurred by these entities are assumed to be zero. Costs for authorities currently involved in the approval and certification process is likely to decrease, as this involvement is no longer required. In addition, the option would also lead to an avoidance of duplication of testing of alarm system products. Again, there would under this option be the necessity to test once if the product conforms the specifications in the directive. This implies reduced revenues for testing houses.

Benefits of the policy options

Option 2

The benefits of option 2 are considered to be limited. It is questionable, confirmed by interviews with industry, whether the voluntary character of the option leads to mutual acceptance of certificates or to the acceptance of the CERTALARM initiative. After all, this would be possible already, and it does not happen. Currently, users or insurers are still demanding nationally certified products. If the Recommendation would not lead to mutual recognition of the industry initiative, benefits of this option would be nil. This is confirmed by the survey under stakeholders as carried out by the European Commission.

Option 3

The benefits of option 3 are more apparent. The legislation would take away the current main problem of multiple testing and certification. As such, it would lead to a reduction of costs for industry. Industry estimates that a saving of 80%+ of the baseline costs for certification and conformity assessment could be saved under this option. The SECERCA study⁷ estimated that 75% of the costs could be saved. Applying the average of this bandwidth to the baseline costs range of €17- 60, then the potential costs savings of this option would be around € 14-48 million per annum. These costs savings accrue to **manufacturers**. This would further allow for **production efficiencies**, as manufacturers would no longer need to amend products to national regulations. The survey of the European Commission under stakeholders indicated that the majority of manufacturers has to amend their products 12 times for this reason. Additionally, the option would also imply that:

- Manufacturers are able to sell their products faster on the entire European market, as the 'one-stop-shop' for EU testing and certification takes away a lengthy process to go through in each of the member states;
- Manufacturers would be able to use the certificates as an EU mark, which is a selling point in the market outside Europe. During the interviews, manufacturers indicated this to be important for markets such as Middle East / North Africa (MENA) and Latin-America. However, it should be noted that also non-European manufacturers are able to obtain their EU certificate and use it as a market instrument. It is not possible to quantify this impact;
- Smaller manufacturers would get access to a larger market, as they don't have to go through multiple testing and certification, which does prevent them to export from their own country in the baseline. This means that they could take different investment decisions for innovation projects, which affects the innovation rate positively in the industry;
- There would arise competition under certification bodies and testing laboratories. This would decrease costs for certification and testing.

In the CBA we have estimated the indirect benefits from a reduced time to market ranging from €40-€80 million per annum. These may likely be passed on to end users to a large extent. From our interviews, manufacturers indicate that they would expect the benefits to be in the same order of

⁷ Ecorys, 2011, Security Regulation, Conformity Assessment & Certification.

magnitude for option 3.1 and 3.2. However, option 3.2 would be building on the standardisation effort from the past 20 years, so it would be most logic to connect to. Respondents to the Commission's survey indicate to expect a higher impact from option 3.2 compared to option 3.1.

Conclusions

On a balance, option 3 is favourable over option 2. Due to the voluntary character of option 2, it is doubtful whether this leads to any benefits while one would need to make costs for the option. The option 3 brings significant direct and indirect benefits which may be above €100 million per year, plus a number of unquantifiable benefits as an improved competitive position on the market outside the EU. It is also likely that the option will have a positive impact on the price of alarm systems from the users perspective.

The distinction between option 3.1. and 3.2 would stem from the costs of the option. However, these also seem to be largely similar. The advantage of option 3.2 would be that the costs burden of the option would be on the manufacturer (either via self-certification or via third party certification), while in 3.1 there would still be a government authority involved. The downside of option 3.2. is that the ESO need to make more costs for further standard development. However, it would connect most to the 20 year positive experience from standard development on European level, and it allows for further rolling out the EU standard to international (outside EU) level (IEC), which could positively affect European products. The survey under stakeholders indicates that stakeholders expect a slightly higher impact from option 3.2 compared to 3.1. as well.

Airport screening equipment

Comparison of certification and conformity assessment schemes around the world

For airport screening equipment we have made another comparative overview. Like for alarm systems, there is no common EU certification and conformity assessment in Europe for airport screening equipment. The ECAC-CEP system exists, but this may still lead to the situation that countries may add national requirements, for which additional testing is required. Outside Europe, the situation differs significantly between countries. The USA has a complete testing and certification procedure. This US testing and certification procedure is free of charge, while the European ECAC CEP system is not. In China, a certification system in place for domestic and foreign manufacturers. Also in Japan, there are standards and certification of airport security equipment required, as in Brazil. Russia issues certificates on a voluntary level, in which there is a modest form of recognition of certificates and approvals from other nations and regions. In addition, there is national testing. South Korea relies on the certificates of the US or ECAC approvals.

Cost-benefit analysis of harmonization of the EU certification scheme

In this study a cost-benefit analysis (CBA) of the harmonization of the certification scheme of airport screening equipment in Europe has been carried out.

The baseline (option1)

There is currently no EU-wide certification system for airport screening security technologies. The EU legislation sets out requirements for airport screening equipment. For LEDS, the Regulation 185/2010 (annex paragraph 12.7.3) provides for the mutual recognition of the test results by all Member States. There is a lack of harmonised standards and of a legally binding conformity assessment of airport screening equipment at EU level. The European Civil Aviation Conference (ECAC) set up the Common Evaluation Process of security equipment (or CEP). This is the central system in the EU for the testing of airport screening equipment towards ECAC standards. ECAC CEP applies only to Explosive Detection Systems, Liquid Explosive Detection Systems, and security scanners. ECAC-CEP system is voluntary. ECAC provides reports to manufacturers indicating whether they passed the relevant test. And when a piece of equipment passes the tests, ECAC reports so to the 44 ECAC member states and on its ECAC website. Approvals or

certificates however, are only given by member states. To date, there are six ECAC- CEP test laboratories specialised in the testing of specific types of security equipment. The test laboratories are not subject to a harmonised accreditation system under EU legislation. 18 countries have a procedure in place for issuing product certificates, but only four countries do issue product certificates. Most commonly used criterion for obtaining an approval or a certificate is the successful passing of the ECAC CEP, . However, four countries do pose additional requirements on top of the ECAC CEP, and ; one further country is considering doing so. The baseline costs for the testing and approval procedures regarding airport screening equipment in Europe have been estimated to amount to approximately €2.6 – 4.6 million per year.

Policy options

The Commission formulated the following policy options in excess of the baseline (option 1):

- Option 2. "Recommendation" - The Commission would issue a recommendation to Member States to mutually accept each other's national approval systems or to rely on the common evaluation process of ECAC, provided that EU laboratories undertaking performance testing respect certain requirements. The aim of this recommendation is for producers of airport screening equipment to have their product approved in one Member State only to be allowed the selling other Member States without further approval requirements;
- Option 3 "Legislation" - The Commission would propose legislation on product certification and compliance testing principles and procedures in order to ensure full compliance with EU security performance standards adopted under Regulation (EC) 300/2008. The legislation would be elaborated jointly with regulators, industry representatives and certifiers alike. The aim of this legislation would be the same as for the recommendation, but implemented through a legally binding act of EU legislation. This approach would ensure that producers can sell their products without restrictions to operators in all Member States once they are certified in a single Member State. Three different legislative approaches were to be considered:
 - Option 3.1. The "directive-based approach" is characterised by a set of detailed specifications which are laid out in the directive itself. This approach is based on the so called "old approach", which usually targets specific technologies and not general areas. Automotive, chemicals and pharmaceuticals are fields in which such approach is applied. Product certification would be based on certification by a governmental authority;
 - Option 3.2. The "standards-based approach" (or "new approach") , focuses on essential requirements that are written in general terms. Product legislation is therefore restricted to the requirements necessary to protect the public goals of health, safety and security. The technical specifications under the new approach are to be elaborated by the responsible European Standardisation Organisations (CEN/CENELEC and ETSI). Within this approach, product certification would be based either on a third party certification or on a self-certification;
 - Option 3.3. The "centralised approach", product certification to be done centrally by an EU agency, such as the European Aviation Safety Agency, which already certifies all EU commercial aircraft.

Costs of the policy options

The costs of implementing the policy options have been estimated as follows:

- Option 2: the costs of implementing policy option 2 seem to be relatively limited. The option does not seem to have requirements that would lead to costs for stakeholders. The only cost impacting feature is that EU laboratories undertaking performance testing need to respect certain requirements. One may expect that these laboratories are audited to verify this. It is unclear which organisation would do this, but it would bring about additional costs. These costs would be directly born by the laboratories, but may be transferred to the manufacturers;
- Option 3.1: Regarding option 3.1 one may expect that the existing national authorities in the member states that currently approve or certify airport screening equipment, would be tasked to

carry out the product certification. However, this would need to be done in only one member state, as the certificate issued would now be valid in all members states. As stated above, currently some 18 member states are issuing certificates or approvals. Apart from one member state, the other 17 would no longer need to certify. It is our understanding that the costs for approval or certification incurred by national authorities are pretty limited. On a balance the costs for certification are therefore considered to be in the same order of magnitude as in the baseline. These costs are incurred by the authorities and passed on to the manufacturers;

- Option 3.2: the same line of reasoning is valid for the costs of certification as in option 3.1. Under the scheme of self-certification, these costs would not be incurred, but that would presumably imply that an auditing scheme must be established to verify whether the certificates are granted according to the requirements. The main costs for implementation of the option 3.2 would be additional effort put on the European Standards Organisations to develop the product standards. One may assume that this would be on average 2-3 staff extra involved in this activity, i.e. costs would amount € 200-300k on average per year. This is borne by the ESOs, which would require additional funding from member states and/or industry;
- Option 3.3: the main costs of option 3.3 would be the extension of EASA (staff) required to accommodate the additional certification task. The costs would be charged to industry applying for certification. These costs are difficult to estimate. However, in EASA's charges and fee publication, it charges around € 2.250 for certification of aircraft products with a value above € 20,000. This seems the most applicable value at the moment. Assuming some 16 types per year the costs would amount to some € 36,000 per annum.

It should be taken into consideration that no choice has been made already with regard to the number of testing laboratories that could become operational after the adoption of the possible Commission's legislative proposal in this area. If one would therefore assume that in each sub-option the same test infrastructure would still be used as in the baseline there is no cost impact for testing laboratories. It may also be assumed that the funding structure of ECAC-CEP would change, as ECAC-CEP is now funded by four member states, and under the options the costs would be shared under 27 member states.

Benefits of the policy options

Option 2

The benefits of option 2 are uncertain. As the option is limited to a recommendation (and thus is not mandatory), it is not clear whether this would lead to the desired effects. Indications from industry are not optimistic in the respect. This is confirmed by the Commission's survey among stakeholders.

Option 3

A key direct benefit is the **reduction of duplication of testing** for manufacturers. Our interview programme indicated that for some 50% of the screening equipment machines offered for testing and approval, additional testing procedures were required due to more stringent requirements from additional national regulation.

Reducing this translates into annual benefits of about 0.5-0.8 M€. This value includes costs for preparation of the testing procedure for manufacturers.

Different national requirements imply that manufacturers need to amend their products to comply with national regulations, which negatively affects production costs. A reduction of national requirements thus offers a **decrease of production costs** for manufacturers. Furthermore, a common EU wide certification scheme brings **more clarity on the testing procedure and timing of the procedure** than in the baseline. This is also positive for manufacturers.

Finally, an EU wide certification and testing procedure coordinated by an EU recognised organisation could reduce the risk for delays in the testing procedure and is likely to **decrease the time to market** of airport screening equipment for European producers. Such time to market improvement has two implications:

- Reduced differences in time to market between European manufacturers. This is not likely to affect the market volume, but will lead to **market share shifts** between European manufacturers;
- **Improved competitive position** of European manufacturers vis-à-vis non-European manufacturers in the European market. This is addressed below.

An EU certificate could function as a quality mark, that could **improve sales of EU manufacturers outside Europe** positively. During the interviews manufacturers stated that having an EU Certificate or Formal Approval would benefit their Go To Market in third Countries and following this the EU influence in equipment used in third countries grows. Their experience is that manufacturers that have a product that is Certified by the Transportation Security Administration, are using this “TSA stamp” in their sales on third markets, especially emerging markets, as a selling argument. This picture is confirmed in some of the country studies such as South Korea. When the EU would also be following the line of issuing formal EU Certificates for security equipment, EU manufacturers could also use this to generate sales in third countries. Therefore third countries would be deciding to accept EU certificates and enlarge the influence of the EU legislation beyond the EU boundaries. This impact has been valued at €35 million, in terms of lower revenue growth on third markets for major EU manufacturers compared to their US competitors for the total period after the introduction of the TSA certification system. This is about €10 million on average per year.

A single EU wide certification system is likely to **improve the competitive position** of EU manufacturers on the EU market, vis-à-vis their non-EU competitors. Non-EU producers can now easily put their products in several EU countries on the market once they are TSA approved. A common EU certification system implies that these manufacturers have to go through the same route of testing and certification as the EU manufacturers. We have quantified this in section 2.4.2 again by comparing the revenue growth rates of EU and US manufacturers, but now for the EU market. This has been quantified at a value of €42 million for the total period since the TSA certification, which is about €12 million per annum.

One could argue that the direct benefits for manufacturers would have a negative impact on the sales price of the equipment. However, based on the current market structure with only a few suppliers per equipment type it is expected that cost pass-through is limited to zero, i.e. the impact on sales price would be absent.

Conclusions

The main conclusions from the analysis are:

- The benefits of option 2 are marginal (if any) due to the voluntary character of the option. At the same time, costs need to be incurred. As a result, benefits do not seem to outweigh the costs for this option;
- The benefits of sub option 3.1, 3.2, and 3.3 are on the same level. Our interview programme with eight manufacturers did not reveal any preference in this respect, as long as the option 3 was implemented (irrespective of the variant). However, the stakeholder consultation carried out by the Commission indicated that impacts are to be expected larger under option 3.3;
- The main benefit of the option 3 is indirect: a European certificate brings European manufacturers ‘on par’ with their US competitors on markets in emerging markets and in Europe. The improved competitive position will increase revenue for the manufacturers and value added for the European economy. This is irrespective of the suboption chosen;

- Option 3.1 scores slightly better in terms of the benefit-to cost balance than the other suboptions, stemming from the difference in costs. However, the degree of uncertainty around the costs could influence this ranking.

III Security R&D Programming

The seven countries covered in this report differ enormously in terms of their security environment, policy priorities, institutional context, technological advancement and other factors. These differences have direct implications for their civil security R&D policies, institutions and performance. Two major factors have a particular importance in this regard:

1. The domestic security environment and public perception of security threats; and
2. The national innovation system.

It is not a pure coincidence that the three countries with the largest number of fatalities caused by terrorist accidents since 2000 – the US, Russia and Israel – are also the countries where the government assign a particular importance to security R&D.

Systematic information on security R&D is limited. The main reason for this lack of data is the fact that security is not included directly in the common classification systems used by statistical agencies to collect R&D data. Even when data are available their comparability is limited by different methodologies used in collecting data in different countries. This lack of information makes it difficult to conduct a comprehensive comparative assessment of security R&D programmes in the selected countries. Nevertheless, our analysis reveals some important facts and observations.

The US federal government is by far largest funder of security R&D. In recent years it has spend between 4.9-5.9 billion USD (or 3.7-4.4 billion EUR) annually on homeland security R&D. This is significantly more than any other country allocate to security R&D. The US Department of Defense and the Department of Health and Human Services (through the National Institutes of Health) were largest funders within the government exceeding the funding from the Department of Homeland Security. The level of homeland security R&D funding in the US has not changed much in the last 5-7 years and even declined in real dollars (i.e. accounting for inflation). At the same time, in Russia federal government's expenditure on security and safety R&D grew very rapidly in recent year and exceeded 800 million EUR in 2012. In other countries (excluding China for which information on security R&D is not known and difficult to judge) public investment in security R&D seem to be significantly lower. However, in Japan and Korea this to some extent is balanced by large investment of private companies in security technologies.

Information on thematic priorities for security R&D tend be scare and disorganised. There are substantial differences between the countries but there are some common themes as well. Probably the most common is cyber security. This area is prioritised in all seven countries. Other popular areas (but probably not common to all countries) include detection of explosives, critical infrastructure protection and biometrics. In the US considerable attention and resources are devoted to countering the threat of bioterrorism.

Lessons for Europe

Finally, the report identifies some lessons (based primarily on the US experience) that can be useful in designing EU security R&D programmes:

1. National context and policy priorities matter a lot in the field of security R&D. The perception of the security threats have direct implications for budget allocations to security R&D and its thematic priorities;

2. Security R&D is in many aspects a new field where an institutional framework is still in the process of active evolution. This increases *the risk of duplication of R&D efforts*. This risk is amplified by often overlapping responsibilities in the security field (e.g. in cyber defence);
3. Security R&D should be oriented to customers' needs. This requires close involvement of first responders and other operational agencies in setting R&D programmes' directions and providing feedback on their implementation;
4. Late stages of R&D is often critical for successful introduction of a product to the market. Pre-commercial procurement and similar instruments should play an important role in facilitating commercialisation of new security technologies;
5. Close collaboration between different actors (between public and private sector, between end users and R&D performers, between universities and applied science institutes, etc.) is important in leveraging R&D investment and fostering new ideas.

Table of contents

Executive Summary	3
1 Scope and objectives of the study	19
1.1 General Context – Background	19
1.2 Aims and Objectives of the study	20
1.3 Approach	20
1.4 Chapter Outline	21
2 Comparative overview of the security industry	23
2.1 Introduction	23
2.2 Global and European security market overview	23
2.2.1 General issues related to market size estimates	23
2.2.2 Security market taxonomy	24
2.2.3 Global and EU security market estimates	25
2.3 Overview of third country security markets	26
2.3.1 USA	26
2.3.2 Russia	36
2.3.3 Japan	46
2.3.4 South Korea	51
2.3.5 Israel	62
2.3.6 China	72
2.3.7 Brazil	88
2.4 Competitive position of the airport screening and alarm systems industries	98
2.4.1 Introduction	98
2.4.2 Overview of the airport screening sector	98
2.4.3 Overview of the intruder and fire alarms sector	113
2.5 Summary and conclusions	125
2.5.1 Competitive position of selected countries	125
2.5.2 Market attractiveness of selected countries	127
3 Alarm systems and airport screening equipment: certification and conformity assessment	131
3.1 Comparative overview of certification schemes around the world	131
3.1.1 Alarm systems	131
3.1.2 Airport screening equipment	134
3.2 EU Certification and conformity assessment – CBA alarm systems	137
3.2.1 Introduction	137
3.2.2 Baseline	137
3.2.3 Quantifying the baseline	142
3.2.4 Policy options	144
3.3 EU Certification and conformity assessment – CBA airport screening equipment	147
3.3.1 Baseline scenario	148
3.3.2 Quantifying the baseline	154
3.3.3 Policy options	156
4 Security R&D programmes	163
4.1 Introduction	163

4.2	General context: overall R&D landscape and security environment	163
4.2.1	Security environment	163
4.2.2	National innovation system	164
4.3	Security R&D	168
4.3.1	Expenditures	168
4.3.2	Main actors	172
4.3.3	Thematic priorities	176
4.4	Lessons from the security R&D in major third countries and recommendations for the EU	177

1 Scope and objectives of the study

1.1 General Context – Background

Security is a fundamental human need and a basic requirement for social and economic development. The security industry provides goods and services that help society to address various threats, in particular associated with organized crime and terrorism. Policy attention to the security industry increased substantially after the terrorist attacks in the U.S. on September 11th, 2001, which raised awareness of new security threats and increased demand for security. Over the last 10 years the global security market has grown about tenfold from some €10 billion to around €100 billion in 2011, though these estimates are surrounded by a quite large margin of uncertainty.⁸ Many studies expect that growth of the worldwide security market will continue to exceed the growth rate of world GDP.

In summer 2012 the European Commission launched an action plan for an innovative and competitive security industry⁹ with the aim to enhance growth and increase employment in the EU's security industry. It notes that many EU companies are among the world leaders in the security industry. However, industry forecasts and independent studies predict that the market share of the EU companies in the world security market could drop from around 25% in 2010 to 20% in 2020.¹⁰

Better understanding of the main competitive strengths and weaknesses of the security industries in the EU and in major other countries should facilitate the development of policy measures aimed at generating a business environment that enables the EU security industry to keep its leading position. Therefore, the first objective of the proposed study is to provide an overview of the competitiveness of the security industries in the EU and in major third countries with a large security industrial base.

One of the main problems in the EU security market identified by the Commission is its fragmentation along national and sometimes even regional boundaries. Absence of EU-wide certification systems for security products has undoubtedly contributed to market fragmentation. As one of the first steps to address this problem the Commission proposed to set up an EU-wide certification system for:¹¹

- airport screening (detection) equipment; and
- alarm systems.

A detailed analysis of the costs and benefits of harmonized certification schemes is a main topic of the study and will provide essential information for establishing such schemes at the EU level.

A further important ingredient for competitive success of the EU security industry is research and development (R&D) investment. After the September 11 terrorist attack many western countries set up national research programmes focusing on security issues. In the EU this led to the creation of the FP7 Security Research Theme. The FP7 budget represents roughly 50% to 60% of the overall EU budget for security research.

⁸ European Commission Communication, Security Industrial Policy - Action Plan for an innovative and competitive Security Industry - COM (2012) 417 final. In Chapter 2 of this report, we provide some alternative and updated numbers for the size of the global and EU security market.

⁹ Ibid.

¹⁰ Ibid.

¹¹ Ibid.

Some countries outside the EU such as the U.S., Russia and Japan have comparatively large civil security research programmes. Their experience could provide important information for the EU research efforts. However, information on civil security R&D programmes in these countries is dispersed in a large number of sources and often quite limited. There is no systematic comparison of these programmes that would include comparative analysis of their strong and weak points, best practices and outcomes. In order to address this issue this study will provide such an analysis and derive lessons for the EU research efforts in the civil security field.

An overview of these research programmes and industry base should also enable the Commission to facilitate future cooperation with these countries and improve competitiveness of the EU industry in particular with regard to alarm systems and airport screening equipment.

1.2 Aims and Objectives of the study

The main objectives of the SER3CO study are:

1. To provide a detailed overview of the competitiveness of the security industries in the EU and major third countries, including Brazil, China, Israel, Japan, South Korea, Russia and the United States;
2. To perform a cost-benefit analysis for establishing harmonised certification schemes for alarm systems and airport screening equipment in the EU;
3. To identify successful practices and measures in the national security research programmes of these major third countries and, based on this analysis, to develop a series of recommendations for the EU security research programme.

1.3 Approach

The approach this study followed to achieve above stated objectives, was first to collect relevant information within respective countries. Amongst the members of our consortium the Country investigations were distributed according to following scheme:

DECISION:	USA, Japan	Planconsult:	China, Israel
FOI:	Korea	TNO:	Brazil
HCSS:	Russia		

The selection was based on these partners having local agents in respective countries and/or the strength of their network.

To collect relevant information desk research and interviews with local stakeholders have been applied; to some extent, also commercially available databases were explored. For some countries national support (diplomatic channels) provided access to sources that otherwise had remained closed for the project team.

Interviews with representatives from European Industries complemented the search for information and to get a European perspective, especially for the certification elements.

The information collected in the Country investigations served as a basis for overall synthesis and analysis of the competitiveness of EU industries in comparison to selected countries, to seek for Research and Development practices in these countries that may be of interest for use within EU and to reflect on EU certification policies.

In practice, the processes of information collection and analysis went in parallel as the lead time to find and collect data took longer than anticipated; language, yes/no access to parties, different regimes with respect to offering open (Internet) information, complex national organisation structures, interwoven defence and security, and - not the least - security policies presented barriers that we could but only partially tackle.

1.4 Chapter Outline

The results of the study are presented in the next chapters. Chapter 2 starts with a synthesis of the security markets and competitiveness of security industries in respective countries. Basically it provides per country a general picture first and then specifies the Alarm Systems and the Airport Screening Systems market segments. This is followed by an assessment of the competitiveness of the EU security industries.

The next Chapter 3 is dedicated to Certification Policies. First, a comparison of Certification policies in respective countries for both Alarm Systems and for Airport Screening Equipment is made. This is followed by a Cost Benefit Analysis for both categories and for a number of policy options as were provided by the Customer.

Chapter 4 finally deals with Security R&D policies and programmes in respective countries and seeks for recommendations for EU R&D programming policies.

The in-depth country reports are consolidated and attached in a separate volume to this report.

2 Comparative overview of the security industry

2.1 Introduction

This Chapter covers two main items:

- Overview of the value of global and European security markets (Section 2.2);
- Summary of the situation and competitive position of security industries in selected third countries (Section 2.3). The summaries for each country are based on information contained in the individual country reports, which are provided in a separate supporting document as Annex to this report.

2.2 Global and European security market overview

2.2.1 General issues related to market size estimates

Ecorys (2009) estimated the value of the global security market at approximately € 100 billion in 2008. The value of the European market was estimated to be in the range of € 26 to € 36 billion. Based on a narrower definition, the European Organisation for Security (EOS) estimated that the European security system market (including border control, protection of infrastructures and of the cyber space, crisis / disaster management) was expected to reach € 11-12 billion in 2012, compared to a world market of € 50 - 60 billion.

Information from commercial market analysts and data providers also reveals substantial differences in the estimated size of the global security markets and segments, therein. For example, Visiongain¹² (2012), which provides one of the baseline sources used in this study, estimates the value of the global (homeland) security market at \$ 206 billion (€ 158 billion) in 2012. The large range of available estimates confirms the difficulty in obtaining a precise idea of the value of the security market and, equally, that of the EU and global security industry.

Among the factors that appear to underlie difference in market size estimates are:

- The definition of the security market, in particular whether a relatively narrow definition is used that is focussed on 'homeland' security (i.e. security against high-level threats such as terrorism and organised crime) or a broader definition that includes security products employed to address a wider range of 'threat' categories and covering broader market segments including ordinary businesses and private households;
- The relative weight attached to public and private sector segments of overall; the weight of public sector is important, since it thought to account for as much 60% and 80% of security market demand;
- The size and scope of security service activities included in the overall estimates of markets size. It is also important to recognise that revenues from the sale of security products (e.g. equipment and systems) represent a relatively small part of the overall value of the security market.

As an illustration of the final point made above, estimates presented by Euralarm indicate that service revenues account for around 70% of the market for access, intruder and surveillance systems (see Table 2.1). Similarly, data on the breakdown of revenues from the leading US

¹² Visiongain (2012): The Homeland Security Market 2012-2022.

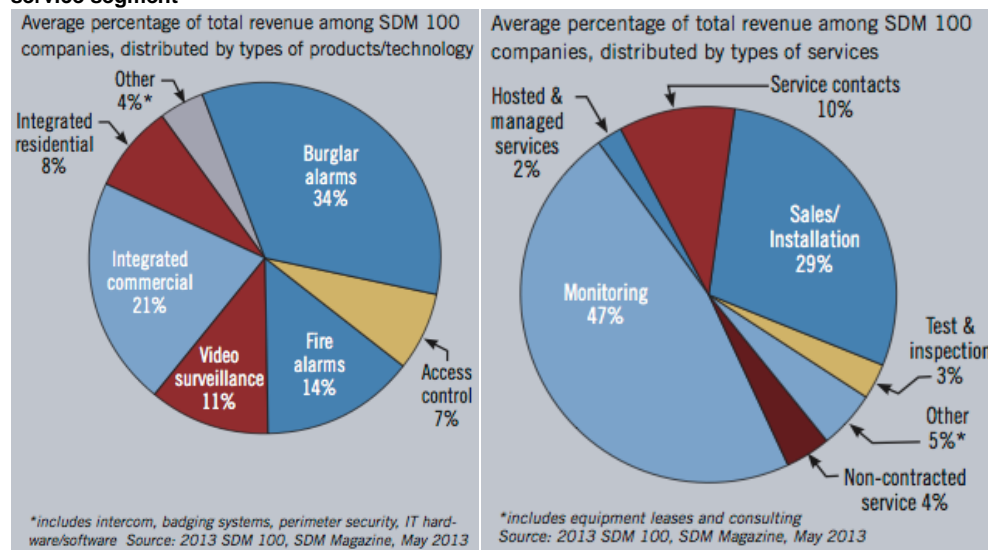
providers of electronic security products and services, indicate that actual sales and installation account for only 29% of revenues (see Table 2.1).

Table 2.1 European Market for Electronic Security Products and Services (EUR million)

	Value	Share
Product revenues		
Access Control	612	5%
Intruder Alarms	720	6%
Video Surveillance	1,933	17%
Service Revenues		
Security Services	8,029	71%
Total	11,294	100%

Source: Euralarm¹³.

Figure 2.1 Electronic Security Products and Services: composition of revenues by product type and service segment



Source: SDM 100.

2.2.2 Security market taxonomy

To assess the division of the security market across segments, we apply the breakdown illustrated in the Table 2.2 below. This taxonomy looks at the market both from the demand (application) and supply sides.

Table 2.2 Taxonomy of the security market

Demand side (Demand based markets)		Supply side (Technologies/Capabilities)
Border Security	↔	Screening (detection)
Civil Protection (CBRNE, disaster management, etc.)		Tracing
Critical Infrastructure Protection		Surveillance
Other		Protection

¹³ Euralarm (2012), "A Vision for a Competitive European Security Industry and Secure Society", Euralarm white paper outlining European Policy Priorities and action agenda 2013-2015. Available at: https://www.euralarm.org/media/news_files/2013/05/White_Paper_14052013.pdf.

2.2.3 Global and EU security market estimates

Drawing on the taxonomy outlined above, Table 2.3 provides rough estimates for the global and EU security market and segments. These estimates are based on various sources, including Ecorys (2009)¹⁴, Visiongain (2012a and 2012b)¹⁵ and abstracts from various commercial analyst reports that are available online, etc. Overall, we estimate the size of the global security market in 2012 to have a value of approximately € 137 billion; this estimate is located in the middle ground between quite a large range of available estimates, some of which suggest that the global market size may even be as high as € 200 billion (notable due to larger estimates of the size of the public market).

Table 2.3 Market size estimates security-segments in 2012 (EUR billion)

Segment	Global	EU	EU share
Aviation	14	4.2	30%
Maritime	10	2.0	20%
Border	13	5.2	40%
Critical Infrastructure Protection (CIP)	18	3.6	20%
Counter Terrorism	25	6.3	25%
Physical Security (Electronic security systems)*, of which:	45	11.3	25%
- Alarm systems / access control	32	10.0	30%
- CCTV			
Protective clothing / other	12	2.4	20%
Total	137	35.0	26%

Sources: Ecorys estimates based on Ecorys (2009), Visiongain (2012 a, b) and expert opinion. Note: * physical security also includes CBRN equipment and physical perimeter access control such as fences.

The EU security market in 2012 amounted to about €35 billion according to our estimate. This represents about a quarter of the global market. The global share of the EU appears to have decreased somewhat compared to the Ecorys (2009) estimate for the year 2008. This reduction is the result of higher growth in emerging markets over the past years, as well as adjustment of some of the segment estimates based on new information.¹⁶

In terms of market segmentation, we make a breakdown for the main market categories (cf. aviation, maritime, border protection, CIP, and counter terrorism). Among the segments with the greatest divergence in estimated global value is counter terrorism, which includes not only some specialised equipment segments but also important components of cyber security/surveillance and intelligence gathering. Information on expenditures of these types of activities is not readily available and the estimate provided in Table 2.3 may be quite conservative (e.g. Visiongain estimate the value of this market segment at around € 45 billion). The segment of physical security relates mainly to electronic security equipment such as access control, intruder alarm systems and detection systems, and (video) surveillance equipment (e.g. CCTV). It also covers other physical security products such as barriers, fencing, etc. It should be noted that physical security products may also find applications in the aforementioned market segments (e.g. aviation, maritime, etc.), such that it is difficult to establish a precise dividing line between the various market segments.

From a technology-based perspective, we are unable to provide a detailed and comprehensive breakdown by technology segment. However, by way of indication: passenger and baggage

¹⁴ Ecorys, in collaboration with Decision Etudes & Conseil and TNO (2009): Study on the Competitiveness of the EU security industry.

¹⁵ Visiongain (2012): The Homeland Security Market 2012-2022; Visiongain (2012): The Aviation Security Market 2012-2022.

¹⁶ For example, we have revised the global aviation security market upwards, as the Ecorys (2009) probably underestimated the market size, even when scaled up to 2012.

screening equipment has an estimated global market value of around €7 billion in 2012, detection equipment is estimated at around €4 billion, and tracking and tracing equipment at €10 billion.

2.3 Overview of third country security markets

2.3.1 USA

Security context

In response to the attacks of 9/11 and to enhance security on its territory, the US government created the Department of Homeland Security (DHS) to improve the protection of the country and its citizens to a broader scope of threats, from terrorist activities to natural disasters. The five missions of DHS are:

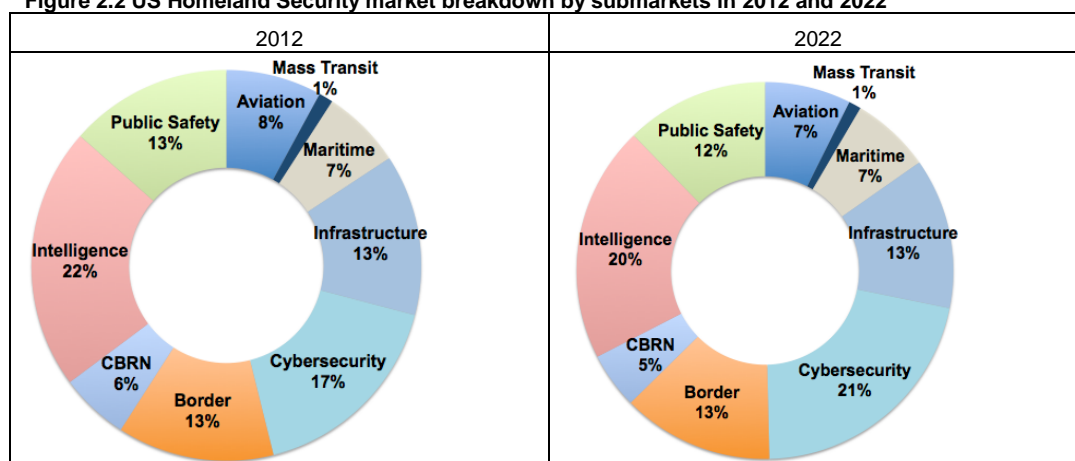
- Prevention of terrorism and enhancing security;
- Securing and managing US borders;
- Enforcing and administering immigration laws;
- Safeguarding and securing cyberspace;
- Ensuring resilience to disasters.

With more than 200,000 people employed and a budget of \$61 billion (€47.5 billion) for the fiscal year 2013, the DHS is a key driver for the security in the US, both from the supply and the demand side.

General security market development

According to Visiongain (2012)¹⁷, in 2012 the US homeland security market reached \$67.3 billion (€52 billion). Accounting for one-third of the global homeland security market, the US is the largest market worldwide.¹⁸ In spite of a forecasted flat growth trend over the ten coming years, it is planned to climb to almost \$80 billion in 2022 (€62 billion¹⁹) and should maintain its world number 1 position with 23% of market share. Over the period, the market is forecasted to grow on average at a low 1.7% per year.

Figure 2.2 US Homeland Security market breakdown by submarkets in 2012 and 2022



Source: Visiongain 2012.

¹⁷ Visiongain (2012): The Homeland Security Market 2012-2022.

¹⁸ As noted earlier (see Section 2.2.1), there are substantial differences in estimates of the overall size of the global market for security. To some extent this may be the result of difference in definitions of the scope and coverage of the 'security market'. At the same time, booming demand in emerging countries (e.g. China and India) relative to lower growth in more mature markets (e.g. EU and USA) imply that the share of emerging countries in the overall market is increasing. Over the past few years the BRIC countries are believed to have enjoyed double-digit growth in demand, hence increasing their share in global markets vis-à-vis the US and the EU. Consequently the share of the US is thought to have fallen from around half the global market to somewhere around one third.

¹⁹ At constant exchange rate (base year 2012).




Situation of the security (equipment) industry

The US security industrial base has become one of the most competitive in the world mainly thanks to the specifics of its national market, which is the largest worldwide for homeland security. In geographical terms, the US occupies a vast territory with two long coastlines and frontiers requiring massive public investment for an efficient protection. The products needed to meet this demand have similar specifications to military equipment and the US firms have taken advantage of their leading positions in the defence industry to create spin-offs or dedicated division to address the US homeland security market. This trend has been reinforced since the creation of the Department of Homeland Security in 2002, which reunited different competencies under a unique national agency responsible for procurement, R&D, etc. in the field of civil security.

Despite a stagnant economic situation, the DHS budget with \$60.8 billion (€47.5 billion) granted for the fiscal year 2013 is still the third largest cabinet budget but contrary to defence spending, DHS expenditure requires the maintenance of a smaller industrial base. Therefore, policymakers are more inclined to reduce the commercial-off-the-shelf (COTS) aspects of the homeland security market like for example the scanners, whose standardized production is easier to resume when budgets are going up rather than, for instance, traditional highly complex defence equipment like tanks, which cannot suffer any disruption in their production process without entailing a quick loss in the skills and competencies of the manufacturers, etc. In the medium term, it could be a threat to the airport screening equipment industry. In addition, US defence companies present on the security market could suffer from the harsh budgetary cuts of the Department of Defence and could less benefit from the economy of scales stemming from defence production.

The US public authorities have developed successful tools to promote the emergence of their small security industrial base and particularly thanks to the SBIR Program, which primary goal is to foster small innovative firms by converting R&D funding into commercial products for the needs of the domestic market and where possible for exports. SBIR is a three-phase program (cf. chart below) that achieved positive outcome according to a survey conducted by the DHS. For example, more than 96% of the companies interviewed reported sales « either to the government and/or primes and/or the open market »²⁰. In 2011, small firms represented the majority of contractors and received around 30 percent of the total contract amount²¹.

Figure 2.3 DHS S&T Directorate SBIR Structure

	Phase I: Scientific and Technical Feasibility	<ul style="list-style-type: none">• \$100K for base effort<ul style="list-style-type: none">• not to exceed 6 months• potential for additional \$50K for Phase I option<ul style="list-style-type: none">• additional 4 months• 33% may be outsourced
	Phase II: Concept Development	<ul style="list-style-type: none">• \$750K for base effort<ul style="list-style-type: none">• not to exceed 24 months• potential for additional \$250,000 for Phase II option• 50% may be outsourced
	Phase III: Product Development	<ul style="list-style-type: none">• Private or non-SBIR government funding• No dollar or time limits• Size standards do not apply

Source: SBIR.

²⁰ The DHS Small Business Innovation Research Program: Engaging Small Businesses to Meet DHS Needs and Achieving Results.

²¹ U.S. Department of Homeland Security Contract Spending and the Supporting Industrial Base, 2004–2011 (CSIC).

Secondly, large economy of scales have been made possible thanks to the large population of the country which now exceeds 300 million of inhabitants and offers a voluminous consumer base for alarm systems equipment and monitoring services. The development of this business activity started an almost one century ago in the US because of the high level of criminality in the country. On the equipment side, the industry is composed of three American leaders namely Tyco, UTC Fire & Security and Honeywell which corner the lion's share and solidified their position through number of acquisitions. The trend for alarm monitoring companies followed suit and was the industry originally very fragmented and localized it began to consolidate in the late 1980s and accelerated in the early 1990s. In the 1990s, the decreasing installation costs pushed the residential market to massively equip with alarm systems. In the coming years, the weight and the sophistication of software will increase to process the flow of data and to steer it to the IP-connected mobile devices of the customer. New market drivers could be also find with the expansion to other security services like the monitoring of medical alert signals, water pipe and gas leaks, etc.

It is to be noticed that both public and private equity and relatively inexpensive debt capital have, over the past few years, raised a wave of investment in the US alarm industry as well as corporate consolidation, which is leading to larger enterprises. Due to the characteristics of the US alarm systems market which has experienced a long track record of stable, recession resilient cash flows but also significant economies of scales combined to an attractive borrowing environment, private equity investors have become more active to seek participations in firms active on this market.

The shift in ownership towards private equity is expected to continue as more alarm companies cross the threshold where they can access the institutional equity and debt markets. The availability of capital among the top, middle, and bottom tier companies is significant as an appetite for yield coupled with a better educated investor base has raised the profile for alarm monitoring companies resulting in oversubscribed syndications.

This rising influence of institutional investors can be seen as a net positive with the implementation of best practices and the investment of capital in new, innovative products and services.

both public and private equity and relatively inexpensive debt capital have, over the past few years, raised a wave of investment in the US alarm industry as well as corporate.

This rising influence of institutional investors can be seen as a net positive with the implementation of best practices and the investment of capital in new, innovative products and services.

Assessment of main DHS contractors

In 2006, the top 20 of DHS contractors was exclusively the preserve of US companies; in 2011 three European firms managed to tap this ranking: EADS, Safran and Securitas AB. In 2011, the Top 20 was composed of a larger number of Information Technology (IT) firms compared to the ranking of 2006, which let appeared a higher number of construction-focused companies (mainly because of the post-Katrina hurricane effort). Indeed, in 2011, 4 out of the 5 first top DHS contractors were providers of IT-related products or services and all of them were US companies. Thus, for example, in 2010 Computer Sciences Corporation (CSC) won a \$500 million contract to provide IT solutions for TSA's IT infrastructure program. And currently, Lockheed Martin is the prime contractor for TSA's Transportation Worker Identification Credential (TWIC) program.

Table 2.4 Top 20 DHS Contractors by amount of contract obligations awarded in 2006 and 2011

Rank	2006		2011	
	Company (Country)	Contract obligations (\$M)	Company (Country)	Contract obligations (\$M)
1	Fluor (US)	1,657	Huntington Ingalls Industries*** (US)	1,053
2	Shaw Group (US)	937	Computer Sciences Corp. (US)	473
3	Integrated Coast Guard Systems* (US)	643	IBM (US)	470
4	Bechtel (US)	517	Lockheed Martin (US)	446
5	Ch2M Hill (US)	481	SAIC (US)	249
6	IBM (US)	456	Hewlett-Packard (US)	236
7	Unisys (US)	427	EADS (Eur)	203
8	L3 Communications (US)	389	General Dynamics (US)	201
9	NISTAC** (US)	362	Booz Allen Hamilton (US)	198
10	American Red Cross (US)	314	Bollinger Shipyards (US)	187
11	Northrop Grumman (US)	262	L3 Communications (US)	181
12	SAIC (US)	242	Safran (Fra)	180
13	JHM (US)	191	Accenture (US/Irl)	156
14	GEO Group (US)	183	Dell (US)	159
15	Akal Security (US)	175	Defence Support Services (US)	139
16	Accenture (US/Irl)	157	Unisys (US)	138
17	Dewberry (US)	156	GEO Group (US)	127
18	Booz Allen Hamilton (US)	150	Northrop Grumman (US)	120
19	General Electric (US)	147	Security Consultants Group (US)	110
20	Parsons Brinckerhoff (US)	146	Securitas AB (Swe)	108
Total for Top 20		7,983		5,130
Total for all industry		17,943		14,217

*Joint Venture of Northrop Grumman and Lockheed Martin.
 ** Now known as Kansas State University Institute for Commercialization (KSU-IC).
 *** Formerly known as Northrop Grumman Shipbuilding (NGSB).

Source: www.fpbs.gov, Bloomberg, CSIS analysis, DECISION.

Structurally, in 2006 the top 20 accounted for almost 45% of the total awarded contracts, but in 2011 its share dropped to 36% meaning the industrial base contracting with DHS is expanding and more contracts are awarded to small or medium-sized companies.

Aviation screening market

In the US, the procurement of airport screening devices is supervised by the Department of Homeland Security's (DHS) arm responsible for global aviation security in the US: the Transportation Security Administration (TSA). Currently, the two major programs dealing with airport security equipment are the Passenger Screening Program (PSP) and the Electronic Baggage Screening Program (EBSP):

- The *Passenger Screening Program* (PSP) serves as the TSA's Program Management Office responsible for the identification, procurement, deployment and sustainability of aviation checkpoint security equipment for federalized airports. It aims to prevent the entry of explosives, firearms, and other prohibited items on commercial aircraft, while ensuring freedom of movement for people and commerce, and consists of three security technology portfolios: people screening technologies, carry-on screening technologies and layered security technologies. Over the past few years, PSP has accomplished the replacement of legacy

systems with Advanced Imaging Technology (AIT) units and Advanced Technology (AT) X-ray systems, to expand use of Explosives Trace Detectors (ETD) and the deployment of emerging technologies such as Advanced Technology-2 (AT-2) X-ray systems, Bottled Liquids Scanners (BLS), Chemical Analysis Devices (CAD), and AIT with Automated Target Recognition (ATR);

- The *Electronic Baggage Screening Program* (EBSP)²² is responsible for ensuring 100% screening of checked baggage in the US using Explosive Detection System (EDS) equipment and Explosives Trace Detector (ETD) devices as the primary screening technologies. With \$700 million allocated in 2010 to accomplish its mission, the EBSP has been one of DHS's top 5 programs by value. EBSP is currently dependent on the DHS Science and Technology Directorate's Transportation Security Laboratory (TSL) for certification of the screening equipment and research and development of emerging screening technologies. As of the end of 2012, TSA had approximately 2,250 EDS and 4,800 ETD units deployed at airports nationwide. A large portion of the EDS and ETD fleet was deployed in 2002 and 2003 to meet the requirements of the Aviation and Transportation Security Act of 2001. As a result, many of these devices are reaching the end of their useful lives of approximately seven to ten years. FY 2012 and 2013 budgets are entirely dedicated to the procurement of EDS equipment. In FY 2012, EBSP was allocated \$697.3 million and shifted its planning and programming focus to make recapitalization a priority, looking first at operational performance. In FY 2013, EBSP's budget was set at \$571.4 million as it will be in a "mixed" acquisition life cycle, focusing predominately on the produce/deploy/support phase of the acquisition process.

²² Data referred to in this paragraph come from the "DHS Congressional Budget Justification report FY 2013". For the EDS, the estimates exist for "the end of 2011" (around 2,000 units deployed), to which have been added the units purchased in 2012 to have an assessment for the year 2012. The same has been done for ETD.

Main companies active in the area of airport screening equipment

Table 2.5 Major airport screening equipment companies

Company (Country)	Turnover			Nb of employees	Business description
	2010	2011	2012		
AS&E (US)	\$166m	\$279m	\$204m	415	100% of the production: X-ray equipment for airports and other locations.
Astrophysics Inc. (US)	-	-	-	-	Designer, developer and manufacturer of x-ray inspection equipment for baggage and cargo screening in security applications. The company buys primarily from US vendors and manufactures in the USA.
Control Screening (US)	-	-	-	-	Control Screening specializes in the design and manufacture of X-ray screening, metal and trace detection systems.
L-3 Security & Detection (US)	\$331m	\$332m	-	1,300 (est.)	Airport security systems, explosives detection systems and whole body imaging systems.
Morpho (F)	-	-	€1.4b	7,200	Morpho Detection division is the world leader of EDS for hold baggage. Morpho has 15 locations in the US through 4 subsidiaries: MorphoTrak (identification and biometric solutions), Morpho Detection (explosives and CBRN detection systems), Morpho Cards (Sim cards and other mobile secure business) and MorphoTrust USA (provider of identity solutions for driver license issuance, passports, etc.).
			€ 420m in the US (est.)	2,000 in the US	
Rapiscan (US)	\$252m	\$295m	\$392m	1,500 (est.)	Worldwide leader of security screening solutions used to inspect baggage, cargo, vehicles.
Reveal (US)	\$61.8m	-	-	125 (2010)	Reveal is an EDS specialist and was took over by SAIC in 2010.
Smiths Detection (UK)	£574m	£510m	£519m	2,300	A world-leading designer and manufacturer of sensors that detect and identify explosives, narcotics, weapons, chemical agents, biohazards, nuclear & radioactive material and contraband. North America accounts for 50% of the business. Alcoa (Tn) is home to manufacturing facilities of Smiths Detection for x-ray screening systems used for cargo inspection.
			£50 in the US (est.)	200 in Alcoa (Tn, USA)	

Source: annual reports, DECISION.

Alarms system market

According to IBISworld²³, the US security alarm service market achieved almost \$17 bn (€13 billion) of revenues in 2012 and comprises companies, which sell security systems like burglar or fire alarms and locking devices, but also install, repair or monitor electronic security alarm systems. An estimate of nearly 35 million locations (residential, commercial, and industrial) were monitored across the country in 2012.

Although the economic recession of the late 2000s negatively affected the security services industry in the US, integrated systems and access control were two of the fastest growing segments of the business along with video surveillance, whereas growth of traditional burglar and fire alarm systems was slow. This increasing demand was due to:

- The crime rates, which increased in the US when the economy started to fall into recession and law enforcement agencies experienced funding cuts, according to a 2009 Police Executive Research Forum (PERF) survey. The falling police capacity and the fear of crimes pushed the US population to ask for more security monitoring services from private companies;
- Sales of residential video equipment and remote control services which have boomed since the late 2000s, because of the technological changeover from analog video security systems to digital recorders. This technological breakthrough is expected to be one of the major future growth market drivers. Indeed, where in 2010, an estimated 18% of US households used professionally monitored security systems and generated about \$10 billion in service fees., by 2020, that figure is expected to rise to 30 percent of households. With the rising use of broadband services and Internet-connected devices (smartphones, digital tablets, etc.) digital systems will gain share as they offer enhanced flexibility and versatility, but also remote viewing and control of video data from one or more interfaces in different locations. They represent a lower total cost of ownership than a corresponding analog system, particularly as the system size grows and allow security firms to expand their relatively stagnant consumer base;
- Consequently, to better handle this rising volume data flow of IP cameras and systems, the demand for software that can more-effectively compress data is increasing. Therefore, video analytics is a fast-growing segment in the North American security software market and will soon account for a third of the market. The largest providers of software in the US market are Schneider Electric (Pelco), ISS, Tyco, Bosch and Honeywell.

Main companies active in the area of alarm systems

According to IBISworld²⁴, in 2012 the security alarm service industry employed around 120,000 people in the US and around 9,000 security companies were registered. In the early 2010s, following the trends of acquisitions by conglomerates, the security services industry became a microcosm of widespread globalization of markets:

- In 2010, the US-based Tyco, owner of the largest electronic security services company in the US, ADT Security Services, took over Broadview Security for around \$2 billion, creating a security giant that held almost one-third of the American residential security systems market. In 2012, the new entity provided electronic security monitoring services to about 7 million customers in business, consumer, and government markets in North America and Europe. Revenues for 2012 exceeded \$10.7 billion (half coming from business activities in North America) with 20,000 employees located in the US (out of 70,000 worldwide);
- UTC Security, a division of UTC, is another American company and industry leader. Some of its offerings included fire security services and products, electronic security systems, and security guards, and most of its customers were commercial or governmental. In March 2010, UTC announced the acquisition of its compatriot GE Security for \$1.8 billion. The firm reported 2011 revenues of almost \$6.5 billion;

²³ <http://www.ibisworld.com/industry/default.aspx?indid=1491>.

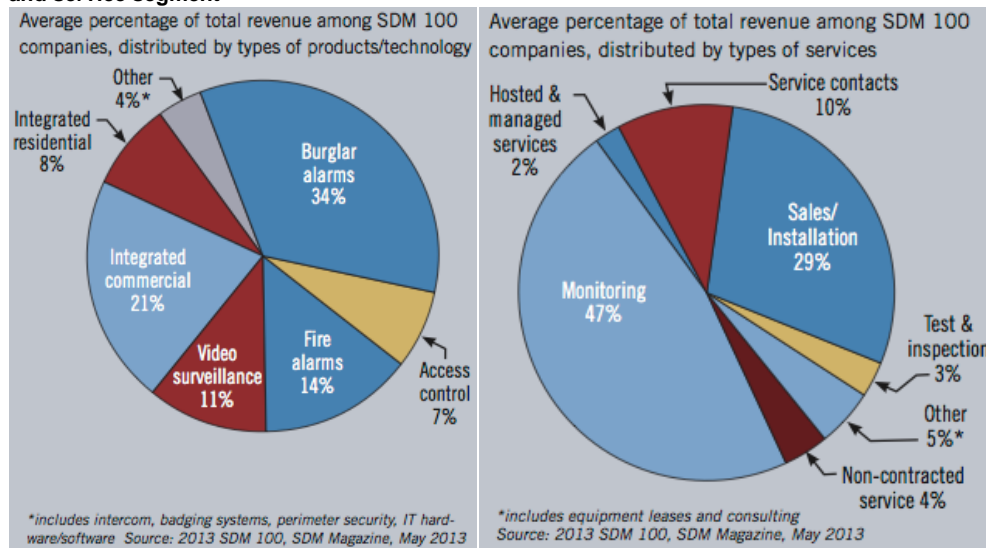
²⁴ <http://www.ibisworld.com/industry/default.aspx?indid=1491>.

- The third largest player is the American Honeywell, whose product portfolio includes security, fire & gas detection systems (access control, CCTV, fire sensors, etc.), infrastructure protection (airport, maritime, industrial, etc.), Integrated systems (plant and building emergency systems) but also protective equipment. In 2012, Honeywell's safety and security division reported \$8.1 billion revenues with around 10,400 employees in the US.

The alarm systems industry is driven not only by the constant introduction of novel technologies but also by legal aspects. Therefore, players of the security market can be represented by trade associations acting as lobby groups. For example, the Central Station Alarm Association (CSAA) is a trade association representing “providers, users, bureaus, and other agencies of Central Station²⁵ protection services that are certified by a CSAA-approved Nationally Recognized Testing Laboratory (NRTL), such as UL, FM and/or ETL”.

According to SDM 100²⁶, US-based security companies derive their revenue mainly from burglar alarms (cf. figure below) and in terms of business segment, their revenues come essentially from monitoring activities.

Figure 2.4 Alarm Systems Products and Services (US-based): composition of revenues by product type and service segment



As a consequence of the maturity of its market, the US security industry is highly concentrated. The increase in company size is being driven organically due to the introduction and adoption of enhanced services, such as remote video monitoring and Web-based home automation services.

²⁵ A central monitoring station (or central station) is a company that receives the alarm signal when the security device detects an alarm event.

²⁶ The SDM 100 magazine has been published since 1991. Its primary objective is to measure consumer dollars gained by US-based alarm companies, in order to present an account of the size of the market captured by the 100 largest security providers.

Table 2.6 Ranking by total annual revenue of the US-based security companies

Rank	2010	
	Company	Total Gross revenue (\$M)
1	Tyco Integrated Security + ADT	11,600
2	Honeywell Safety & Security	7,000 (est.)
3	UTC Fire & Security	6,100 (est.)
4	Diebold Security	3,000
5	Stanley Convergent Security	1,644
6	Vivint Inc.	399
7	Protection 1	376
8	Monitronics International	350
9	Slomins Inc.	291
10	Vector Security Inc.	234
11	G4S Technology LLC	157
12	Guardian Protection Services	150
13	ASG Security	119
14	Interface Security Systems	113
15	Bay Alarm Company	103
16	Guardian Alarm Company	79
17	Koorsen Fire & Security	79
18	Security Networks	79
19	AFA Protective Systems Inc.	74
20	Kastle Systems	68
Total for Top 20		21,083
Total for all industry		31,043

Source: SDM 100/DECISION.

SWOT analysis

The US market is the single largest security market worldwide. A SWOT analysis of US security industry therefore shows its access to this market as a key strength, due to the scale economies and large public and private consumption base. Many of the world's leading security equipment firms are US based, though in some technologies this is changing partly due to mergers and acquisitions.

Some segments, especially in security (monitoring) services, still suffer from lack of national harmonization of regulation. Budgetary pressures pose both opportunities and threats to industry. Private markets need to take over partly, which is possible in some segments (alarm systems), but not in others (airport screening).

From the EU side, the sheer size of the US market offers new opportunities in high-end segments, where access is likely to improve by demand pressures. New technological developments that drive demand growth in US markets to IP applications pose a threat, as leading producers are mostly located outside the EU.

Table 2.7a US Security Market SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Easy access to a large domestic market; • Historical reasons (high criminality rate, etc.) have made the US population aware of security issues; • Strong defence industry entailing economy of scales; • Unique and dedicated public agency (DHS) for the R&D, procurement, certification, etc. 	<ul style="list-style-type: none"> • Mature market with low growth perspective; • The DHS suffered from long-lasting criticism about the efficiency of its R&D policy: budgetary opacity, lack of strategy guidance and prioritization process, duplication and overlapping contracts, etc.
Opportunities	Threats
<ul style="list-style-type: none"> • The current low value of the US dollar reinforces the relative good competitiveness of the US industry by acting as a natural protection against the foreign competition on the domestic market but also by fostering exports; • Strong presence in the ITC industry; • Public fundings of R&D are planned to boom for FY 2014. 	<ul style="list-style-type: none"> • Harsh budgetary constraints on the US budget could lead to a preference of the maintenance of the defence-related industrial base to the detriment of the security one.

Table 2.7b USA Alarm Systems Industry SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Major leaders in safety and security (alarm systems) are US-based; • A large consumer base of more than 300 million inhabitants; • Shift towards private equity ownership; • Increasing demand in cloud-based solutions where the US have strong positions (IBM, etc.). 	<ul style="list-style-type: none"> • Lack of harmonization in the certification of central stations at the national level due to the fact that is mainly an insurance-driven business.
Opportunities	Threats
<ul style="list-style-type: none"> • Budget pressure on public law enforcement agencies could boost the private security equipment market; • Ageing population to monitor; • Inexpensive credit and strong equity investor appetite should lead new mergers & acquisitions and therefore consolidation. 	
Opportunities for the EU	Threats for the EU
<ul style="list-style-type: none"> • Need of high-end equipment and more complex softwares. 	<ul style="list-style-type: none"> • Smartphones and digital tablets are more and more taken into account for residential alarm systems: leaders are no more European.

Table 2.7c USA Airport Screening Equipment Industry SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Air Transport security has become a key priority of the US administration since the 9/11 events, which boosted both demand and supply to field the dense network of Federal airports; • The high-level qualification and certification procedures imposed by the US administration drives the airport screening equipment manufacturers to develop cutting-edge technology; • The costs of the qualification and certification procedures for airport screening equipment are totally free for industrials as they are entirely supported by the US administration; • A large number of manufacturers produce in the US. 	<ul style="list-style-type: none"> • A majority of American airport screening equipment manufacturers are too dependent on the US domestic market.
Opportunities	Threats
<ul style="list-style-type: none"> • S&T Directorate budget is planned to almost double for FY 2014. Consequently R&D spendings for explosive detection works should increase too, which should benefit to US airport screening equipment manufacturers. 	<ul style="list-style-type: none"> • Rapid changing technology; • The industry is highly dependent on the US administration rules.
Opportunities for the EU	Threats for the EU
<ul style="list-style-type: none"> • The US airport screening equipment industry still comprises relatively small companies that are specialized on niche segments. With a favourable \$/€ parity, European manufacturers could expand their business by acquiring US firms. 	<ul style="list-style-type: none"> • Due to rising costs, S&T could allow TSL to charge foreign, and therefore European, airport screening equipment manufacturers for certification of their products in the US.

2.3.2 Russia

Security context

Crime and terrorism statistics shows that internal security risks within Russia are quite substantial. For example, the 2012 Global Terrorism Index developed by the Institute for Peace and Economics ranked Russia as 9th most affected by terrorism country ahead of such countries as Israel, Colombia or Algeria that are often associated with high terrorism risk.²⁷ Commercial providers of terrorism risk analysis such as Maplecroft and AON also put Russia in a group of countries with a very high terrorism risk. In addition, although their visibility has declined compared to the 1990s, Russian organised crime groups remain active and are developing new methods to exploit opportunities created by technology (through cybercrime) and globalization (trade-related fraud).²⁸

In addition to a high level of terrorism and crime activity there are other factors that are likely to boost security demand in Russia. Some of them include:

- Russia has the second longest land border in the world (after China) of circa 20,000km.²⁹ Large parts of it that were created after the dissolution of the Soviet Union including its 6,800 km border with Kazakhstan are often poorly equipped and require major investment;

²⁷ <http://www.visionofhumanity.org/globalterrorismindex/#/2011/OVER/>.

²⁸ Europol, Russian Organised Crime Threat Assessment Report (ROCTA), 2008.

²⁹ http://en.wikipedia.org/wiki/List_of_countries_and_territories_by_land_borders.

- Russia has large stockpiles of WMD and radiological materials. They present potential target for terrorists and has to be reliably secured;
- The strong reliance on the domestic industrial base in the issues involving national security help to maintain a substantial level of demand reserved for domestic security providers.

The threat of terrorism became one of the top issues on the public policy agenda in Russia even before the terrorist attacks in the U.S. on September 11, 2001. The main catalyst was the First Chechnya War in 1994-1996. Two high-profile terrorist attacks during this war – in Budennovsk in June 1995 and Kizlaur in January 1996 – each involving massive hostage taking and casualties clearly demonstrated the dangers of terrorism. Vladimir Putin won his first presidential election in 2000 by making the fight against terrorism one of the central points in his program. Since then terrorism remained one of the main priorities for the Federal Government. The National Security Strategy of the Russian Federation to 2020 published in 2009 lists terrorism as one of the main threats to state and public security in Russia.

Unlike the United States which has the Department of Homeland Security Russia does not have a dominant public body responsible for most areas of internal security and safety. Similar responsibilities in Russia are allocated between various ministries and agencies. The largest among them is the Ministry of the Interior, which also includes the Internal Troops (a paramilitary gendarmerie-like force). In addition, the Ministry controls “Okhrana” – the largest provider of the manned guarding services and installer of alarm and access control systems in Russia³⁰; this state-owned company was created as a spin-off of one of MVD’s departments and its management is appointed by and reports to the MVD. The other public agencies in the field of domestic security, public order and safety include the Federal Security Service, Federal Protection Service, Drug Control Agency, Ministry for Emergency Management, etc.

General security market development

The demand side of the Russian security market can be divided into the following sectors based on the type of end-use customers:

1. Public sector security agencies, primarily the FSB and MVD;
2. Public and private organisations responsible for critical infrastructure;
3. Private sector and other public (non-security) authorities.

There is a significant contrast between the first and the third sectors. Public security agencies are technically sophisticated consumers that often demand unique equipment and have substantial in-house science and technology expertise supported by a number of R&D centres. Demand in some sub-markets of the security market such as border security, secure communication, CBRN security and counter-terror intelligence comes almost exclusively from this sector. The number of suppliers in these specialised sub-markets is limited and foreign equipment is often avoided. Most information on procurement by the security agencies is classified. The level of demand in this sector is determined by government expenditures on security. All these factors make this market sector quite close to the defence market in terms of its structural characteristics.

The third sector is quite different from the first one. It is comprised of a large number of private sector companies, public authorities as well as private persons. Demand from this sector primarily covers the physical security market and IT security. The main focus is on preventing and responding to ordinary crime and vandalism rather than terrorism. Although private companies are largest consumers of security equipment in this sector the public authorities still represent a substantial share of the total demand – around 30%. A very fragmented demand side of this sector corresponds to a fragmented supply side in the physical security market. Foreign competition is strong

³⁰ <http://fgup-okhrana.ru/about/default.htm>.

and in some sub-markets foreign companies dominate. Equipment offered to customers in this segment is mass-produced.³¹ Demand is driven by diverse factors such as general economic growth, investment in new construction and infrastructure, new regulatory requirements for safety and security.

Critical infrastructure protection takes a middle position between these two segments. Critical infrastructure is one of the main potential target for terrorist groups and its protection is one of the priorities for the government. Many infrastructure providers in Russia have been privatised (some airports) or set up as private companies from the beginning (i.e. mobile communication providers) but many remain under the state control. These include such large state-owned companies as Gazprom (natural gas transmission and distribution network), Transneft (oil pipelines), Rosatom (nuclear power plants), Russian Railways (railway tracks and stations), etc. A significant part of demand in critical infrastructure protection is for physical security equipment but typically with higher than the average performance and reliability characteristics. Infrastructure companies also procure more specialised and high-technology equipment, for example, explosive detectors in the aviation security.

Our estimate is that Russia's physical security market was worth approximately €1.56 billion (2.0 billion USD) in 2012.³² These estimates include installation and integration services but exclude manned guarding services. As a simple rule of thumb, the size of the Russian physical security market in the last 3-4 years can be very roughly estimated as 0.1% of Russia's nominal GDP for a particular year.

Table 2.8 Russian security equipment market size, in EUR million, all number are rounded

Security market segments	Value, 2012 (€ million)	Average annual growth rate	
		2007-2011	2012-2016
Physical security, <i>including:</i>	1,560	8%	5%
Alarm systems and perimeter protection	640	7%	4%
Video surveillance	610	10%	7%
Access control	310	8%	5%
Information (IT) security	710	18%	15%
Overall security market	2,270		

Source: HCSS estimates.

Before the financial crisis of 2008 the Russian security market was expanding rapidly with reported growth rates of 15-25% pa (measured in USD). This rapid growth was halted by the financial crisis of 2008-2009. The crisis forced the corporate sector to drastically reduce all investment expenditures including those on new security projects and equipment. At the same time the public sector expanded its security procurement and this helped to contain the fall. The drop in the market size was less than the decline in nominal GDP. The market recovered quickly in 2010-2011 but in 2012 its growth rate slowed down.

The public sector is the largest buyer of security and safety system. Some analysts estimate that it accounted for 28% of the security market in 2008. This share has increased since and is close to one third of the market. The demand from the public sector side is boosted by various programmes such as municipal "Safe City" programmes (with the main focus on video surveillance), the federal

³¹ The integration of security equipment into a single system is obviously customized for the needs of a particular customer but the underlying equipment is not produced for a specific client.

³² Russian as well as foreign sources typically provide the security market size in Russia in US dollars based on the average exchange rate for the year reported.

transportation security programme, the preparation for the Sochi Winter Olympic Games in 2014, and large public infrastructure projects.

Another important end user segment of the security market is critical infrastructure. Most of it is controlled by large state-owned companies, such as Gazprom (natural gas transmission and distribution network), Transneft (oil pipelines), Rosatom (nuclear power plants), Russian Railways (railway tracks and stations), etc. Security expenditures of these companies are often very substantial given the scale of their infrastructure. For example, Russian Railways spends annually circa 12 billion RUB (€300 million) to ensure security of passengers and protection of its infrastructure. In 2010 it procured 4.5 billion RUB (€110 million) worth of security equipment and systems. Rosatom itself is the largest provider of security systems in Russia (more information on this is given below). The Federal Government in some cases also directly supports security improvements at critical infrastructure facilities. In 2012, for example, it spent 1.8 billion RUB (€45 million) upgrading perimeter security at 12 airports.

Retail trade, banking, mining and energy companies are the largest business users of security equipment. In general the security market tends to be quite concentrated on the demand side: by one estimate 500 largest public and corporate customers account for 80% of all physical security market purchases. This is a reflection of a very concentrated structure of the Russian economy in general and a large role of government agencies in the market.

It should also be mentioned that IT security is large and rapidly expanding part of the security market. It is also quite distinct in terms of companies operating in this segment and technologies used. Therefore, it is typically covered separately from the physical security market. The increasing reliance of many physical security systems on IP networks and sophisticated software will mean that the distinction between physical and cyber security will become more and more blurred.

Geographically the main demand centres are in two largest Russian cities – Moscow and St. Petersburg. Some reports put their combined share of the market to 70% although others suggest that it is less than 50%. In any case these two cities are way above the rest in terms of their market size.

Situation of the security (equipment) industry

The supply side of the Russian security market reflects division of the demand side of the market into two broad segments: civil and private security markets that was described earlier although the boundaries between the segments is more blurred on the supply side.

The largest player in the Russian security market is the state nuclear corporation, Rosatom, whose main business includes all stages of the nuclear fuel cycle from uranium mining to operating nuclear power plants to generate electricity. It is also responsible for the Russian nuclear weapon complex, the fleet of nuclear ice breakers and other areas. Physical security is one of the areas where it possesses strong capabilities as well. Rosatom includes at least four enterprises working in the physical security sector and its own manned guarding services. The largest among these enterprises is SNPO Eleron created in 1963 as a research laboratory for the development of intrusion detection sensors and systems. It grew to become the largest provider and installer of perimeter protection and integrated security systems in Russia. It designs and installs security systems for military installations, state border, critical infrastructure, etc. Other Rosatom's security companies are smaller but the main focus of their activity is essentially the same. Their legal separation seems to be a product of history and geographical location rather than of business logic.

Russian defence companies are important players in the high-end civil security market especially in the areas where civil security capabilities are closely related to military capabilities. However, they tend to be very specialised (there is no Russian equivalent to broad-based defence-security conglomerates existing in the West if one excludes Rostec, which is more a restructuring agency rather a normal company) and supply equipment in specific areas such as small arms, secure communication, information security, infrared cameras, but there are no signs that they aim to become broad-based security suppliers.

Some small and medium-sized private companies, which are often spin-offs (formal and informal) of state-owned defence and security companies and research labs, also operate in this segment. One example of such company is Aspect, a spin-off from the Joint Institute for Nuclear Research in Dubna, develops and manufactures a range of radiation detection and monitoring equipment. U.S. National Research Council in its report noted that "U.S. experts were extremely impressed with the state of the art of the Russian equipment" produced by Aspect during its evaluation at Los Alamos National Laboratory.³³ Neutron Technologies, another spin-off from the same institute, develops drug and explosive detectors based on the tagged neutron technology.³⁴ A rare example of a Russian company that became successful internationally is Centre for Speech Technologies which is active in the area of speech biometrics. Companies in the civil security market tend to invest substantially more in R&D than their peers for the private security market.

The private security market segment is very fragmented. Revenues of the largest companies in the security market are close to about a half of Eleron's revenue. This suggests that their share of the total physical protection market does not exceed 3-5% (but it is higher for a specific technological segment such as video surveillance and access control systems). Many smaller companies focus only on specific regions and do not operate nation-wide. Almost all players in this segment are private companies and most of them were created after 1991.

There are several types of companies operating in this field:

- Producers;
- Distributors;
- Installers and system integrators.

Boundaries between these types of companies are becoming more fuzzy as some distributors move into system integration and sometimes start manufacturing their own equipment. Producers also often not only manufacture equipment but are ready to install and maintain it. Most of security equipment produced in Russia tends to be lagging behind best products from the OECD countries in terms of performance and quality. Its advantages often include lower prices and adaptation to specific Russian conditions (such as the ability to operate at low temperatures). Video surveillance and access control equipment produced in Russia is often based on imported components most often from China and South Korea. Their production does not involve much of R&D.

³³ National Research Council, U.S.-Russian Collaboration in Combating Radiological Terrorism, 124 pages, 2007, p.62.

³⁴ <http://ntech.jinr.ru/index.php?id=about> and <http://www.rusnano.com/about/press-centre/news/75462>.

Table 2.9 Some of the leading security system manufacturers in Russia

Name	Turnover/ operating profit, €million		Number of employees 2011	Description
	2010	2011		
SNPO Eleron (Rosatom) www.eleron.ru	101.5	111.2	3000	Designs and manufactures integrated security systems for important and sensitive facilities.
	5.1	6.3		
Kompania Bezopasnost www.bezopasnost.ru	32.3	45.9	n/a	One of the leading Russian producer and integrator of security systems. Its products include video surveillance and access control systems, cargo screening equipment, fibre optic perimeter intrusion detection systems, etc.
	3.1	3.7		
NVP Bolid bolid.ru	41.1	42.7	n/a	Manufacturer of burglar and fire alarms, access control and integrated security systems.
	13.8	13.3		
SPC Aspect www.aspect.dubna.ru	27.9	29.6	n/a	One of the leading Russian developers and manufacturers of professional radiometric, spectrometric and dosimetric equipment.
	7.6	9.6		
Centre for Speech Technologies speechpro.com	14.4	17.1	290	Audio processing and analysis systems, voice and facial biometrics, speech synthesis.
	n/a	n/a		
Byterg byterg.ru	11.0	15.0	200	One of the leading Russian manufacturers of video surveillance cameras under MVK brand.
	0.3	0.8		
OAO Dedal ³⁵ (Rosatom) www.dedal.ru	14.8	10.2	310	Designs and manufactures integrated security systems including intrusion detectors, perimeter protection, access control equipment, etc.
	1.8	1.4		
Smiths Heimann Rus http://www.smithsdetection.com	75*	n/a	100÷250	Russian subsidiary of world's leading manufacturer of screening and detection equipment.

* This number corresponds to sales in 2007. More recent figures for Smiths Heimann Rus are not available.

Source: SPARK database, companies' web sites, CNews.ru.

Aviation screening market

Russia has suffered from several terrorism accidents in the aviation sector in recent years. In 2004, Muslim suicide bombers managed to pass airport security at the largest Russian airport, Domodedovo, and then carried out the bombings of two passenger planes during their flight. In January 2011 a suicide bomber killed 37 people and injured 173 people in the arrivals hall of the same airport. This accident led to new tougher rules in aviation security.

The number of airports in Russia has been steadily declining mainly due to the closure of many small local airports where maintaining operations given small traffic volume became uneconomical³⁶. However, the number of international airports has increased and passenger traffic through major airports has been rapidly increasing - from 36 million passengers in 2000 to 106 million in 2011. Small local airports have a very limited financial capacity to procure modern

³⁵ <http://www.dedal.ru/index2.html>.

³⁶ Among all Russian airports only top 19 had traffic exceeding 1 million passengers per year in 2011. Data from the Russian Airport Association, http://www.airport.org.ru/08_02_news.html.

screening and detection equipment. As a result, many airports in Russia are lacking technical means for passenger and cargo screening. Russian official recently reported that 15% of the Russian airports do not have stationary metal detectors, 28% do not have x-ray scanners, and 73% do not have explosive trace detection devices.³⁷ The installed screening systems tend to be technically outdated.

Data on the size of the market for aviation screening equipment are not available but a reasonable estimate would be that the total market size for cargo and passenger screening equipment could be valued at just €9 million annually.³⁸ Security upgrades of airports in the preparation for the Sochi Olympics in 2014 and the FIFA World Cup in 2018 might significantly expand the aviation security market.³⁹

Most of equipment used for security screening at large Russian airports is produced by major global companies as Smith Detection, L-3, OSI (Rapiscan Systems).⁴⁰ The share of Russian companies on this market is small. They supply less sophisticated and lower quality equipment. Typically these companies specialise in industrial non-destructive testing or medical market and the aviation security market (as well as cargo scanning at border crossing points) is a secondary market for them.

Direct estimates of the Russian aviation security market were not available during this study. Some airports, however, reported their expenditures on security. For example, Domodedovo spent 10.6 million RUB (€260,000) on procurement of x-ray based screening equipment in 2012.⁴¹ The second largest Russian airport, Sheremetevo, spent 130.8 million RUB (€3.2 million) in 2011 on security investments, but this amount also included investment in physical security protection of the airport itself.⁴² As it was already noted, in 2012 the federal government spent approximately €3.75 million per airport improving perimeter security at 12 airports. If one assumes that security expenditures at international airports in Russia are on average equal to one quarter of Sheremetevo's security spending (i.e. €0.8 million) it translates into the total aviation security market of €55 million (including perimeter security).

A comparison with similar countries provides a useful check on that estimate. In Brazil, a country with a large territory and comparable to Russia level of GDP, the size of the aviation security market was estimated at 220 million USD in 2012 by Visiongain in its Aviation Security Market 2012-2022 report. Adjusting this number for the differences in air passenger traffic between the two countries (it is larger in Brazil) and converting the resulting value into euro gives the size of the Russian aviation security market as €99 million (using the value of the global market from the same report would produce significantly higher number). This is probably an overestimation. The International Transport Forum reported that overall investment in Russian airports was €470 million in 2010. It is unlikely that more than a fifth of total investment goes to security. Therefore, our rough estimate of the Russian aviation security market is approximately €50 million with the share passenger and baggage screening equipment of 40% or €20 million. Security upgrades of airports in the preparation for the Sochi Olympics in 2014 and the FIFA World Cup in 2018 might significantly expand the aviation security market in Russia.

³⁷ <http://www.transportsecurity.ru/svezhij-nomer/soderzhanie1/24-vozdushnyj-transport/121-sovershenstvovanie-zakonodatelstva-put-k-povysheniyu-bezopasnosti-i-zashchishchennosti-transportnogo-kompleksa>.

³⁸ See country report for the basis of this estimate.

³⁹ Indirect indicators provide a perhaps more optimistic assessment for the Russian market. In 2006 Smith Detection, a leading global company in aviation security, decided to open a production facility in St. Petersburg to improve its opportunities "to serve the fast-growing Russian security market." Other indicator of the interest to the Russian market is that Smith Detection and Rapiscan Systems maintain Russian language web sites.

⁴⁰ <http://www.aeromash.ru/en/o-kompanii/operational-activity>.

⁴¹ Investment Programme of the Domodedovo Airport for 2012.

⁴² Sheremetevo, Annual Report 2011, <http://www.svo.aero/investors/annualaccount/>.

Some leading companies seem to share this view. In 2006, Smith Detection, a leading global company in aviation security, decided to open a production facility in St. Petersburg to improve its opportunities “to serve the fast-growing Russian security market.”⁴³ Another indicator of the interest to the Russian market is that Smith Detection and Rapiscan Systems maintain a Russian language web sites.

Alarms system market

Alarm systems and perimeter protection

The market size for burglar and fire alarms and perimeter protection is estimated at circa €640 million (820 million USD) and it accounted for slightly more than 40% of the total physical security market. It is the largest segment of the Russian security market. However, it has been expanding slower than the video surveillance market and is likely to be overtaken by it in a near-term future. Construction activity has a large influence on the level of demand in this segment as new buildings are often equipped with alarm systems in particular with fire alarms. The regulation is another important factor.

There are important differences between the demand-side sectors in the alarm systems and perimeter protection segment. The corporate sector and in particular construction (i.e. the third sector in our classification) are mainly interested in low-end inexpensive products. The demand from the security agencies (and military) and from critical infrastructure operators is often for highly reliable, high-end systems. Russian manufacturers mainly dominate the market but foreign competition has been increasing across the whole range of quality spectrum, especially until 2008. Between 2001 and 2008 imports of alarm systems to Russia increased more than 5 fold. On the low-end side foreign competition come mainly from China and Ukraine, while suppliers of higher quality equipment are mainly from the EU and the USA.

Trade data indicate that imports of burglar and fire alarm systems in the last two decades significantly exceeded the value of Russian exports of such systems indicating that Russian production is not particularly competitive on the international markets. At the same time, imports have been very volatile. Two financial crises in Russia – in 1998 and in 2008 – both led to a very large drop in imports. The EU is the main supplier of alarm systems to Russia accounting for close to 70% of all imports (based on the EU reported data). Italy and Germany were the largest suppliers within the EU. Other main suppliers of alarm system to the Russian market were the U.S., Ukraine and China (in descending order). Russia exports such systems mainly to the countries of the former Soviet Union (especially Kazakhstan), India China, and Iran. The EU is also a significant export market for Russia.

Video surveillance

Video surveillance market has experienced the fastest growth rates in recent years compared to other security market segments. In 2012 it is likely to account for 39% of the physical security market with the total sales amounting to circa €610 million (780 million USD). The transport sector, oil and gas, and retail are largest end users of video surveillance in the private sector. In the public sector procurement by municipal authorities (“safe city” programmes) and law enforcement agencies seems to account the largest shares. Technologically, the Russian market has been experiencing a transition from analogue closed circuit television (CCTV) to Internet Protocol (IP) video surveillance systems. Wireless systems and cameras with the day-night functionality are also getting in popularity. However, the probably the most important trend is toward wider application of video analytics software (also known as video content analysis software).

⁴³ http://www.smithsdetection.com/1025_1076.php.

This market is very competitive and to a large extent is dominated by foreign suppliers, which account for 75-90% of the total market according to expert estimates.⁴⁴ There are a number of Russian video surveillance manufacturers but they rely almost exclusively on foreign components for the assembly of their systems and tend to produce cameras for the budget segment of the market. The main suppliers of video surveillance systems to Russia include the U.S., UK, Japan, Korea and China. Practically all leading brands are well represented on the Russian market. Among the most popular foreign suppliers are Sony, Panasonic, Samsung, Bosch, Aviglion, Axis Communication and other. Large Chinese companies such as Hikvision and Dahua are also increasing their efforts to capture a larger share of the Russian video surveillance market.

Most of Russian manufacturers rely on foreign components for the assembly of their systems and tend to produce cameras for the budget segment of the market. Leading Russian companies in this sub-market are Byterg,⁴⁵ ITV/Axxon⁴⁶ and Elvees.⁴⁷ ITV/Axxon seems to have the most ambitious international expansion plans among these companies and opened many international offices. All these companies put significant effort in developing their own video management and content analysis software as their main competitive advantage.

Access control system

Access control systems comprise various equipment used for authentication including card-based systems (proximity cards, smart cards, and others), biometric systems, keypad-based systems (including touch screens), and audio- and video-door contact systems. This segment is the smallest in the physical security market with the total sales of about €310 million (400 million USD) or 25% of the total market. The Russian market of access control systems is generally several years behind western countries in its technological development. High-end, large scale systems tend to be supplied by foreign companies. However, overall Russian companies have around 50% of the market.⁴⁸ Smart cards are gradually replacing proximity technology and in 2012 accounted for around 30% of sales. The use of biometric systems is limited and fingerprint authentication technology keeps a dominant position in the biometric market.

European companies are the market leaders in this segment. More specifically Bosch Security Systems, Siemens and HID Global (based in California but owned by Swedish Assa Abloy) take the leading positions in supplying high-quality access control systems to Russian clients.

SWOT analysis

Security industry does not function in a vacuum – typically, it shares strengths and weaknesses of the broader manufacturing sectors. There are some exceptions to this rule. One of the most visible examples was the Soviet Union: a country with unsophisticated civil industry was nevertheless able to create a relatively advanced and broad-based defence industry.⁴⁹ This was achieved through a massive public investment, including in R&D. However, even in this case the Soviet Union struggled to keep the pace in the arms race with the U.S. and was typically several years or more behind the U.S. industry in its technological development with an exception of some narrow segments.

Russian security industry is not an exception to this rule. One feature that it shares with the Russian manufacturing industry in general is its low labour productivity. Although the lack of data precludes a comprehensive analysis of this issue in the security industry but revenue per employee at the

⁴⁴ Finpro, Corporate Security & Safety Market in Russia, May 2010, p.21.

⁴⁵ <http://byterg.ru/>.

⁴⁶ <http://www.axxonsoft.com/>.

⁴⁷ <http://elvees-nt.com/>.

⁴⁸ Finpro, Corporate Security & Safety Market in Russia, May 2010, p.54.

⁴⁹ Software sector in India represents another such an example.

leading Russian security company, Eleron, stood at €37,300 in 2011 and was even less at Dedal. This is substantially less than at similar companies in the Western countries. Labour productivity also has not improved significantly over the last few years.

Small scale of the Russian security companies indicate that companies with potentially good technologies have struggled to grow and export (unlike some Chinese companies that have similar roots in a centrally planned economy). One of the problems preventing faster growth of Russian companies is a difficult business environment – Russia was ranked only at 112th place among all countries in the 2013 Ease of Doing Business Index developed by the World Bank. The 2012 Corruption Perception Index from Transparency International put Russia to the 133th place – the highest level of perceived corruption in Europe. Small size and narrow technological focus of many Russian security manufacturers makes their revenue stream more volatile and limit potential synergies between different areas of the security market, e.g. in R&D.

One (potential) strength that the Russian security sector can enjoy is Russia's expertise in software development and analytics. Software will play a bigger role in the future security systems. There are several Russian companies that try to capitalize on this strength in the video surveillance market by developing video analytics software such as ITV/Axxon, SpetsLab, and Elvees. The last firm recently received an investment from a state venture fund, Rusnano.⁵⁰

Relatively large and expanding Russian security market is one of the most important opportunities for the security sector as it provides a favourable environment for companies' growth. Russia's government's large investment in security R&D and procurement of the security systems are other important opportunities for security companies.

Overall, SWOT analysis for the Russian security industry is presented below. It applies to industry in general as well to its alarm systems segment. Many of its points can be used to describe the aviation security segment. However, in this area Russia suffers from a complete absence on the international markets.

⁵⁰ <http://elvees.ru/index.php?id=198>.

Table 2.10 Russia Security Industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Large pool of highly qualified technical personal; • Pockets of expertise and know-how in some areas (especially defence-related); • Strong skills in software development and analytics. 	<ul style="list-style-type: none"> • Companies are small scale and missing economies of scale and scope; • Corporate structure - leading player is a non-core unit of a large state corporation; • Weak international marketing /sales capabilities; • Low labour productivity.
Opportunities	Threats
<ul style="list-style-type: none"> • Good traditions of scientific and technical education and a large number of students in these areas; • Large and growing domestic market; • Large government investment in security&defence R&D; • Technology alliances and joint ventures with Western companies. 	<ul style="list-style-type: none"> • High level of perceived corruption in Russia; • Difficult business environment; • Volatility of energy prices in the future might negatively affect government public procurement and R&D in the security field.
Opportunities for the EU	Challenges for the EU
<ul style="list-style-type: none"> • Growing Russian market present attractive opportunities for EU security providers; • Forming JVs, alliances, partnerships or acquisition of Russian companies could provide access to technological advances in some security fields. 	<ul style="list-style-type: none"> • Russian security industry unlikely to present big challenges for the EU industry on the global market but might intensify competition on the domestic market.

2.3.3 Japan

Security context

Due to its aggressive colonial past, and also because East Asia has never experienced effective reconciliation after WWII, modern Japan has inherited several problems with its immediate neighbouring countries, that have never been solved and constantly hinder the development of positive and durable international relations in the area. These include sovereignty disputes with its 3 main neighbours (Russia – Kuril Islands; South Korea - Takeshima/Tokdo Islands; China - Senkaku/Daoyu Islands). It must also deal with the unpredictable behaviour of (maybe) nuclear armed North Korea, which has constantly shown an aggressive and provocative attitude. Furthermore, Japan's wealthy economy and its constant support to the US foreign policy places it on top of the target list for numerous terrorist organisation. Moreover, Japan's high dependence on external trade that must pass through sea lanes located in contested and/or pirate-infested areas make security of transport a critical concern.⁵¹

Japan has to deal with specific security concerns related to its geographical and demographic characteristics, of which the most important are:

- Numerous and sometimes highly destructive earthquakes and tsunamis, as well as destructive typhoons and associated problems of flooding;
- High population density in urban and suburban areas; its population is concentrated in only 30% of its territory;

⁵¹ These broader (external) security are reflected in the Japanese defence budget that is focused on (i) permanent threat situation from North Korea (setting a multi-layered ABM umbrella and constant monitoring of NK's suspicious activities); (ii) Ensuring the security of sea trade routes, and (iii) building an organized and complete response to large scale disasters, as well as patrolling, monitoring and protecting remote and uninhabited islands. Furthermore since FY2011 a supplementary budget has been allotted to comply with emergency new requirements, response to new issues (mainly from NK and China).

- Remote islands (uninhabited or sparsely populated) and a very large littoral/EEZ (Exclusive Economic Zone) area and heavily indented shoreline;
- An aging population, with many old persons living in remote and under-equipped locations that are difficult to reach;
- High risk industrial facilities located in close vicinity of urban areas.

Considering its situation and the evolution of the Japanese society, Japan has developed a number of dedicated responses to its specific security problems, especially focusing on:

- **“Border” surveillance and control**, including both maritime ports and airports, as well as airspace, coasts, remote islands and EEZ areas watch and protection;
- **Transportation security**, including train, aviation and maritime transportation (monitoring sea routes) and general protection (terrorism/guerrilla attack and large scale natural/industrial disasters);
- **Perimeter surveillance and protection of government related facilities and critical infrastructure** (including monitoring and management of contamination from Fukushima Daiichi Nuclear Power Plant);
- **MDW/NRBC⁵² monitoring, detection and response** (this also includes natural diseases such as new influenza);
- **Others:** Arms control, surveillance of populations or activists related to unfriendly countries, illegal immigration control, Cyber security⁵³, related R&D, etc.

General security market development

Although Japan security preoccupations differ substantially from those of the other countries, the Japanese security market has been showing a steady progression for many years and thus plays an important – and growing - role in the national economy. Estimates⁵⁴ for FY2008 estimated the total value of the security markets at \$12.3 billion (of which: security service companies above 55 %, manufacturers less than 40%, and installers less than 6%). In terms of market distribution, the main product categories are, in descending order: hardware (33%), surveillance (32%), access control (11%), home automation/security⁵⁵ (11%), central management software (9%) and alarms make-up (4%). This market distribution is believed to have proved relatively steady, although with a notable growing share for information security.

Overall, the Japanese (homeland) security market development is suffering from the same constraints as many others: budget reduction, due to aging population, feeble economic growth, reconstructing Northern economy, etc. Estimates from Visiongain (2012)⁵⁶ put the size of the Japanese (homeland) security market at around \$ 3.8 billion (€2.9 billion) in 2012, with annual growth expectations for the coming years in the range of 1 to 3 percent. However, the MLIT⁵⁷, which oversees railway companies, expects significant security improvements for mass transportation in the coming years, especially in emergency preparedness items such as bio-chemical material and explosive detection / containment systems.

⁵² Mass Destruction Weapons / Nuclear, Radiological, Biological and Chemical.

⁵³ The response to hacking attacks and the prevention of data fraud/theft are considered as a major issue in Japan.

⁵⁴ Asmag, May 20th, 2008: Operating in Japan's Security Market.

⁵⁵ This sector is evolving from home automation (seen as a must for new housing purchasers since the 2000's) to home automation/security, particularly due to the sharp increase of elderly and single person households since around 2005. The major manufacturers (Panasonic, Softbank Mobile, etc.) now propose dedicated integrated solutions where detected intrusion leads to alert procedures using any electronic means already in use in the house.

⁵⁶ Visiongain (2012): The Homeland Security Market 2012-2022.

⁵⁷ Ministry of Land, Infrastructure, Transport and Tourism.

Situation of the security (equipment) industry

The main product sectors and leading suppliers to the Japanese security markets are currently as follows:

- **Surveillance items** (mainly cameras systems): main suppliers (integrators) are Panasonic, Mitsubishi, Sony, Canon and CBC;
- **Access control/authentication** (smart cards and SC related equipment): Main providers are Sony Corporation, bitWallet, TUV SUD, for cards; Mitsubishi, Azbil, National, NEC, Amano and Art, for related equipment; SECOM, ALSOK, CSP and SENON as service providers;
- **Biometrics** (vascular, eye, fingerprint recognition and management systems): Main suppliers are NEC, Fujitsu, Hitachi and SHIMON;
- **Alarms** (for instance, intrusion alarms): Main providers are TAKEEX, Optex, Atsumi, Selco and ALEF.

IT security is also a key sector, which is monitored by the Japan Network Security Association.

Japan's security market is widely open to foreign initiatives, and many equipment providers from China, South Korea and the US are making their way. This relatively young market attracts every year many newcomers, offering new solutions with high technological added value to new needs. Japan's security market is also a comprehensive dedicated solution-oriented market, as customers generally tend to buy all in one solutions, and scarcely isolated components, so providers mainly focus on networked solutions, intelligence performance, component miniaturization and digital memory, more than striving to develop any new hardware. Consequently Japanese manufacturers tend to provide high-end global systems or sophisticated equipment, so there is room in Japan for smaller and less sophisticated component manufacturers, especially from China and South Korea, which are more and more active in this market. At the same time, this trend does not mean that Japan lacks component manufacturers and Japanese suppliers present especially in surveillance cameras (IP/megapixel cameras, along with mobile devices), memory support (e.g. smart cards⁵⁸) and dedicated software.

All integrators stress out that IP security is a promising field in Japan, as it represents more than 10% of the provided solutions, although its cost is still viewed as an impediment which should logically lower in the next future. The offer in IP security is thus dramatically growing every year.

Alarms system market

There is not much released about the alarm market and systems in Japan, except for some large-scaled systems that are currently in use nationwide, and which have been jointly developed for military and civilian security purposes.

Aviation screening market

Economic growth in the East Asian Pacific region has led to the development of infrastructure projects, including airport facilities, in order to cope with growing demand. The Japanese Aviation market, although quite developed, remains moderate, due to economic constraints and high airport charges, but facilities should be completely restructured in the next future, leading to a significant growth in security needs.

Within the MLIT⁵⁹, the Civil Aviation Bureau (CAB) is responsible for regulating security measures for air carriers and air operators, by establishing security standards, supervising the security measures based on these standards and by securing the budget for aviation security activities. The CAB also provides random inspections at local and national airports and provides dedicated

⁵⁸ Main smart cards manufacturers are Sony, BitWallet, TuVSud.

⁵⁹ Ministry of Land, Infrastructure, Transport and Tourism.

training for security personnel. After September 2001 events, the Japanese government raised the national security standards to the highest level immediately, and then developed new security standards in accordance with the international standards to require further enhanced measures for aviation security. Based on these enhanced security standards, installation of advance screening equipment such as new explosive detection systems have been introduced to address more elaborate methods of hijacking and terrorist acts. These countermeasures have inevitably increased the cost for aviation security, so the CAB has secured the budget of over 8 billion yen in the 2007 fiscal year for aviation security.

Estimates from Visiongain (2012)⁶⁰ put the size of the Japanese aviation security market at around \$ 560 million (€ 430 million) in 2012, with annual growth expectations for the coming decade of around 5% (CAGR).

Table 2.11a Japan Security Industry SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Very high GPI⁶¹ (ranking 5th in 2012) • High quality goods and innovative solutions in several advanced technology fields, meeting all international standards; • Leader in several technologically advanced industry sectors, namely electronic equipment; • Among the world top leaders in each high-tech sector which security solutions make use of: Japan hosts more 2/3 of world the electronic/biometric/soft integration and miniaturization companies; • Consequently, world 10th top leader in terms of R&D investment and 1st in terms of patent number (472,417 granted in 2012); • Supportive GVT policy in terms of R&D, especially in high technology projects (various large-scaled anti-terrorism projects led by Government bodies (mainly MoD and NRIPS) involving private companies); • Easy (partly online) certification procedures. 	<ul style="list-style-type: none"> • Aging society (about 23,30% of the population over 60), due to a very low birth renewal, etc.;⁶² • Numerous remote/sparsely inhabited areas, thus difficult to protect; • Numerous densely populated urban areas, easy targets for terrorist organizations; • Largely depending on the international situation (Japan has more or less an export-based economy) and on very (and constantly) difficult natural conditions (earthquakes, eruptions, tsunamis, typhoons, floods, mudslides, etc.);⁶³ • Continuing deflation, which somehow hinders R&D investment. • Weak experience in the international terrorism⁶⁴ management and strong dependency in U.S. terrorism experience and policy.

⁶⁰ Visiongain (2012): The Aviation Security Market 2012-2022.

⁶¹ GPI: Genuine Progress Indicator.

⁶² Depending on the point of view: This can also be considered as a strength regarding security matters, as it boosts, in a way, dedicated R&D, as Japan shows – currently – no intention to open more its borders to new immigrants and is thus committed to find technological solutions to the numerous problems inherent to the current situation.

⁶³ Japan rank 5th in NRI (natural risk index).

⁶⁴ Until the 2000s, Japan considered itself as a target only for Japanese terrorist groups, namely the former Japan Red Army (https://en.wikipedia.org/wiki/Japanese_Red_Army), active in the 70s and 80s, and the syncretic sect AUM Shinrikyô, which committed an attack in Tokyo Underground in 1995 (yet still active).

Opportunities	Threats and Risks
<ul style="list-style-type: none"> • Growing demand in advanced technology goods and systems; • Japan developing (and now exporting) high technology solutions for natural disaster affected countries; • Currency artificially maintained low (Abenomics policy), increasing the competitiveness of the Japanese goods and products in the global market, namely the security related ones. 	<ul style="list-style-type: none"> • Bank cross holdings risk; • Exceptional natural disaster, for instance the foreseen and coming great earthquake that should hit Tokyo area in a very next future; • Missile attack or similar threat from North Korea (although already under control by the U.S. Navy); • Possible armed conflict with China, due to the latter aggressive attitude against Japan regarding the Senkaku Islands issue; • Attack of Japanese assets and individuals in international terrorism related areas (outside Japan).

Table 2.11b Japan's airport screening sector SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Numerous, large scaled and highly busy airport infrastructures; • Currently no budget/public opinion special constraints for airport screening; • Strong public support and interest for innovative technologies, especially as regards airport security; • Strong support from the US Government; • High quality goods and innovative solutions in several advanced technology fields, meeting all international standards; • Leader in several technologically advanced industry sectors, namely electronic equipment. 	<ul style="list-style-type: none"> • Weak experience in international terrorism management (with a strong feeling that terrorism is first and foremost an external security issue); • Heavy reliance upon US security standards; • Due to the last decade economical bad results, some main airports suffer budget reduction.
Opportunities	Threats
<ul style="list-style-type: none"> • Top level technology platform, especially as regards biometrics and real-time information management; • High experience in integration of different technologies; • Strong support from the Government, which fully endorses the current US policy regarding airport security. 	<ul style="list-style-type: none"> • Exceptional natural disaster or external aggression that could lead to a highly critical situation; • Strong dependency on the US foreign security policy.
Opportunities for the EU	Challenges for the EU
<ul style="list-style-type: none"> • Government willingness to export in a next future locally developed and tested solutions; • Strong interest in any innovative technology, which can lead to fruitful co-operation and partnership. 	<ul style="list-style-type: none"> • Due to a highly restrictive legislation, non-disclosure of any defense related data or technology.

Table 2.11c Japan's electronic security (alarm) systems SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Top level technology platform, for what concerns (any kind of) sensors, signal management, information management and integration technology; • Long experience of large-scale natural disasters; • Strong support from the population both to innovative technology and solutions dedicated to natural risks; • Long experience of integrated and comprehensive systems. 	<ul style="list-style-type: none"> • Quite fragmented market; • Partially declining sector (namely detector and cam manufacturing); • Japan's main companies more oriented on global solutions; • Huge gap between Japan's regions towards innovative solutions.
Opportunities	Threats
<ul style="list-style-type: none"> • Increasing need and demand for video surveillance systems in urban areas; • Increasing need and demand for detection and alarm systems in remote and sparsely populated areas; • Increasing need for solutions that could be easily integrated in current comprehensive risk management and alarm systems. 	<ul style="list-style-type: none"> • Risk of declining interest of local companies for not so high value added business; • Harsh competition with foreign manufacturers, namely from China, Taiwan and South Korea.
Opportunities for the EU	Challenges for the EU
<ul style="list-style-type: none"> • Weak experience in private alarm systems; • Relatively feeble presence of Japanese companies in the sector of alarms. 	<ul style="list-style-type: none"> • Competition with other foreign manufacturers, already established or distributed in Japan.

2.3.4 South Korea

Security context

From a civilian security point of view the Republic of Korea (ROK) on the southern half of the Korean peninsula is a special case. Formally, the country is still at war with its northern neighbour and only an Armistice signed in the summer of 1953 prevents extended open hostilities. The only land border the ROK has is along the 38 parallel North, the demarcation line between North and South Korea delineated in the Armistice agreement. Reoccurring military incidents between North and South and the constant threat of renewed major hostilities dictates much of security thinking and practice in the south.

Albeit democratic and economic developments in the ROK have been phenomenal, rivalling all but the wealthiest countries in the world mirror, realities of war and the constant threat of renewed hostilities dictate much of security thinking and practice in the south. Border security, for one, is in large parts a military, not a civilian responsibility.

General security market development

The threat emanating from North Korea still dominates security thinking in the ROK also from a civilian perspective. A larger than normal part of internal (what may be called Homeland) security focuses on particular threats from North Korea. Espionage and sabotage are high on the national agenda. Coupled to these problems is terrorism which is also primarily related to the North Korea threat. Those terrorist acts that have been carried out in the ROK have with few exceptions been North Korean.⁶⁵ After the 1980's few acts of terrorism have taken place in the ROK. Vigilance on

⁶⁵ Wang, S.J., Choi, J.T., Arnold, J.L.: "Terrorism in South Korea", *Prehospital and Disaster Medicine*, Vol. 18, No.2, (2003).

the combined threats posed by espionage, sabotage and terrorism has however been incentives for ROK authorities to keep improving surveillance and personal control on borders and inside the country. In the post 9/11 era the ROK has therefore had relatively easy to conform to international standard in counter terrorism. A 2010 report on implementation of several UNSCR (Security Council Resolutions) makes it clear that the ROK demonstrates “excellent law enforcement and intelligence capabilities” to combat terrorism.⁶⁶ Such capabilities also include well working screening, alarm and access control systems in the real world as well as cyber and information security on a high level.

The focus on information security and more recently cyber security can in part be explained by the need to control propaganda from North Korea. This has been an issue as long as the conflict has been going on, but with an ever expanding array of information channels and platforms security needs have evolved. The ROK has since many years expanded its censorship against information from North Korea to the internet. Critics mean that recent measures amount to an expansion of internet censorship into politics, limiting freedom of speech rights.⁶⁷ The information censorship is but one part of the larger information and cyber security field which South Korea has taken very seriously. The demand in this area also in part explains the phenomenal expansion of South Korea's IT-industry. The March 2013 cyber-attacks targeting the ROK financial sector is the latest example of the real and serious cyber threat the ROK is suffering.⁶⁸

The rise to prominence of the overall industrial sector has meant an increase in demand for security products and services. Physical protection, access control, CCTV, information and cyber security are all needs within the high tech industry. The rise in income and personal wealth is likely to have driven demand in the alarm sector field.

To summarize; on a national level South Korea faces many of the same problems and civilian security needs of other countries. Being an integrated part of the developed world the ROK has at large conformed to international security standards in transport and communications as well as counter-terrorism and counter-proliferation. The rise of world leading companies and wealthy people has given rise to a wide array of corporate and private security needs in Korea.

The ROK also has a unique legacy coupled to North Korea. The conflict with the North has presented the ROK with unique challenges and threats. These have in the past and continue to be of particularly importance in driving security demand, not only on the military but also on civilian side. This legacy is also a key to understanding how the civilian security industry has developed (see Table 2.12 below). Three main drivers influencing civilian security can be distinguished:

1. The need to control movement of people into and out of Korea. Apart from the normal control of the movement of people which every country exercises, North Korean espionage, sabotage and terrorism have since long figure prominently as a primary security issue;
2. The need to neutralize North Korean propaganda and more recently information flow and cyber threats emanating from the North from across a number of possible information and communication technologies and platforms;
3. The need to have effective civil defence and emergency preparations for a range of conflict contingencies and war, especially in relation to the CBRN (chemical, biological, radiological and nuclear) threat South Korea is facing.

⁶⁶ *Country report on Terrorism 2009: Republic of Korea*, Office of the Coordinator for Counter Terrorism, August 5, (2010), URL: http://seoul.usembassy.gov/p_sr_080610a.html.

⁶⁷ “Korea Policing Internet. Twist? It's South Korea” *New York Times*, August 13, 2012, p. A1.

⁶⁸ “South Korea's “DarkSeoul” Attack Highlights Challenges for Cybersecurity”, U.S.News, March 29, 2013.

Situation of the security (equipment) industry

The security industry in the ROK traces its origins from two distinct industrial sectors: the defence industry and the IT industry. Civilian security in the ROK has evolved in a militarized setting defined by the North-South conflict. Since the industrialisation of its defence sector the ROK has evolved from being a country which is entirely dependent on foreign military technology to becoming a very advanced producer of military equipment. The defence and security industry continues to develop rapidly, not least as a result of the increase in domestic demand facilitated by the on-going conflict with North Korea, a dynamic defence reform and increased focus on improving civilian security in several sectors, such as aviation, maritime and crisis management. The threat of international terrorism has not directly affected South Korea, but regulations coupled to combating terror have been adopted by the ROK.

According to Visiongain the *Homeland Security* market was assessed to be worth € 1.41 billion in 2011 and € 1.47 billion EUR in 2012⁶⁹; this places the ROK in 15th place in terms of Homeland Security spending on an international ranking with a 0.9% global market share in 2012. In the terminology of Visiongain the Homeland Security market consists of several subsectors, all of them relating to public safety and security, which appears to correspond closely to civilian security demand of the ROK government covered under the concept of 'Homeland Defence', which excludes the private market demand for security related products, both hardware software and services. Visiongain predicts a compound annual growth rate (CAGR) of 4.0 % for the period 2012-2022 is predicted which makes the Korean market a fast growing one. Budget increase by government is reinforced by recent reports on the 2013 budget.

Within the ROK, the civilian security industry is referred to as *Knowledge Information Security*; the reason being that much of what is currently seen as being part of the civilian security industry emanated from various IT-sectors. A nation-wide survey from 2012 illustrates the prevailing distinctions and vocabulary used in the ROK. According to the "Survey for Knowledge Information Security Industry in Korea 2012"⁷⁰ conducted by the Korean Internet Security Agency (KISA), civil security industry is defined as "knowledge information security industry" which produces security technology embedded products such as code, surveillance as well as security technology based service against disaster and crimes.⁷¹

Within this broadly defined *Knowledge Information Security* sector one finds the following categories:⁷²

- **Information security industry** is categorized into network, systems, contents/information spill prevention, code/certification, security management, and others, where services include five areas such as security consulting, maintenance, security control, training/education, certification service;
- **Physical security industry** produces DVR, Camera, IP video device, engine/chipset, solution, peripheral device, access control, biometric, and alarm/monitoring. This category includes alarm system products. In the physical security sector service industry is a substantial part. Three

⁶⁹ *Homeland Security Market 2012-2022*, Visiongain.

⁷⁰ This survey was carried out in order to investigate the market size of domestic Knowledge Information Security Industry through a total inspection of 666 enterprises which consists of member companies of Korea Information Security Industry Association and other companies. Out of 666 companies, physical security related companies are 388 as of September 2012. (KISA, 2012).

⁷¹ Article 32, Information and Communications Technology Industry Promotion Act (Act no. 9708).

⁷² A further category of converged security may be added to this list. Converged security includes systems and equipment that incorporate both physical security measures and the IT technology-based information security. It is sometimes alternatively referred to as the security monitoring and control sector. Examples of the coverage of this 'industry' range from electricity infrastructure security (i.e. smart grid), pipeline security, transport security and even health care security.

broad categories of services are mobile security personnel⁷³, video security, others such as guard services.^{74,75}

According to KISA the overall security industry is one of the fast growing businesses in South Korea. In 2011 sales amounted to KRW 5,282 billion (€3.6 billion) and are estimated for 2012 at KRW 5,842 billion (€4.0 billion). Sales have been growing on average by 13.4% annually since 2009.⁷⁶ The *physical security industry* has witnessed rapid growth (9.2% between 2011 and 2012) as a result of government's reinforcement of regulation on security, increasing attention due to security incidents occurred in recent years⁷⁷, growing investment in security by government and companies and increasing export of physical security product/service. Moreover, KISA predicts that sales will continue to grow at average of over 14.3% to exceed KRW 10,300 billion (€7.0 billion) by 2016. Sales of physical security products/services are estimated at KRW 4177 billion (€2.9 billion) in 2012. The most important sub-segments being mobile security service⁷⁸ (27%) and camera sector (20%). In terms of growth, biometrics is growing fast (24.0% between 2011 and 2012) followed by alarm/monitoring products (19.0%), engine/chipset (18.8%), and IP image devices (18.6%). In service sector, other security service has grown significantly (25.0%) due to networking of physical security products and the development of new service area such as home security services.

Table 2.12 Sales and ratio of physical security items (KISA, 2012)

Items		2011		2012		Growth
		Sales	Share(%)	Sales	Share(%)	
		(€million)		(€million)		
Products	DVR	389	14,5	398	13,6	2.3
	Camera	562	21,0	592	20,2	5.2
	IP image device	109	4,1	130	4,4	18.6
	Engine/chipset	67	2,5	80	2,7	18.8
	Solution	123	4,6	133	4,6	8.9
	Peripherals	61	2,3	69	2,3	12.6
	Access control	169	6,3	187	6,4	10.8
	Biometrics	88	3,3	109	3,7	24.0
	Alarm/monitoring	114	4,3	136	4,6	19.0
	Others	75	2,8	83	2,8	10.3
	<i>Subtotal</i>	<i>1 756</i>	<i>65,6</i>	<i>1 914</i>	<i>65,5</i>	<i>9.0</i>
Services	Mobile security	720	26,9	793	27,1	10.2
	Video security	158	5,9	163	5,6	3.1
	Others	43	1,6	54	1,9	25.0
	<i>Subtotal</i>	<i>921</i>	<i>34,4</i>	<i>1010</i>	<i>34,5</i>	<i>9.7</i>
Total		2 677	100,0	2 924	100,0	9.2

Source: KISA (2012a).

⁷³ Mobile security service refers to "physical security deployment service," such as security patrols and emergency alarm response services.

⁷⁴ Convergence security industry is growing fast, however, its scope and range is changing, so this report doesn't include convergence security industry. KISA (2012).

⁷⁵ Security personnel services companies are as an example organized within its own industry association, the Korean Security Association, www.ksan.or.kr/eng/.

⁷⁶ Korea Internet Security Agency (2012a) *Survey for Knowledge Information Security Industry in Korea 2012*, p. vi, URL: http://kisis.kisa.or.kr/kor/notice/dataView.jsp?p_No=55&b_No=55&d_No=21&cgubun=&cPage=1&searchType=ALL&searchKeyword=.

⁷⁷ For instance, the distributed denial of service (DDoS) attacks launched in March 2011 against sites affiliated with the South Korean government, military, and civilian infrastructure.

⁷⁸ See footnote 4: Mobile security service refers to "physical security deployment service," such as security patrols and emergency alarm response services.

KISA estimates that exports account for over 20% of security industry sales, with over 30% of sales of physical security products going to export but only around 3% of information security products. By items, export sales of camera products and DVR products constitute the main export product categories. In terms of growth, biometrics and IP image device are growing fastest.

Table 2.13 Export value of physical security products and services

Items		2011		2012		Growth
		Value	Share(%)	Value	Share(%)	
		(€million)		(€million)		
Products	DVR	234	29,2	267	29,1	13,7
	Camera	302	37,7	342	37,3	13,2
	IP image device	57	7,1	69	7,5	22,2
	Engine/chipset	44	5,5	48	5,2	9,5
	Solution	42	5,2	47	5,1	10,7
	Peripherals	21	2,6	26	2,8	19,7
	Access control	46	5,7	55	6,0	18,2
	Biometrics	13	1,6	16	1,7	25,0
	Others	42	5,2	49	5,3	18,6
Total		802	100,0	918	100,0	14,6

Source: KISA (2012a).

More than half of export of information security products/service goes to Japan, whereas major destination of physical security export is the U.S and China.⁷⁹

Table 2.14 Major export destination of security industry in 2012

	Information security	Physical security
Japan	54,4	11,7
U.S.	8,1	10,9
Europe	22,1	26,0
China	1,6	24,8
Others	13,8	26,6
Total	100,0	100,0

Unit: share (%).

Source: KISA (2012a).

Evaluating the competitiveness of *Knowledge Information Security* companies compared to those in the most advanced countries, KISA (2012a) found that the information security industry has its competitiveness in brand and quality, while the physical security industry has competitiveness in quality and marketing. On a product basis, Korea Evaluation Institute of Industrial Technology (KEIT) concludes that Korean companies have comparative strengths in video surveillance and biometric, however, they are lacking some core technologies according to the survey KEIT conducted.⁸⁰ This report considers the U.S is on the top as 100% and assesses that Korea has 80% of capability compared to the U.S. The report presents an assessment that Korean companies have relative strength in smart phone based security service, network/systems in information security market. The physical security industry has been export-oriented so it has relatively more strengths than products/services of information security. For example, Korean security industry has the advantage in DVP products, finger print recognition system, CCTV camera, and video

⁷⁹ Authors could not find source that determine the ratio of contract and licence manufactured v.s. "indigenous" brand export. However, interviewees in Korea claim domestic companies are exporting "indigenous" Korean products to a substantial degree.

⁸⁰ KEIT (2012).

monitoring and control system. However, it assesses that convergent security industry is in the beginning step, where security issue is attracting more attention in several areas, such as smart grid, manufacturing process control system, vehicle communications, medical equipment software, and so on. It concludes that it takes more time to see new convergent security technologies.⁸¹

Table 2.15 International comparison of security technology level

	Technology level (%)	Time of gap (year)
South Korea	79,8	1.8
US	100,0	0,0
Japan	86,3	1.1
Europe	89,7	0.7
China	70,6	2.5

Source: KEIT (2012).

Main companies active in the security industry

According to a survey by a South Korean credit information institute, NICE, the top five security companies based on revenue in South Korea are:⁸²

1. Samsung Techwin (comprehensive security and defence industry);
4. S1 Corporation (security services provider);
5. ADT CAPS (security services provider);
6. KT Telecop (security services provider);
7. Hiltron (camera and direct video recording industry).

Samsung Techwin has by far the largest revenue. Since the company is active in many areas the civilian security (dominated by camera and digital video recording, (DVR) manufacturing amounts to about 25% of the revenue or 606 million EUR. Defence material amounts to 53% of sales. Export oriented, a total of 68% of revenues are generated by exports. Hiltron, the other manufacturer on the top five list, is also active in camera and DVR manufacturing. This further underlines the dominance of the camera and DVR segments of security industry. Hiltron is an extreme exports oriented company with over 90% of sales generated by exports.

The dominance of the camera and surveillance manufacturing industry in the security sector is further underlined when the *ASMAG Global Security Network Top 50* list of security companies in the world is consulted.⁸³ Eight ROK companies are on the top list, first among them Samsung Techwin. Oddly enough Hiltron is not on the list, indicating that there is significant difference in assessment and evaluation between the NICE survey and the ASMAG ratings. Never the less, out of the eight companies on the ASMAG list six are defined as manufacturers of *Video Surveillance*, one *Access Control* and Samsung Techwin as *Multiple*.

⁸¹ Ibid.

⁸² NICE Credit Information Service Co., Ltd provides a comprehensive credit information service. They provide "KIS-VALUE", financial and credit information to subscribers. www.kisvalue.com.

⁸³ URL: http://www.asmag.com/rankings/security50_rankings.aspx.

Table 2.16 Korean Security Companies on 2012 Top Security List

Top 50 rating 2012	Top 50 rating 2011	Company	Headquarters	Product Group	Total Revenue (EUR, Millions)		Revenue Growth 2010- 2011
					2011	2010	
8	6	SAMSUNG TECHWIN	Korea	Multiple	€ 382.2	€ 340.7	5.1%
17	14	CNB TECHNOLOGY		Video Surveillance	€ 80.9	€ 79.0	2.4%
19	17	IDIS	Korea	Video Surveillance	€ 79.9	€ 69.2	15.6%
38	49	HDPRO	Korea	Video Surveillance	€ 40.0	€ 21.8	83.7%
44	41	C-PRO ELECTRONICS	Korea	Video Surveillance	€ 29.0	€ 26.6	9.4%
45	35	ITX SECURITY	Korea	Video Surveillance	€ 28.7	€ 32.5	-11.7%
47	47	SUPREMA	Korea	Access Control	€ 27.7	€ 22.7	21.9%
49	50	WIN4NET	Korea	Video Surveillance	€ 23.5	€ 17.5	34.3%

Source: ASMA Global Security Network, http://www.asmag.com/rankings/security50_rankings.aspx (original numbers listed in USD. Author has translated to EUR with exchange rate EUR 1= USD 1.3118 as detailed in Annex 4).

The overall number of active Korean companies nationwide active in either *Information* or the *Physical security industry* is 666 in total. 67% of them are located in the Seoul area, 97.1% of them established in the form of incorporated company, and in terms of the capital status, 92.2% of them on domestic-funded, 90.8% of them as unlisted company, 57.4% of general type companies, 83.7% with their employees less than 100 persons, and 87.9% of them was those with less than 3.4 million EUR in revenue.⁸⁴

Aviation screening market

South Korea has greatly expanded its aviation industry and the leading airport Seoul's Incheon Airport is one of the busiest in the world. According to Visiongain it is ranked second for cargo and tenth for passenger traffic. The legacy focuses on control of people to minimize the risk of espionage, sabotage and terrorism has merged with new requirements in screening and safety. This means the overall focus on aviation security is strong and the market is large. Government policies have supported and encouraged expansion of the aviation industry. Incheon is meant to become a major hub for international travel by 2020 as outlined in a government plan the Air City 2020". Investment in new and old facilities is extensive. By 2016 a new terminal will be finished at Incheon, several airports are going through renovation and upgrade.

The focus on security means that South Korean air ports have been quick to adopt new technologies. Finger print and facial recognition technology was installed at several air ports in 2010. Full body scanning has been of strong interest. South Korea is likely to continue to stay in the frontline of technological development in airport safety and security systems. This is reflected in market size which is substantial. Visiongain assesses that the ROK has 2% of the aviation security

⁸⁴ Korea Internet Security Agency (2012a) *Survey for Knowledge Information Security Industry in Korea 2012*, p. vi, URL: http://kisis.kisa.or.kr/kor/notice/dataView.jsp?p_No=55&b_No=55&d_No=21&cgubun=&cPage=1&searchType=ALL&searchKeyword=.

market on the demand side. The market size in 2012 was 358 million EUR and predicted demand will be worth 625 million EUR in 2022.

As for airport screening demand, specific numbers have been more difficult to come by. All enquiries undertaken suggest that airport screening equipment is imported into Korea. There is no evidence of any domestic airport screening industry. When consulting the *Source Securities* list on X-ray and metal detection manufacturers in South Korea seven companies were found.⁸⁵ All of these are subsidiaries or branches of non-Korean companies, American, Chinese, Indian and UK firms. This state of things in the airport screening market is corroborated by the *U.S. Commercial Service* which states that “U.S. firms are the major suppliers of airport and port security equipment, which includes X-ray scanning systems, computerized tomography scanners, magnetometers, hand-held detectors and explosive trace detectors” to South Korea.⁸⁶

Alarms system market

Those industrial sectors that can be defined as alarm system industry are sorted under the *physical security industry* category in Korean statistics. Within this category the alarm systems is a separate subsection. However, this subsection seems to relate only to indoor alarm detection technology. Other subsections that could be included in a more broad definition of alarm systems are CCTV, peripheral alarm, biometrics and perhaps DVR. A detailed breakdown of the *physical security industry* is provided above (see 9). If a conservative definition is used (including only the subcategory alarm/monitoring) the value of the alarm system industry is quite small, only 114 million EUR annual sales in 2011. If, however all the industry categories in table 2.17 are defined as being alarm systems, the alarm system market is quite large. The total value of the alarm system industry in this case represents 51% of total industry revenue.

Judging from the data shown in Tables 2.17 and 2.18, the Alarm Systems industry in South Korea seems to be diverse and successful. There are few or no industry segments lacking and revenue within each sector is predicted to increase. Growth numbers differ. The saturated DVR and CCTV camera markets have lower revenue growth between 2011 and 12. All other areas grow quickly indicating competitiveness as well as R&D into new technologies for surveillance and alarm.

The broader alarm systems industry also seems healthy and competitive from an analysis on export shares to total revenue. A comparison between sales (Table 2.17) and export numbers (Table 2.18) reveals that both the DVR and Camera industries are strong in exports. By items, export sales of camera products was 302 million EUR in 2011 followed by DVR products with 234 million EUR, each industry exporting more than 50% of their products. Export shares of revenue are also high in the IP image transmission industry (basically routers that allow large volumes of CCTV video to be distributed over a TCP/IP protocol) 52%, and peripheral alarm 34%. Biometrics, an industry under rapid development has yet to expand exports shares which currently account for 15% of revenue.

⁸⁵ http://www.sourcesecurity.com/companies/search-results/company-search.html?order=&product_area=x-ray-and-metal-detection&country=korea-south&type=.

⁸⁶ Global Safety and Security Resource Guide 2013 – 2014, U.S. Commercial Service, 2013, p. 128.

Table 2.17 Sales and ratio of Physical Security Industry (KISA, 2012)

Items		2011		2012		Growth
		Sales in million EUR	Share (%)	Sales in EUR	Share (%)	
Products	Digital Video Recording (DVR)	389	14,5	398	13,6	2.3
	Cameras	562	21,0	592	20,2	5.2
	IP image transmission devices	109	4,1	130	4,4	18.6
	Engine/chipsets	67	2,5	80	2,7	18.8
	System integration	123	4,6	133	4,6	8.9
	Peripheral alarm	61	2,3	69	2,3	12.6
	Access control (card keys etc.)	169	6,3	187	6,4	10.8
	Biometrics	88	3,3	109	3,7	24.0
	Alarm/monitoring	114	4,3	136	4,6	19.0
	Others	75	2,8	83	2,8	10.3
	Subtotal	1 756	65,6	1914	65,5	9.0
Service	Mobile security	720	26,9	793	27,1	10.2
	Video security	158	5,9	163	5,6	3.1
	Others	43	1,6	54	1,9	25.0
	Subtotal	921	34,4	1010	34,5	9.7
Total		2 677	100.0	2924	100.0	9.2

Unit: million Euro / %.

Source: KISA (2012a).

Table 2.18 Export value of physical security products and service

Items		2011		2012		Growth
		Value	Share(%)	Value	Share(%)	
Products	Digital Video Recording (DVR)	234	29,2	267	29,1	13,7%
	Camera	302	37,7	342	37,3	13,2%
	IP image transmission device	57	7,1	69	7,5	22,2%
	Engine/chipset	44	5,5	48	5,2	9,5%
	System Integration	42	5,2	47	5,1	10,7%
	Peripheral alarms	21	2,6	26	2,8	19,7%
	Access control (card keys etc.)	46	5,7	55	6,0	18,2%
	Biometrics	13	1,6	16	1,7	25,0%
	Others	42	5,2	49	5,3	18,6%
Total		802	100.0	918	100.0	14,6%

Unit: million EUR/share of total exports %.

Source: KISA (2012a).

SWOT analysis

SWOT analysis for the Korean security industry shows the following key findings. Due to its focus on electronics and information security, the Korean industry is strong in video surveillance, web-based system security and biometric system. For other segments of physical and information security, the dominance and restrictions related to the role of the defence sector implies that development into new areas is somewhat hampered. The technology base and export position are generally weak. Increased priority of new security threats and stricter regulation provide opportunities for industry at the local market. However, Korean industry faces competition from other Asian countries in the low end, and lags behind the technology leaders in the high end of the market. Convergence of physical and information security hardware and software into

comprehensive systems of system products offers opportunities to further develop the strong segments referred to above. However, increased exposure of such integrated solutions to cyber terrorism comes as a related threat.

As described above, sales and export revenues are fairly strong and investment in R&D is constant. Technologically Korea lags a bit behind the most advanced countries, but not by far. The opportunities in big conglomerates such as Samsung to transfer technological developments from one business sector to another are clear. This is an advantage for security industry.

One problem that may face the Korean security industry is a leaning towards extreme specialisation. Many of the top companies identified in this study are CCTV or DVR providers only. Their R&D activities are likely to deal with further refining and or developing new technologies within the particular area of operations. Radically new technology is less likely to be developed in such an environment. Specialisation may also be a problem given that the trend globally and in the Korean market is towards system integration (or convergence as it is called in Korea) this may present a problem. This problem may be exacerbated by the culture of business rivalry that to some extent is a limiter on business collaboration in Korea. Korean businesses have a disadvantage in systems integration. This weakness seems to be a function of the lack of R&D into these sectors. Another potential problem is that there are industry sectors missing. There is no X-ray screening industry and in an era of further integrated and refined security, protection and alarm systems this is a weakness.

Some positive elements coupled to Korean R&D are possible to highlight. First, government support for the industry remains strong even when R&D budgets have not reached planned levels. The regulatory environment and increased public spending on security has in part compensated for lack of specific R&D investments. Companies have at large been able to uphold R&D investment levels. Specific R&D support for an industry, which to a very high degree is civilian in nature and to a certain degree dependent on developments in other civilian areas such as IT and cyber, may not be that effective. Regulations and initiatives to help industry cooperate and get better in coordinating R&D and system integration effectiveness may be a better option.

From the EU perspective, the Korean market offers opportunities in the high end products related to new security threats. Airport screening equipment is an example. Technology transfer in more traditional products, such as broader alarm and access control systems, provides an opportunity for collaboration with Korean industry. This may be beneficial to EU industry in case it can benefit from new elements in web-based security solutions developed in Korea.

A SWOT analysis⁸⁷ conducted by KEIT (Korean Institute of Industrial Technology) on Knowledge Information Security Industry is presented in Table 2.19a. This assessment represents the Korean view of the total security industry. As a comparison, a SWOT on the Alarm Systems industry is made by the authors and presented in Table 2.19b.

In this SWOT it is concluded that the security industry has strength in video surveillance, web-based system security and biometric systems; however, these markets are threatened by China and Taiwan. According to Korean assessments of their own industry there are technology gaps with the most developed countries, such as the U.S. and this gap does present a challenge. Core

⁸⁷ Korea Evaluation Institute of Industrial Technology (2012) *Industrial Convergent R&D Strategy for Information and Communication Industry*:
http://www.keit.re.kr/article.do?psStep=view&psPage=1&bbsCD=itep_data1_bor&shSearch=&shKeyword=&shCategoryC D=&shUserID=&gbn=04_32&Bidx=72261.

technologies for the next generation of security products/services are also lacking which presents overall industrial development with significant challenges.

One reflection is that IPR (Intellectual Property Rights) are assessed to be a weakness. But a UK report on South Korea assesses policy and legislation to counter IPR theft to be comprehensive.⁸⁸ The inclusion of IPR into the Korean SWOT as a weakness may therefore reflect the fact that South Korea has become a victim to IPR theft, owing to the high level of internet connectedness of Korean society. Weakness in this case is likely to reflect risk of theft from industry rather than IPR problems in general.

Table 2.19a South Korea Security Industry SWOT analysis

Strength	Weakness
<ul style="list-style-type: none"> • Online certification system (PKI); • A lot of experience in dealing with internet infringement cases; • Top technology in applied services such as Web security, VoIP security; • Video surveillance and biometrics; • Advanced IT industry and active IT-based convergence. 	<ul style="list-style-type: none"> • Weak IPR acquisition; • Lack of preceding research for next generation security technologies, such as big data, cloud, BYOD, etc.; • Lacking a good ecosystem where technology transfer/development/creating new market can be active; • Hardware based-video surveillance business and lacking developing software; • Inefficient R&D support due to lacking coordination among government agencies.
Opportunity	Threat
<ul style="list-style-type: none"> • Increasing demand for new security services such as big data, cloud service; • Public awareness of importance of security and strong support from the government; • More strict security regulations, hence, increasing demand and new security market created; • More demand for physical security products/services due to increasing concerns about public order and terrorism; • Public awareness of convergent security in the areas of Electricity, oil&gas, vehicles, remote treatment, etc. 	<ul style="list-style-type: none"> • Weakening global competitiveness due to lack of supplementary measures when security vulnerability occurs; • Bigger global IT companies appear through M&A, such as Intel & McAfee; • Low price market is threatened by China and Taiwan, while technology is behind advanced countries in high price market; • Increasing cyber-attacks /threats as active convergence with other industries based on IT.

Source: KEIT (2012).

With regard to the alarm systems sector – as opposed to the overall SWOT assessment for the security industry as a whole - this industrial sector is successful and competitive as shown by large domestic and export sales numbers. The technology level in this industry sector is also judged by several surveys used in this report to be high. The industry also has strong backing from the government. However the full amount of R&D investments planned since 2008 have not been made. What is not mentioned in the Korean SWOT is that Korean businesses have a culture of fierce competition. This is, as mentioned before, a limiter as joint ventures and cooperative business initiatives are harder to establish. Also the Korean SWOT does not specifically mention a saturated domestic market as a threat. Although recent free trade agreements are a clear opportunity for Korean companies in the Alarm sector, arguably more so than for European ones in

⁸⁸ *Intellectual Property Rights Primer for Korea: A Guide for UK Companies*, UK Trade & Investment, URL: <http://www.ipo.gov.uk/ipr-guide-korea.pdf>.

the saturated Korean market, this could also become a problem for Korean businesses when demand were to decrease internationally.

Table 2.19b South Korea Physical Security Industry (Alarm systems sectors) SWOT Analysis

Strength	Weakness
<ul style="list-style-type: none"> • High level of technology and specialization in the CCTV and DVR sectors; • Reliable home market as a foundation; • Spill over effects and use of technological R&D in the successful electronics industry within the same corporations/business groups; • Strong policy support from government level. 	<ul style="list-style-type: none"> • Hardware based-video surveillance business but software development lagging behind; • Inefficient R&D support due to lacking coordination among government agencies (reflecting a strong reliance on continued close state-industry cooperation); • A culture of harsh competition and non-cooperation between large corporations/business groups in Korea.
Opportunity	Threat
<ul style="list-style-type: none"> • Public awareness of importance of security and strong support from the government; • More strict security regulations, hence, increasing demand and new security market created; • More demand for physical security products due to increasing concerns about public order, cyber security and terrorism; • High level of technology and competitiveness in CCTV and DVR sectors make increase in exports highly possible; • Recent free trade agreements allowing for easier access to EU and US markets. 	<ul style="list-style-type: none"> • Saturated market in Korea; • Weakening global competitiveness due to lack of redundancies when security incidents such as cyber-attacks from North Korea occur; • Larger global IT companies appear through M&A, such as Intel & McAfee; • Market shares in the low price market is threatened by China and Taiwan, while technology levels in all but some areas are behind advanced countries in high price market; • Specialization could lead to decreased ability to refine products and services in a future comprehensive alarm system market; • New global financial downturn.

2.3.5 Israel

Security context

Israel faces continued terrorist threats from Hamas, the Popular Resistance Committees, and Palestinian Islamic Jihad, particularly from Gaza but also from the West Bank, and from Hizballah in Lebanon. Gaza-based Palestinian terrorist organisations continue rocket and mortar attacks into Israeli territory, and multiple terrorist attacks were launched along the Gaza security fence as well as the Israel-Egypt border. Gaza also remains a base of operations for several violent Islamist extremist splinter groups. Arms smuggling continues from Iran through Egypt into Gaza to Palestinian terrorist organisations.

Israel was hit by a record volume of rocket fire from Gaza in 2012. The rocket attacks demonstrated technological advancements, and Gaza militants for the first time used longer-range rockets to target major Israeli population centres in the greater Tel Aviv and Jerusalem areas. Israeli experts maintained that militants successfully smuggled long-range rockets from the Sinai Peninsula through tunnels into Gaza, and subsequently began producing rockets in Gaza. Gaza militants made significant quantitative and qualitative advances in capabilities in the last four years.

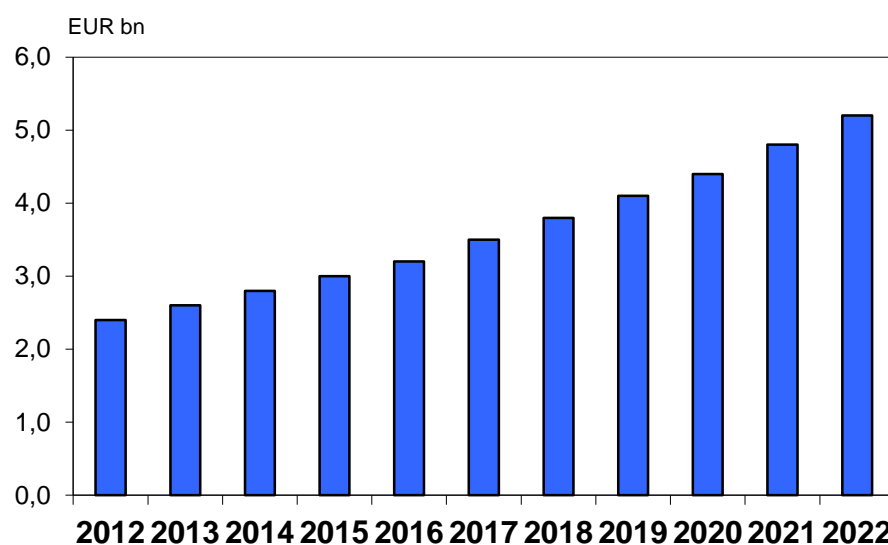
On the Northern border, Israeli security officials remain concerned about the terrorist threat posed to Israel from Hezbollah and its Iranian patron, arguing that Iran, primarily through the efforts of the Islamic Revolutionary Guard Corps-Qods Force, continued to transfer arms to Hezbollah in

Lebanon. Also, in light of the unrest in Syria, Israeli officials were concerned about proliferation of conventional and non-conventional weapons from Syria to terrorist organisations. Israeli politicians and security officials pointed to Hezbollah's efforts to rebuild and re-arm following the 2006 Lebanon War as evidence that the group remained a threat to Israel. According to the Government of Israel, Hezbollah has stockpiled 50,000 missiles in Lebanon, some of which are capable of striking anywhere in Israel, including population centres.

General security market development

VISIONGAIN indicates an annual revenue of Israel's homeland security industry of approximately EUR 2.4bn⁸⁹, the ICD RESEARCH of EUR 2.0bn⁹⁰. Both institutes estimate an export share of 25%. Different institutes forecast the annual sector market growth at 6 to 15%. In Figure 2.5 an annual average increase of 8% is assumed. Following⁹¹ the national market in total will grow from 2.4 to 5.1bn EUR between 2012 and 2022.

Figure 2.5 Annual average revenue of Israel's homeland security industry



Source of data: VISIONGAIN The Homeland Security Market 2012-2022, with own growth estimation for 2013-2021.

Situation of the security (equipment) industry

Homeland security (HLS) has always been a top priority in Israel, strongly connected with the military sector. The need for special technologies and self-reliance has led to a diversified, competitive industry, with products suitable for the most demanding situations and environments. With leading players in the computer sector, the vehicle protection segment and state-of-the-art solutions for airport and seaport security, Israel stands among the most experienced countries in the world.

Up to the nineteen-eighties the economy of Israel was characterised by state influence, because key enterprises (chemistry, construction, banks, communication, arms and security industry) were state owned. In the early nineties state enterprises were privatised and SMEs and innovation promoted. A lot of venture capital supported start-ups and created international success stories. Today Israel is seen as an industrialised country with a strong high technology and innovation sector and Israel has become very successful in the IT-, arms and security sector. Many high-tech products (especially in the security sector) have their source in the military sector. More broadly, technology is a key focal area in homeland security and Israel leads the world in start-ups per

⁸⁹ VISIONGAIN: The Homeland Security Market 2012-2022, Chapter 6.1, page 289.

⁹⁰ ICD RESEARCH: Homeland Security Expenditure in Israel to 2015: Market Brief.

⁹¹ VISIONGAIN: The Homeland Security Market 2012-2022, Chapter 6.1, page 289.

capita, has more venture capital money flowing in (especially from USA) than France, Germany, and the United Kingdom combined, all investing in Israel's technology. More than 100 American companies, including tech giants such as INTEL, IBM, MICROSOFT and GOOGLE have established major R&D facilities in Israel.

Today around 600 Israeli companies are active in the military and security sector, therefrom 350 in the security sector (including manufacturers of "dual-use" products and equipment) which export their products worldwide. Within the security sector Israel has very innovative SMEs and start-up companies, which are later frequently bought by foreign large companies. The two biggest firms active in the Israeli security market are Honeywell Security from USA and Bosch Security from Germany. Some Israel firms such as Magal Security Systems, Iomage and Elbit Systems are among the worldwide leading firms within the homeland security field.

The Israeli security industry can be divided in two groups:

- Big companies, all of them belonging to the state or under state influence, like IAI, ELBIT, RAFAEL, ELTA and TAAS (annual sales between 0.37 up to 2.6bn EUR and 3,500 to 16,500 employees) in year 2012 (see Table 2.20);
- SME's (enterprises with less than 500 employees), which are for a very small part subsidiaries of the big companies, and mainly private owned or owned by foreign firms (especially from USA).

The seven biggest companies of the Israeli security industry have export shares between 40 and 90%. The export shares of "small" SME's acting as R&D-Centre or innovation supplier of foreign co-operation partners are even higher.

Table 2.20 Ranking of Israeli producers of security systems & equipment by sales volume (2012)

Rank	Company	Sales EUR mn	Export Sales EUR mn	% total sales	Employees Number	Parent company / institution
1	Israel Aircraft Industries Ltd	2,606.7	2,039.2	78.2	16,548	State of Israel
2	Elbit Systems Ltd	2,137.4	1,608.1	75.2	12,545	Private
3	Rafael Advanced Defence Systems Ltd	1,501.1	883.1	58.8	7,258	State of Israel
4	Israel Aircraft Industries Elta Systems Ltd	759.0	669.4	88.2	4,000	Israel Aerospace Industries (State of Israel)
5	Taas - Israel Military Industries	367.7	144.0	39.2	3,497	State of Israel
6	Magal S3 Security Systems Ltd	67.2	59.6	88.6	279	BMI Capital (USA), Grace and White (USA) e
7	Star Defence Systems Ltd (SDS)	46.1	37.0	80.2	305	Star Night Technologies
8	Semi-Conductor Devices (SCD)	80.2	30.5	38.0	522	Elbit Systems + Rafael
9	PCB Technologies Ltd	73.9	10.1	13.7	682	Prioritech
10	Kinetics Ltd	73.6			295	Elbit Systems
11	Attenti	70.0			175	3M

Note: Exchange rate on April 25, 2013: 100 ILS (Israeli Shekel) (NIS = New Israeli Shekel) = 21,2 EUR.

Source: Dun & Bradstreet Israel Ltd, Tel Aviv.

In addition to larger and more established players, there exists a number of successful “start-up companies”, for example:

- Airport security:
 - TRACE TECH SECURITY LTD which is co-operating with RAPTOR (USA) and producing an alternative to body scan. Its product “Tech Trace” is an alternative to the body scanner and became an export-hit of the Israeli security industry. In USA it is implemented in at minimum 19 airports;
 - SUSPECT DETECTION SYSTEMS LTD (SDS), offering devices like a lie detector;
 - BELL SECURE (real time communication and alerts for travellers and cars);
 - WEB VR (smart camera systems);
 - ELTEL TECHNOLOGIES LTD (competency check of passengers through monitoring scans);
 - WECU TECHNOLOGIES LTD (technical support of psychological checks);
 - IDO SECURITY LTD (“Mag-shoe”, shoe scanner);
 - VIGILANT TECHNOLOGY (surveillance monitoring system);
 - BRIEFCAM LTD with offices in New York and Beijing (surveillance);
 - ACRO SECURITY (“pen” for identification of explosive materials).
- Smart surveillance systems:
 - MATE INTELLIGENT VIDEO (video surveillance);
 - ADAPTIVE IMAGING TECHNOLOGY (surveillance software, working with a grant from the US MINISTRY OF DEFENSE);
 - VIGILANT SYSTEMS (video surveillance);
 - BRIEFCAM LTD (video surveillance);
 - SEA-EYE UNDERCRATER TECHNOLOGY (video systems);
 - AGENT V (video analytics software security), 16th fastest growing company in Israel;
 - MAGAL SECURITY SYSTEMS with subsidiaries in USA and Canada and an office in China (annual turnover in 2011: EUR 68.1mn, number of employees in 2011: 279) (command and control systems, perimeter intrusion detection systems);
 - CAMERA-TECH LTD (special cameras for surveillance);
 - BYNET (mobile video surveillance system).

The main sectors of the Israel's security industry are:

- **Aviation, Maritime and Land Transportation Security.** Israel's expertise in this field includes active and passive protection for aircraft, surveillance, access control, virtual fences for perimeter security, and the protection of facilities and assets on land (airports, seaports, and transportation hubs). Israeli-made subsystems address specific threats, such as protecting aircraft from shoulder-launched missiles. Other elements focus on specific missions, from autonomous, unmanned surface vessels that secure sensitive maritime areas, to fixed and mobile satellite communication facilities that are operable on-board aircraft, trains and ships:
 - In the aviation field, security checks include a “suspect detection system” (SDS), an automated technology analysing responses of travellers to questions, by voice and hand. The security check at Ben-Gurion-Airport consists of preliminary checks at gates, inline checks, analysis of behaviour and scanning of passengers and their luggage. The company IDO developed a walk-on-scanner for the detection of devices in footwear. In 2011 Israel announced a new biometric passport;
 - In the field of maritime security, in addition to conventional military forces, unmanned maritime patrol vehicles stand are operation, developed by the Israeli company RAFAEL ADVANCED DEFENSE SYSTEMS.
- **Border Protection.** Israel's expertise in border security dates back to 1960, when its initial investments in border security, surveillance, route clearing and patrols were made. Israeli companies offer sophisticated electronic fencing and covert “virtual fences,” backed by video

motion detection capabilities, radar, and electro-optical-based surveillance sensors, and autonomous, unmanned aerial, ground and maritime patrol vehicles. Computerised information technology systems offer sophisticated tracking and screening of people, vehicles, and cargo, ensuring that open borders do not become a security risk. Around 17,000 illegal crossings take place per year over the border with Egypt alone. In 2011 Israel started the construction of a 250 km long fence on its border with Egypt, which includes 40 towers with ground surveillance radars. Among the suppliers are the companies ELBIT SYSTEMS and ELTA SYSTEMS, delivering surveillance systems, motion detection, floodlight and checkpoints;

- **Municipal Integrated Security Programs - "Safe Cities".** Video cameras and other elements of communication infrastructure that are already widely available throughout a modern city are becoming crucial tools for a new generation of information systems that empower law enforcement forces, first responders, and the emergency services, as well as official municipal authorities. Such systems, developed and deployed by several Israeli systems integrators, are deployed as part of "safe city" programs. These systems employ existing or dedicated command, control and communication networks, utilising digital maps and geographical information systems (GIS) to establish a clear picture of the situation and assist authorities in emergency response. Israel is a leader in developing best practices and novel technologies to protect its cities and towns from internal threats. Israel has developed a range of capabilities to ensure continuity of key commercial and civilian services in "worst case scenarios."
- **Infrastructure Protection.** This comprises perimeter protection, by physical obstacles (fences) and/or virtual obstacles (electro-optical, radar, seismic or magnetic sensors), triggering alarms when an intrusion is detected. Aerostat-based sensors and unmanned patrol units employing autonomous, unmanned vehicles can also be integrated into the system. A wide range of access controls, tampering sensors, and sophisticated cyber guards protecting communication links are also employed to extend this protection to cyberspace. Companies with an interest in Israel's protection its infrastructure have been involved in numerous projects including sensors, intrusion detection, image processing, surveillance, commodity protection, and many others. For example, 15 Israeli companies participated in a €154 million project for the Athens 2004 Olympic Games. Activities included venue protection, command and control rooms, maritime security, airports, urban security, crowd control, preparation of law-enforcement units, access control, communication and more. Israel has also constructed an additional operations room for the national electricity grid, and doubled the main operating centre of computer and communication networks as well as the water supply;
- **CBRN Protection.** Facing the threat of chemical, biological, radiological and nuclear (CBRN) attacks from hostile nations as well as from terrorist organisations, Israel has invested a major effort in the development and deployment of CBRN monitoring, defence, and countermeasures. Israeli systems provide collective NBC filtration for individuals, vehicles, shelters, and medical and mobile facilities (including tents and shelters). Radiological monitoring and detection systems are employed in detection portals, scanning containers, trucks, trains and other vehicles, in search of illegal radioactive sources. Much smaller sensors are also employed on miniature unmanned aerial vehicles (mini-UAV), which are used to monitor cargo vessels at sea. Handheld sensors are used as portable monitoring devices, supporting emergency response. Israel also maintains a Centre for Counter CBRN Terrorism;
- **Counter-Terrorism.** Anti-terror operations comprise many fields of activity, many of which are addressed by Israel's expertise. Israeli products developed for these applications include compact weapons, special ammunition, breaching and assault measures, non-lethal weapons, specialised weapons integrating sights and sensors that facilitate rapid and effective target acquisition, discrimination of targets under difficult visibility (targets hiding around a corner, or behind obstacles or walls), sophisticated remotely controlled or autonomous sensors that are capable of sensing movement, and transfer images or trigger alarms, etc. Special gear is

provided to protect operators and combat teams, including combat webbing, helmets, bullet-proof vests, transportable shields, armoured vehicles and more;

- **Emergency Management.** Israel's experience dealing with terrorism, commencing far before 9/11, is considered to be integral to its homeland security. Israeli security experts dedicated to emergency management even go as far as to train U.S. ground police personnel and first responder teams to be more effective safeguarding passengers at airports, thus preventing future terrorist attacks. Due to this humbling advantage, Israel attracts not only HLS companies, but companies from a broader range of sectors. To further expand their expertise, Israel facilitates several training missions within its borders, as well as externally, including several U.S. airports, police academies and other law enforcement agencies. Israel has developed a range of capabilities to ensure continuity of key commercial and civilian services in "worst case scenarios." For example, Israel has built a facility that enables the stock market to continue functioning in case of a protracted war;
- **Cyber Security.** Cyber security plays a large role in the HLS industry of Israel, which belongs to the world leaders in high-tech and cyber-security innovation. Israel sees 1,000 cyber-attacks every minute and targets have been - among others - the stock exchange, the airline and different banks. While many countries are beginning to realise the threat of a vulnerable cyber infrastructure, the Israelis are well ahead of the curve thanks to their ability to identify cyber security risks. In August 2012 a National Cyber Directorate was established to coordinate cyber-security development for Israel's military, security and industrial sector. Funding is anticipated at roughly €46 million with another €40 million to be provided by the private sector.

Through the years Israel's security has been founded on innovative technologies, operationally proven methodologies and highly trained and skilled human resources. The technologies essential to Israel's security have evolved over three generations, addressing a broad spectrum of threats. As a nation facing constant threats, particularly on its military, transportation and critical infrastructure, from hostile nations and terrorist organisations, Israel must maintain a high level of vigilance, credible defence and effective security to survive and prosper. Israel's security relies mostly on domestically developed, matured and tested capabilities.

The aforementioned characteristics provide the bedrock for Israel's competitiveness in the security field and are also driving Israel's security offerings in the international market, empowered by the know-how, products and skill development employed for the nation's defence. These solutions also rely on the extensive operational experience gathered here, in countering terror and preparing for emergencies. In the past Israeli companies have been strong in the fields of border and perimeter protection, information security and CBRNE detection and these fields continue to deliver sales volumes. In the future, unmanned systems will be added to current border and perimeter protection systems, driving more opportunities for Israeli expertise in this area.

Over 350 exporting companies, members of the ISRAEL'S EXPORT & INTERNATIONAL CO-OPERATION INSTITUTE (IEICI), are offering products for the Homeland Security market. Key technologies include:

- A wide range of **perimeter and border surveillance**, visible and invisible, as well as barriers used for border and perimeter protection and security solutions for critical infrastructure;
- Specialised devices are provided for the **inspection of vehicles and cargo**;
- Traditional counter terror and chemical, biological and emergency management and response (CBRNE) are also high on the Israeli exporters' agenda;
- Israeli Safe City and Smart City solutions address a wide range of capabilities, from **wide area surveillance** to **command and control** and **emergency response**. The associated programs based on integrating complex data-intensive processing for effective command and control of emergency response in dense urban areas are expected to rise;

- In the **cyber domain**, Israeli specialist providers offer telecommunication and network security, financial processing and data security, communications surveillance and a wide range of cyber security solutions;
- Other sectors include **intelligence and information processing** systems.

Israeli HLS capabilities include protection against explosive devices, electronic jammers used to counter remotely operated explosive devices, and ballistic or special armour, used to protect personnel, vehicles and buildings from explosions, fragments and blast. Other solutions include systems for law enforcement and riot control solutions, as well as non-lethal measures, emergency management and more.

Aviation screening market

Aviation security in Israel has a very high reputation. The last hijacking of an Israeli aircraft occurred on July 23, 1969 and no plane departing Ben-Gurion-Airport, just outside Tel Aviv, has ever been hijacked. It was in 1972 that terrorists from the Japanese Red Army launched an attack that led to the death of at least 24 people at Ben-Gurion-Airport. Since then, security at the airport relies on a number of fundamentals, including a heavy focus on the “human factor”, which may be generalised as “the inescapable fact that terrorist attacks are carried out by people who can be found and stopped by an effective security methodology.”⁹² In line with this focus on this so-called “human factor”, Israeli airport security measures emphasise the passenger and not their luggage. This does not imply, however, that automated systems are not part of security measures; for example, in 2012, Morpho Detection (Safran Group) announced that the Israeli Airports Authority (IAA) had selected its advanced technology “System of Systems” to help meet its stringent hold baggage screening requirements at Tel Aviv’s Ben Gurion International Airport. This followed a successful pilot test of the system integrated in the new baggage handling system.

Visiongain (2012)⁹³ expects that the Israeli aviation security market will grow from €177 million in 2012 to €485 million in 2022.

Alarms system market

The market for alarm systems and its development cannot be seriously calculated because of the strong relations between the security and the military sector (for example the barbed wire fencing with watchtowers and alarm systems on the border with Egypt or the construction of a concrete wall between the Gaza Strip and Israel).

SWOT analysis

The key insights from a SWOT analysis of the security industry in Israel are as follows. The industry has a strong focus on innovation and nurturing innovative start-ups. This reflects a strategic recognition that the international market has to provide a stable basis of demand, as well as opportunities for technological cooperation. This implies that SMEs also have an innovative and outward orientation. The current state of certification schemes is a weakness of the sector, as it leads to fragmentation of its markets.

Opportunities for the industry follow from the high priority of security, ensuring high and stable demand in the civil security market. The reliance on public demand, though, poses a challenge at the same time, mostly to be solved by serving export markets. The outward orientation in R&D offers opportunities for industry in widening its technological base, especially relevant for integrated security solutions. Too much focus on domestic suppliers by public authorities may potentially

⁹² SecuritySolutions.com, What can we learn from Ben-Gurion-Airport in Israel to help push aviation security in the U.S. to the next level? (http://securitysolutions.com/news/security_exposing_hostile_intent/).

⁹³ Visiongain (2012): The Aviation Security Market 2012-2022.

threaten the viability of industry, as it is shielded from international competition while it can only thrive when successful on foreign markets.

Focus on innovation and cooperation in R&D offers chances to EU industry if technology transfer can be realized. On the other hand, Israeli security firms are strong competitors on the EU market.

Table 2.21a Israel Security Market SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Permanent use and test of security equipment against neighbours; • Strong promotion of industrial investment and investment in R&D Centres in all sectors including security technologies in Israel; • Strong governmental support of research and development; numerous R&D programmes; • Israel follows a policy of a "start-up nation". Innovations are created in Israel but also overtaken from outside; • Compliance with commercial law including intellectual property rights; • Highest R&D expenditures in % of GDP compared with other OECD countries; • High innovation at SMEs as well bigger companies; • Israeli Government relies on local firms; • Detailed security policy and regulations; • Funding through state budget and financial aid from USA; • International integration (USA, EU-R&D, different Free Trade Agreements); • Sufficient venture capital. 	<ul style="list-style-type: none"> • Protectionism: Preference given to local companies; • Compared with other countries (Saudi-Arabia, Brazil etc.) small inland market; • Demand coming especially from general/regional/local government; • Difficult certification; • Bureaucracy; • High taxes; • Government instability.

Opportunities	Threats
<ul style="list-style-type: none"> • Strong demand in HLS caused by the political situation. Big interest of the Government in the best available security technologies; • Detailed security regulations; • Integration in the Research Framework Programmes of the EU; • Free Trade Agreements with North America (USA, Canada, Mexico) and most of Western European countries; • "Open policy" - simple realisation of contacts with other (foreign) companies and organisations; • Special support of the establishment of R&D centres in special zones of Israel by foreign companies; • Big interest in international co-operation and foreign markets because the inland market is too small; • Close co-operation with US firms of the security and computer sector increases the competitiveness of (rather small) Israeli security firms. 	<ul style="list-style-type: none"> • Strong competition: Approximately 350 local competitors among Israeli suppliers of security products within Israel; • Dependence from Government; • Fast innovation of local competitors; • Strong relation military forces – HLS; • Dependence from US-government, -policy and -financial support; • Inefficient government bureaucracy; • Inadequate supply of infrastructure.
Opportunities for EU Industries	Threats
<ul style="list-style-type: none"> • Co-operation in the R&D field, participation in Israeli innovations; • Good chances for M&A; • High governmental support for establishment of R&D centres; • Qualified workforce with lower salaries than in Europe; • "Open policy" of the Israeli business policy. 	<ul style="list-style-type: none"> • Very small inland market with - additionally - strong protectionism; • Unknown consequences for the much bigger Arab markets (for example Saudi Arabia belongs to the biggest markets of the world); • Big U.S. companies already cooperating with Israeli firms; • Missing co-operation in the military sector disturbs security business with Israel; • Political importance of USA is much bigger than of the EU because USA is guaranteeing the existence of the country Israel; • non-transparent certification process for the import of security products (responsibility: partly ISRAEL SECURITY AGENCY (ISA), partly ISRAELI POLICE); • Policy instability.

Table 2.21b Israeli airport screening industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Innovation solutions of Israeli enterprises strengthen the technology and marketing related co-operation with the USA in the airport security and screening sector; • After the Open-Sky-Agreement between EU and Israel from April 2013 increase of passengers and necessary airport expansion expectable; • Strong regulatory framework; • No budget constraints for airport screening; • Strong public support for R&D sector supports innovations in airport screening products. 	<ul style="list-style-type: none"> • Limited number of international airports; • Limited import demand (only X-Ray equipment at Ben-Gurion-Airport from company SIEMENS, other airport screening products from own production); • Israeli system for airport security emphasises the passenger and not the luggage.
Opportunities	Threats
<ul style="list-style-type: none"> • Strong co-operation in airport security and screening with USA; • Big worldwide demand; • Israeli products are competing the body-scanners and other airport screening products (note: High innovative Israeli products run/will be running under American brands); • Government relies on inland products; • Many international co-operation agreements. 	<ul style="list-style-type: none"> • Diminished threat (not predictable); • Economic recession reduces passenger flights (not predictable because of start of Low-Tariff-Airlines in Israel).
Opportunities for EU Industries	Threats
<ul style="list-style-type: none"> • Co-operation in the R&D-sector and marketing; • Growing number of passengers, but not of international airports in Israel; • In manufacturing qualified personnel for lower salaries than in Europe available; • R&D undertaken in Israel permits participation in the strong financial R&D related support of Israel's Government; • Limited production capacities within Israel. 	<ul style="list-style-type: none"> • Protectionism; • Reaction of Arab neighbouring states unknown; • Development of economy and therewith number of passengers; • Competition with USA in Israel's security oriented R&D sector; • Non-transparent certification process for the import of security products (responsibility: partly ISRAEL SECURITY AGENCY (ISA), partly ISRAELI POLICE).

Table 2.21c Israeli alarm systems industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Permanent use and checks of existing and new developed systems; • Successful innovations; • Strong governmental promotion of innovation in the field of alarm systems; • Local government relies on local technical solutions (for foreigners: protectionism); • Continuing threat; • Strong regulatory framework; • State budget increased by US Security Assistance. 	<ul style="list-style-type: none"> • Political situation in the region; • In the future possible budget constraints; • Strong relation with military forces; • Dependence of innovation level on the generosity of the R&D policy.
Opportunities	Threats
<ul style="list-style-type: none"> • Strong sales/export arguments based on own experiences; • Co-operation with the US industry active in the field of alarm systems. 	<ul style="list-style-type: none"> • Diminished threat; • Political constraints of the Government to reduce investment in alarm systems and to stop the extension of existing alarm systems.
Opportunities for EU Industries	Threats / Weaknesses
<ul style="list-style-type: none"> • Co-operation in the R&D. 	<ul style="list-style-type: none"> • Protectionism; • Non-transparency of the Israeli alarm systems market because of its close relation with military forces and defence policy; • Statistical data about the Israeli alarm systems market not published; • Uncertainties about the use of Israel alarm systems in other environments; • Competition with Israel-USA co-operation.

2.3.6 China

Security context

In the ongoing 12th Five Year Plan (2011-2015) of China (with 1.344bn inhabitants the most populous country of the world) strengthening of security is one of the main goals in order to improve (emergency) control, social public order control and civil-military integration. There are three security related demands which are direct consequences of the 12th Five Year Plan:

- The promotion of urbanisation. In China already more than 50% of the population lives in cities. This percentage shall increase. In 2020 in China more than 200 cities with more than 1mn inhabitants will exist;
- The extension of existing and the construction of new railway lines, subways, airports and ports become necessary and therewith the security related control of critical infrastructure;
- The improvement of information systems for cyber-security.

Growing urbanisation will need more public traffic (this means more critical infrastructure within the cities, subway etc.) and between the cities (regional transport). For the connection between the growing number of cities in the Western region with the big cities in the Eastern region and the internationalisation of all Chinese regions the aviation sector shall be extended. This means construction of new airports and increase of capacities of existing airports needing modern screening and other security equipment. At present 23 airports in West and Central China stand

under extension. The demand in security scanners will also increase in other transport fields (water transport, container transport etc.).

General security market development

At present China is the second biggest security market in the world, following the USA at no. 1. The market research institute VISIONGAIN (United Kingdom) estimates the China security market at EUR 24bn, the HSRC Homeland Security Research Corporation (USA) at EUR 28bn and the CSPIA (China Security and Protection Industry Association) (with 1,800 members of the Chinese security industry) at EUR 33bn (all data for 2012). It is expected that within 10 years the security market in China will reach or nearly reach the size of the US-market. The high growth rates concern especially the sectors airport screening and aviation security. During the next 10 years the market for aviation security in China will grow by 140% and of alarm systems by 200%.

50% of the total market is covered by video surveillance systems, an increase of more than 30% compared with 2010. In the ranking of market share, access control systems hold the second and alarm systems the third position.

Table 2.22a Total market for Homeland Security and Public Safety 2010-2020 (2012 and 2020 forecast) in EUR mn

	2010	2011	2012 forecast	2020 forecast
Critical infrastructure security	5,604	6,379	7,270	18,378
Aviation security	2,769	3,018	3,290	6,667
Maritime security	746	831	923	2,285
Mass transport security	992	1,121	1,267	3,368
Land border security	1,138	1,177	1,231	1,980
Safe Cities	10,153	12,185	14,378	31,260
Total	21,402	24,711	28,359	63,938
Index	100,00	115,46	132,51	298,75

Table 2.22b China Homeland Security and Public Safety Market for foreign based companies (2012 and 2020 forecast) in EUR mn

	2010	2011	2012	2020
Critical infrastructure security	2,522	2,807	3,126	6,432
Aviation security	1,800	1,931	2,073	3,672
Maritime security	448	490	535	1,143
Mass transport security	447	493	545	1,179
Land border security	569	577	591	792
Safe Cities	5,585	6,580	7,620	14,067
Total	11,371	12,878	14,490	27,285
Index	100,00	113,25	127,43	239,95

Market = products and services sales excluding post installation maintenance, upgrades and refurbishment.

Source: HSRC (China Homeland Security & Public Safety Market 2012-2020" published in October, 2012.

The main security related institutions of China

- Ministry of Public Security (MPS)

The MPS is the principal police and security authority of the mainland of the People's Republic of China and the government agency that is ultimately responsible for day-to-day law enforcement. It is headed by the Minister of Public Security. The Ministry operates the system of

many Public Security Bureaus which are broadly the equivalent of police forces or police stations in other countries;

- Public Security Bureaus (PSBs)

Most major Chinese cities will have a PSB assigned to deal with local security needs.

Additionally, all the provinces and special regions (excluding the Special Administrative Regions) have PSBs to deal with provincial security issues. As the main domestic security agency in the People's Republic of China, the MPS is the equivalent of the national police in other countries. It also controls and administers the People's Armed Police. Hong Kong and Macau have their own security bureaus/agencies and police forces;

- People's Armed Police (PAP)

The People's Armed Police (, officially Chinese People's Armed Police Force (CAPF), is a paramilitary force primarily responsible for civilian policing and fire rescue duties, as well as for providing support during wartime. The PAP is estimated to have a total strength of 1.5mn with over half of its strength (800,000) employed in its internal security units;

- The Ministry of State Security (MSS) of the Government of the People's Republic of China is the security agency of the People's Republic of China. It is also probably the Chinese government's largest and most active foreign intelligence agency, though it is also involved in domestic security matters.

Situation of the security (equipment) industry

In the production of security products and equipment, approximately 20.000 (twenty thousand) enterprises are active, mainly SME's⁹⁴, producing on a lower level alarm systems, airport screening devices for the control of passengers and luggage, video surveillance systems, access control systems etc.

At present China's security industry cannot cover all sectors of security products and has a very limited number of available product types of low to mid technological level. It is also surprising that following the estimations of CSPIA the current export of security products is very low. Among the factors influencing imports of security products into the Chinese market are:

- the barriers for market entrance of foreign products in the field of security and protection are very low;
- the interest in mid to high technology is very high;
- certification and/or approvals are necessary for:
 - burglar alarm / detector intruder systems;
 - safe cabinet (box)
 - security alarm systems for cars,
 - airport screening equipment.

⁹⁴ Face-to-face interviews with CHINA SECURITY AND PROTECTION INDUSTRY ASSOCIATION (CSPIA) on 25 June, 2013 and later.

Table 2.23 Importers of security products and equipment

China National Electronic Import & Export Corporation (CEIEC)	CEIEC established 1980, is a trade enterprise with import and export of electronic technology and products including security products as well as other services. The company has 56 subsidiaries (home and abroad), 5 offices abroad and more than 200 joint ventures. Since 1992, CEIEC has been ranked among the top ten of the 500 largest Chinese importers and exporters for consecutively several years. By the end of 2011, CEIEC's total assets and sales revenue have respectively reached RMB 21.2bn and RMB 25.1bn. The company imports command and control systems, radar, communications, electro-optic systems, electronic warfare systems, security and counter-terrorism systems (perimeter security system, special operations system, city security and emergency response system, communication surveillance system, checkpoint security system), unmanned aerial vehicles and logistics support facilities.
China North Industries Corporation (NORINCO)	NORINCO is an enterprise group engaged in both products and capital operation, integrated with R&D, manufacturing, marketing and services. NORINCO mainly deals with: defence products (precision strike systems, amphibious assault weapons and equipment, long range suppression weapon systems, anti-aircraft & anti-missile systems, information & night vision products, high-effect destruction systems, anti-terrorism and anti-riot products, small arms, military supplies), petroleum & mineral resources exploitation, international engineering contracting, opto-electronic products, civilian explosives & chemical products and sports arms & equipment.

Table 2.24/part 1 Ranking of greatest China producers in the field of security following the turnover 2012

Ranking	Company	Info	Turnover EUR mn (2012)	Number of Employees (end 2012)	Products
1	HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO. LTD.	Web: http://hikvision.en.hisupplier.com	907,3	appr. 8,000 (end 2012)	<ul style="list-style-type: none"> • CCTV, DVR, cameras, DVS; • compression abroad.
2	CHINA SECURITY AND SURVEILLANCE TECHNOLOGY INC.	Web: www.csst.com	573,9	3,500	<ul style="list-style-type: none"> • IP Surveillance, CCTV; • Intrusion detection; • Intercoms; • Infrared IP cameras; • Video Door Phone Kits; • Digital and intelligent video analysis; • Access control.
3	ZHEJIANG DAHUA TECHNOLOGY CO., LTD.	Web: http://www.dahuasecurity.com Reg. capital: RMB 66,8mn, EUR 8.20mn Total capital (2012): RMB 3,397mn, EUR 416.61mn Date of establishment: March 12, 2001	444,4	2,731	<ul style="list-style-type: none"> • NVR; • DVR; • Special DVR; • Network and PTZ cameras; • Analog cameras; • HD-SDI camera; • Compression card; • Traffic surveillance.
4	SHENZHEN SECURITY GROUP CO. LTD.	Web: http://en.chinesessg.com	appr. 400,0	appr. 6,000	<ul style="list-style-type: none"> • CMS Central Monitoring Stations; • Alarm + DVR systems; • 3G and IP cameras; • Video call systems; • 3G Intelligent Video Intercom; • CCTV systems.
5	NUCTECH COMPANY LIMITED	Web: http://www.nuctech.com/en Reg. capital: RMB 165mn, EUR 20.24mn Total capital (2012): RMB 4,110mn, EUR 0,504mn Date of establishment: December 19, 2000	299,6	appr. 1,500	<ul style="list-style-type: none"> • X-ray inspection system; • Relocatable container/vehicle inspection system.

Source: Face-to-face interviews with CHINA SECURITY AND PROTECTION INDUSTRY ASSOCIATION (CSPIA) on 25 June, 2013 and later. Austrian Embassy in Beijing, Commercial Department: Information.

Table 2.24/part 2 Ranking of greatest China producers in the field of security following the turnover 2012

Ranking	Company	Info	Turnover EUR mn (2012)	Number of Employees (end 2012)	Products
6	GULF SECURITY TECHNOLOGY CO. LTD.	17F, 2# Building, BOYA International Centre, No.1, Lizezhongyi Road, Chaoyang District, 100102 Beijing, China Web: http://gst.com.cn/default.asp	70,0	appr. 500	<ul style="list-style-type: none"> • Fire network and alarm systems; • Intelligent fire alarm systems; • Intelligent control panels; • Video entry systems.
7	SHANGHAI EASTIMAGE EQUIPMENT CO., LTD.	Web: http://www.en.eastimage.com/cn Reg. capital: RMB 35.2mn, EUR 4.32mn Total capital (2011): RMB 260mn, EUR 31.89mn Date of establishment: February 20, 2003	60,8	appr. 200	<ul style="list-style-type: none"> • Luggage detection: X-ray inspection equipment, Liquid inspection, Explosive detecting, Narcotics detecting; • Body inspection: Metal detectors, Metal radiation probe, Handheld metal detector; • Vehicle detection and inspection; • Auxiliary products.
8	BEIJING ZHONGDUN ANMIN ANALYSIS TECHNOLOGY CO., LTD.	Web: http://www.fiscan.cn/framework_en Reg. capital: RMB 90mn, EUR 11.04mn Total capital (2011): RMB 380mn, EUR 46.60mn Date of establishment: February 27, 2004	41,5 (2011)	318	<ul style="list-style-type: none"> • Baggage x-ray inspection system; • Metal detection; • Large container/vehicle inspection system; • Body scanner x-ray inspection; • Liquid security inspection system; • Backscatter x-ray security inspection; • mini-van.

Source: Face-to-face interviews with CHINA SECURITY AND PROTECTION INDUSTRY ASSOCIATION (CSPIA) on 25 June, 2013 and later. Austrian Embassy in Beijing, Commercial Department: Information.

Table 2.25 Foreign investors in the field of electronics and security

EADS Defence & Security China	<p>The EADS Group and its joint ventures currently have more than 1,100 employees in China and the company and its divisions are present in multiple locations across China:</p> <ul style="list-style-type: none"> • A partner-ship between EADS daughter firm CASSIDIAN and Chinese companies (CETC and CASIC) started to provide integrated public safety and HLS solutions that guaranteed the security for the 2008 Beijing Olympic Games; • CASSIDIAN has deployed the TETRA radio systems in airports all over the country and won in 2010 the contract from the Guangzhou government for a TETRA network to ensure security at the 16th Asian Games in 2010. It also co-signed a contract to provide the Shenzhen Public Security Bureau with a TETRA radio system that offered secure communication services during the 26th World University Games in 2011; • ASTRIUM is actively pursuing co-operation with China in the space sector. In 1997, ASTRIUM and CASC set up a joint venture, EURAS-SPACE, which constitutes a link between both major industry players. In 2003, ASTRIUM signed a major contract with CAST for the setting up in Beijing of the world largest Compensated Compact Test Range (CCR120/100). Through ASTRIUM Geo-information Services, ASTRIUM is also extremely active in the Earth Observation domain. BEIJING SPOT IMAGES (BSI) is the joint venture founded in 1998 between SPOT IMAGE and CEODE, an affiliate organisation of the CHINESE ACADEMY OF SCIENCES; • EUROCOPTER CHINA is a 100% subsidiary of EADS. EUROCOPTER is China's No. 1 helicopter partner (more than 150 helicopters sold including armed helicopters) and is believed to have a share of almost 50% of the market share in China.
Shanghai Sikorsky Aircraft Company Ltd.	<p>SHANGHAI SIKORSKY AIRCRAFT COMPANY LTD. is a joint venture between SIKORSKY AIRCRAFT CORPORATION and SHANGHAI LITTLE EAGLE SCIENCE AND TECHNOLOGY CO., LTD. Since their business license approval in March of 2003, a new helicopter company was established in China. SHANGHAI SIKORSKY is the exclusive manufacturer and sales agent for the product line of light helicopters. SIKORSKY is a subsidiary of UNITED TECHNOLOGIES CORPORATION, which provides a broad range of high-technology products and support services to the aerospace and building systems industries including security police and public safety agencies helicopters.</p>
Bosch Security Systems	<p>BOSCH set up its first sales office in China as early as 1909. In 1926, the first Bosch car service was opened in Shanghai. Today, all three BOSCH business sectors are present in China: Automotive Technology, Industrial Technology, and Consumer Goods and Building Technology. BOSCH employs 30,200 persons at 51 legal entities across China, and has a holding company in Shanghai. Consolidated sales in China reached 42.3 billion yuan in 2011. In the area of security, BOSCH produces video surveillance, voice alarm, intrusion alarm, access systems and other security products in China. Since 2011, BOSCH has participated in the extension of the Xian Xianyang International Airport through the delivery of surveillance systems and other security products.</p>
GE Security Asia (China)	<p>GE SECURITY ASIA (CHINA) is a Shanghai based distribution company of security products. GE Security was a division of GENERAL ELECTRIC INC'S GE ENTERPRISE SOLUTIONS and was acquired by UTC UNITED TECHNOLOGIES CORP. on March 1, 2010 and is now part of UTC FIRE & SECURITY, a global provider in fire fighting safety and security solutions. GE SECURITY ASIA (CHINA) main Homeland Security products are: CCTV surveillance systems, IP surveillance, Access control and Perimeter intrusion detection.</p>

Honeywell Security Group	HONEYWELL has a long history in China that goes back to 1935 when it established the first franchise in Shanghai. HONEYWELL was among the first multinationals to set up a representative office in Beijing, where they began a series of high-quality investments. Today, all of HONEYWELL's four Strategic Business Groups are represented in China, and all of them have relocated their Asia Pacific headquarters to China. Over the years, HONEYWELL has set up subsidiaries and joint ventures in over 20 cities across the country. As of 2012, HONEYWELL has invested USD 600mn in China and employs over 11,000 people. HONEYWELL SECURITY GROUP offers intrusion, access control, video surveillance products and systems, control panels, keypads, expansion modules and accessories, wireless products, alarm communications, sensors, life safety products, structured wiring, cabling products and kits. The company also offers commercial and public safety security services using Internet video, alarm net and structure wiring systems.
Siemens Building Technology (China)	SIEMENS became active in China in 1872. Over the years, the company became an integral part of the Chinese economy. In fiscal year 2011 (October 1, 2010 - September 30, 2011), the sales of SIEMENS in China amounted to EUR 6.39bn and new orders totalled EUR 6.24bn. SIEMENS currently has about 29,000 employees in China, making it one of the largest foreign-invested employers in the country. SIEMENS offers the following Homeland Security products: CCTV surveillance systems, Port security systems and Airport security systems.
IBM China	IBM's first equipment in China was utilised by Beijing Union Hospital in 1934, IBM's presence in China has a long history. IBM China grew dramatically during the past eight years. It operates two research centres and several software labs across the country. IBM China's main Homeland Security & Public Safety Product Lines concern smart and safe cities information technology.
Panasonic China	PANASONIC is present in China through PANASONIC CHINA. It has three R&D companies (Panasonic R&D Centre China Co., Ltd., Panasonic R&D Centre Suzhou Co., Ltd., and Panasonic Software Development Centre Dalian Co., Ltd.). PANASONIC CHINA also has 20 manufacturing companies operating in China. PANASONIC's main products in Homeland Security are CCTV surveillance systems, Video displays, CCTV cameras and Perimeter security OEM products.

The role of SME's in the Chinese Security Industry

Privately owned SMEs are become more and more important in the Chinese security product industry. The following examples for different product groups provide an indication of the creation, export orientation and innovation power of Chinese SMEs supplying security equipment products:

X-ray detection and related products:

- CHANGZHOU MINKING ELECTRONICS CO., LTD is a manufacturer of speed dome cameras, infrared systems, CCTV systems and x-ray devices. The company was established in 2001 and exports worldwide including Europe and North America. There are over 300 employees including 50 persons active in R&D. Around 55% of the production are exported;
- SHANGHAI DASHING SCAN TECHNOLOGY CO., LTD produces human body scanners, which display bombs or drugs imbedded in the human body. It displays metal, non-metal, knives, guns and liquid substances carried by or concealed in the human body. The company is a manufacturer with own R&D department. Additionally the company produces container and truck as care systems and a scanning x-ray imaging detector;
- SHANGHAI RAYS ELECTRONICS SCIENCE & TECHNOLOGY CO., LTD is specialised in research, manufacture and sale of x-ray security devices. The company was established in 2010;

- SUNELL TECHNOLOGY CORPORATION founded in 2002 is producing surveillance cameras, software and x-ray devices.

CCTV and related products:

- ZHEJIANG DALI TECHNOLOGY CO., LTD, producing human body temperature measurement, infrared thermal imaging cameras etc. The company was established in 1984 and transformed from ZHEJIANG TESTING TECHNO-LOGY INSTITUTE to DALI;
- SAE ELECTRONIC CO., LTD is a leading CCTV products manufacturer and designer in China. The products are sold to more than 60 countries and used in city surveillance, transportation, retail, education and government.

Access control:

- SHANGHAI HUAYUAN ELECTRONIC CO., LTD is a manufacturer of proximity cards and RFID tag laminate. Established in 1994 it is one of the biggest Chinese suppliers for access control cards and printing cards in China. It is also manufacturing IC and ID cards;
- SHENZHEN YETONG TECHNOLOGY CO., LTD manufactures access control systems. It was established in 2006 and has more than 200 employees, therefrom 10% in the R&D department. It is a high-tech enterprise for fingerprint systems;
- ACCESS CONTROL CHINA CO., LTD was established in 2005 and has more than 200 employees. It is a manufacturer of access control systems, RFID readers and tags and CCTV equipment.

Biometrics:

- MIAXIS BIOMETRICS CO., LTD. This company was invested by INTEL (USA) and other investors. It is China's leading biometrics company specialised in biometrics products R&D, manufacturing and distribution. The products range from fingerprint care products to fingerprint access control. Fingerprint technology is offered since 1996. The company is active in banking security, government and military area. In China's financial sector MIAXIS has a market share of more than 60%. Export is made worldwide;
- HANWANG TECHNOLOGY CO., LTD, founded in 1993, is a specialist for development and delivery of software to be used in handwriting.

Airport screening market

The Chinese market for airport screening is characterised by the extension of existing airports and the construction of new airports (see previous chapters). A large market can be expected for passenger, luggage and cargo screening. A forecast is only available for aviation security in total (including airport screening).

The China aviation security market in EUR mn in the period 2010-2020 is forecasted by HSRC as shown in Table 2.26.

Table 2.26 Development of the China aviation security market 2010-2020 in EUR mn (2012-2020 forecast)

	2010	2011	2012	2020
Foreign companies	1,800	1,931	2,073	3,672
Domestic companies	969	1,087	1,217	2,995
Total	2,769	3,018	3,290	6,667

Market = products and services sales excluding post installation maintenance, upgrades and refurbishment.

Following the suggestions of HSRC⁹⁵ the market share of foreign companies will develop from 65% in 2010 to 55% in 2020 but in respect to the growth of the total market the sales of foreign companies is expected to grow by more than 104% between 2010 and 2020, this means more than doubling.

Main Producers of Airport Screening Equipment

Table 2.27 prepared by the CHINA SECURITY AND PROTECTION INDUSTRY ASSOCIATION (CSPIA) presents producers of airport screening equipment for the control of passengers and luggage.

Table 2.27 Ranking of China's main producers of airport screening equipment

Ranking	Company	Turnover 2012 (EUR mn)
1	NUCTECH COMPANY LIMITED	299.6
2	SHANGHAI EASTIMAGE EQUIPMENT CO., LTD.	60.8
3	BEIJING ZHONGDUN ANMIN ANALYSIS TECHNOLOGY CO., LTD.	41.5 (2011)
4	SHENZHEN XINYUANTONG ELECTRONICS CO., LTD.	15.1

Firm	NUCTECH COMPANY LIMITED
Website	http://www.nuctech.com/en/
Turnover	EUR 299.6mn (2012) EUR 222.8mn (2011) EUR 232.8mn (2010)
Infos	Registered capital: EUR 20.8mn Date of establishment: 19-12-2000 Total capital: EUR 517.2mn (2012) Number of employees: approximately 1,500 Certificates approved: <ul style="list-style-type: none"> • ISO9001 Quality Management System Certification; • ISO14001 Environment Management System Certification; • OHSAS18001 Career Health & Safety System Certification; • Security Engineering Enterprise First Level Certification; • Radiation Safety Certification authorized Environmental Organization.

Firm	SHANGHAI EASTIMAGE EQUIPMENT CO., LTD.
Website	http://en.eastimage.com.cn/
Turnover	EUR 60.8mn (2012) EUR 12.8mn (2011) EUR 26.6mn (2010)
Infos	Registered capital: EUR 4.4mn Date of establishment: 20-02-2003 Total capital: EUR 32.7mn (2011) Number of employees: approximately 200 Certificates approved: <ul style="list-style-type: none"> • ISO9001 Quality Management System Certification; • ISO14001 Environment Management System Certification; • Occupational Health and Safety GB/T28001:2001.

⁹⁵ Homeland Security Research Corporation (HSRC) (USA): "China Homeland Security & Public Safety Market 2012-2020" published in October, 2012.

Firm	BEIJING ZHONGDUN ANMIN ANALYSIS TECHNOLOGY CO., LTD.
Website	http://www.fiscan.cn/FrameWork_En
Turnover	EUR 41.5mn (2011)
Infos	<p>Registered capital: EUR 11.3mn</p> <p>Date of establishment: 27-02-2004</p> <p>Total capital: EUR 47.8mn (2011)</p> <p>Number of employees: 318</p> <p>Certificates approved:</p> <ul style="list-style-type: none"> • ISO 9001 Quality Management System Certification; • ISO14001 Environment Management System Certification; • Occupational Health and Safety Management System Certification.

Firm	SHENZHEN XINYUANTONG ELECTRONICS CO., LTD.
Website	http://en.xinyuantong.com/
Turnover	EUR 15.1mn (2012)
Infos	<p>Registered capital: EUR 4.0mn</p> <p>Date of establishment: 07-2000</p> <p>Total capital: EUR 25.2mn (2012)</p> <p>Number of employees: approximately 300</p> <p>Certificates approved:</p> <ul style="list-style-type: none"> • ISO 9001 Quality Management System Certification; • ISO14001 Environment Management System Certification; • Occupational Health and Safety Management System Certification.

Alarms system market

Within the Alarm Systems Market some typical segments can be distinguished:

- Alarm systems for critical infrastructure
Critical infrastructure includes governmental and private infrastructure, like energy, IT-communication, drinking water, the food sector, public facilities and transport. As shown in Chapter 1 following the 12th Five Year Plan the Chinese infrastructure will strongly grow. The infrastructure investments are a key to the economy and will cause a lot of security demands;
- Alarm systems and other security systems for maritime security
The China maritime security market includes many components of security: command, control and communication of the seaport (IT hard- and software), container explosives screening and other checks, port perimeter protection systems, screening of passengers and their luggage and special screening systems for nuclear/radiological containers;
- Alarm systems for mass transportation security
Following the 12th Five-Year Plan in more than 20 cities subways will be built, among them Baotou, Datong, Haikou, Huizhou, Hohhot, Jiaxing, Jiman, Jiujiang, Kunshan, Lanzhou, Luoyang, Mudanjiang, Quanzhou, Taiyuan, Weifang, Xiamen, Yinchuan, Zibo, Zhangjiagang, Zhongshan and Zhuhai;
- Alarm systems for land border security
China has a total land border of 22,117 km, with 14 countries. The border with North Korea has a massive concrete and barbed wire fence along parts of its border with the country in order to discourage refugees.

Table 2.28 China critical infrastructure security market by local and foreign based companies (2010-2020) in EUR mn

Alarm systems	2010	2011	2012	2020
critical infrastructure	5,604	6,379	7,270	18,378
maritime security	746	831	923	2,286
mass transportation security	992	1,121	1,267	3,368
land border security	1,138	1,177	1,231	1,980

Market = products and services sales excluding post installation maintenance, upgrades and refurbishment.

Source: HSRC China Homeland Security & Public Safety Market 2012-2020, Oct 2012.

Main Producers of Alarm Systems

Table 2.29 presents an estimated ranking of main producers of alarm systems (estimated by the CHINA SECURITY AND PROTECTION INDUSTRY ASSOCIATION (CSPIA)).

Table 2.29 Ranking of main producers of alarm systems

Ranking	Company	Turnover 2012 (EUR mn)
1	HIKVISION DIGITAL TECHNOLOGY CO., LTD	907.3
2	CHINA SECURITY AND SURVEILLANCE TECHNOLOGY, INC.	573.9
3	ZHEJIANG DAHUA TECHNOLOGY CO., LTD.	444.4
4	SHENZHEN SECURITY GROUP CO. LTD.	400.0 (estimation)
5	GULF SAFETY TECHNOLOGY CO. LTD.	70.0 (estimation)

Firm	HIKVISION DIGITAL TECHNOLOGY CO., LTD
Website	http://www.hikvision.com/en/
Turnover	EUR 907.3mn (2012) EUR 654.4mn (2011) EUR 453.7mn (2010)
Infos	Registered capital: EUR 251.7mn Date of establishment: 30-11-2001 Total capital: EUR 1,341.9mn (2012) Number of employees: approximately 8,000

Firm	CHINA SECURITY AND SURVEILLANCE TECHNOLOGY, INC.
Website	http://cn.csst.todayir.com/html/about_profile.php
Turnover	EUR 573.9mn (2012) EUR 459.4mn (2011)
Infos	Registered capital: EUR 75.5mn Date of establishment: 2006 Total capital: EUR 427.5mn (2012) Number of employees: approximately 8,000

Firm	ZHEJIANG DAHUA TECHNOLOGY CO., LTD.
Website	http://www.dahuasecurity.com/
Turnover	EUR 444.4mn (2012) EUR 277.5mn (2011)
Infos	Registered capital: EUR 144.2mn Date of establishment: 03-2001 Total capital: EUR 427.5mn (2012) Number of employees: 2,731

Firm	SHENZHEN SECURITY GROUP CO. LTD.
Website	http://www.chinesessg.com/
Turnover	Estimation 2012: around EUR 400mn
Infos	Private enterprise producing wireless alarm systems Number of employees: approximately 6,000

Firm	GULF SAFETY TECHNOLOGY CO. LTD
Website	http://www.gst.com.cn/en/index.asp
Turnover	Estimation 2012: around EUR 70mn
Infos	Private enterprise Number of employees: approximately 1,000

SWOT analysis

A key strength of the Chinese security industry lies in the low to mid-range of security technologies. Given the large scale of the Chinese market in this range, both public and private, firms can attain economies of scale, even if competition among 4,000 firms may yet have to rationalize the industry. A further strength is the large interest and support of national authorities for high-tech security products. This provides a base for development towards higher end products. It is noteworthy in this respect that innovation appears to concentrate in SMEs rather than large companies.

A weakness of the low and medium range industry segments is the extent of protectionism, reflected in difficult certification procedures for foreign suppliers. Though the high-end market is more open to foreign competition, the reliance of demand on the public sector could become a problem for nurturing indigenous growth in the industry. A focus on export markets would be needed here to generate alternative sources of demand.

Opportunities for industry are all related to the growth of demand. The high pace of construction and infrastructure investment create a wealth of opportunities.

Challenges to successful growth are found in the regulatory uncertainty, fuelled by dependence on multiple layers of government and incidence of corruption. Also, domestic competition and protection against foreign competitors may threaten survival of part of the industrial base. It is paramount that conditions for survival should not disadvantage often more innovative SMEs. At present, this may be the case though. Opening low- and medium range markets to effective international competition could help the more competitive to survive. In contrast, in high end segments of the industry, strong foreign competition still appears to hamper local development of an industrial base.

For EU industry, high-end market potential fuelled by public sector demand offers opportunities for entering Chinese markets. Critical infrastructure protection appears a promising segment in this respect. A threat is posed by weak intellectual property protection, which may serve to enable Chinese industry to successfully enter in high-end segments via reverse engineering. In low end markets, EU industry faces strong competition from China, but value chain restructuring appears to have settled into this reality by now. Components and hardware are produced in China, while value EU (and US) companies are focused on the development and supply of value-added services (system design and integration, monitoring services).

Table 2.30a China General security industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Huge size of the market; • Besides the governmental plans also security programs of the provinces and municipalities are existing; • Strong financial support of the Government for investment based on assumed strong demand (internal and external terrorism etc.); • Strong growth of the security market because of growing urbanisation (in 2020 more than 200 cities with more than 1mn inhabitants) and therefrom big demand in critical infrastructure and corresponding security equipment; • Big interest in <i>high-tech</i> security products in general (low- and mid-level equipment is produced in China). Note: Limited enforcement of intellectual property rights; • Long-term planning by the Government on the basis of Five Year Plans. 	<ul style="list-style-type: none"> • Protectionism: low and medium level products are taken from the local production where more than 20,000 manufacturers are active as competitors (mainly SMEs). Only mid to high tech products (premium products) are imported; • Difficult certification; • At present main customers are the general and regional/local Government; currently enterprises and other organisations have less or no interest in security products; • The very big HLS producers are state-owned and therefore privileges on the market; • Local payments; • Limited enforcement of intellectual property laws (despite WTO membership).
Opportunities	Threats
<ul style="list-style-type: none"> • Big interest of the Chinese Government in mid to <i>high-tech</i> security products; • Product innovation in bigger (state owned) companies slow, in SMEs, joint ventures and foreign companies faster; • Integration in the EU Framework Programmes; • Reduction of production costs by manufacturing in China; • Big market for security products and services in enterprises in China. 	<ul style="list-style-type: none"> • Around 20,000 local competitors in the field of low to mid level security technology. Growing innovation of SME's; • Dependence on the general/regional/local Government; • Strong competition from companies of the whole world; • Strong relations military forces – HLS; • No removal of local payments; • Cyber attacks.

Opportunities EU Industries	Threats
<ul style="list-style-type: none"> • Delivery of mid to <i>high-tech</i> security products and equipment in a huge market; • Strong attacks of Muslim and other minorities would increase the security demands; • China's political wish of independence from the USA; • Hong Kong (with functioning law system) as good base for marketing in PRC; • Use of low wages/salaries for manufacturing (but they are higher than in India and other Far East countries); • Extension of R&D co-operation with the EU; • Twinning projects (training of Chinese personnel in Europe); • Strong presence of EU firms supports marketing of security products in "neighbouring" markets (for example: aircraft-airports); • In the future growing interest of Chinese enterprises in security supplies and services expectable. 	<ul style="list-style-type: none"> • Protectionism: low to medium level products are taken from the local production where more than 20,000 companies are active as competitors. Only mid to <i>high tech</i> products (premium products) are imported; • Development of a complicated certification process; • The very big HLS producers are state-owned and therefore privileged on the market; • Local payments; • Pressure of USA against European high-tech deliveries; • Decrease of China's development to a free market; • Acceleration of the innovation process (especially at universities and SMEs) makes production of high-level technologies in China possible; • Military conflict between PRC and Republic of China (RC); • Limited Intellectual Property Rights; • Essential reduction of economic growth.

Table 2.30b China airport screening industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Building of new and expansion of existing airports as consequence of urbanisation and growing internationalisation which need new airport screening equipment; • Growing number of passengers demands extended capacities in airport screening; • Following the results of our sample of security products producing firms China seems to be stronger in other security sectors than in airport screening; • Local firms cannot deliver equipment with mid to high level technologies; • Selection of airport screening will be a part of the general planning of new airports. Most likely the planning process will be undertaken by a foreign planning office or planning subsidiary of a Western airport. This supports the choice of foreign equipment. 	<ul style="list-style-type: none"> • Relatively low local experience with airport screening; • Very slow innovation process in the airport screening sector compared with other states; • Available Chinese capacity only for parts of low to mid level technologies in airport screening; • Competition between fast trains and airplanes cannot be prognosed for short distance flights.

Opportunities	Threats
<ul style="list-style-type: none"> • Big interest of the central/regional/local government in mid to <i>high-tech</i> screening equipment. In this segment the Chinese security industry is not as strong as in other sectors; • Where possible: consideration of airport screening in international R&D programs; • Where possible: twinning projects (training of Chinese experts at EU airports). 	<ul style="list-style-type: none"> • International competition influenced by the state policy, the aircraft industry and the branch of planning and construction firms; • Uncertainties about the design of complete security concepts for (new or renewed) airports; • Smaller economic growth reduces number of passenger flights and therewith demands in new airport capacity and equipment; • Growing international competition especially from these organisations which plan the whole airport.
Opportunities – EU Industries	Threats
<ul style="list-style-type: none"> • Huge, in the future strongly growing airport screening market (urbanisation, building of own aircraft industry etc.); • Long-term goals are well known through five year plans; • EU-firms present in the local aircraft market. 	<ul style="list-style-type: none"> • Protectionism (low to medium level devices taken from local companies); • Local payments; • Limited enforcement of Intellectual Property Law; • Trade policy of competing countries.

Table 2.30c China alarm systems industry SWOT Analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Huge market; • Saturation point will not be reached for many years because mostly enterprises are not aware of the demand in security up to now; • The size of the market will grow with increasing urbanisation: safe cities, critical infrastructure etc.; • China has big own capacities for low to mid level technologies in the field of alarm systems; • No budget constraints; • Control of persons is part of the general policy of the Government. 	<ul style="list-style-type: none"> • Missing of centralised command systems, complete building “steering systems” and other <i>high-tech</i> equipment; • Strong internal competition; • Slow innovation; • Limited enforcement of the Intellectual Property Law.
Opportunities	Threats
<ul style="list-style-type: none"> • Big interest in joint ventures with foreign mid to <i>high-tech</i> firms; • Promotion of international co-operation in the R&D field. 	<ul style="list-style-type: none"> • Economic recession reduces speed of urbanisation; • Strong competition through other countries with lower wages than China (India and other countries of Far East).
Opportunities EU Industries	Threats
<ul style="list-style-type: none"> • Huge market and growing demand; • Up to now practically an “open market” at industry which is mainly inefficiently equipped with alarm systems; • New demands coming from critical infrastructure, for example the energy sector and offshore oil production; • Elaboration of security concepts for complete complexes; • Slow local innovation; • Broad experience of the EU countries in 	<ul style="list-style-type: none"> • International competition; • Reduction of urbanisation which is also depending on economic growth; • Local payments.

Strengths	Weaknesses
<ul style="list-style-type: none"> urbanisation, which is higher than in China; • Business acquisition through training in EU-countries (twinning projects); • China's participation in EU-Research Programmes; • Opportunities for EU-firms already active in China with a product segment "alarm systems". <p>Opportunities for sale concern only mid to high level technologies.</p>	

2.3.7 Brazil

Security context

With a population of almost 200 million people, Brazil is a fast growing and young nation and the largest economy in South America. According to statistics⁹⁶ Brazil is among the most violent countries in the world. According to Waiselfisz (2013)⁹⁷ Brazil is the country with the largest number of homicides by firearms in the world (in 2010, per day 108 deaths). Brazilians also share this view as they classify public security and drug trafficking as, respectively, the second and third most important issues facing the country, according to a study performed by CNI⁹⁸ in 2011 (CNI 2011).

General security market development

Visiongain (2012)⁹⁹ estimates Brazil's Security Market to be one of the twenty largest in the world, with a value of \$1.74 billion (€1.13 billion). The market is also expected to be one of the fastest growing over the coming year, and is expected to reach \$4.2 billion (€3.2 billion) by 2020.

The Security Industry Association (SIA) 2012 report on the Brazilian security market¹⁰⁰, provides an estimate of the value of the market for electronic security equipment of \$592 million (€453 million). Moreover, it is expected that this market segment will at least triple this value up to US\$1.8 billion (€1.38 billion) by 2017. Part of this growth can be explained by the increasing need for integrated security systems in high-end developments and of the use of electronic equipment instead of traditional use of personnel for security purposes.

Key developments in the Brazilian security market include the following¹⁰¹:

- **Border security.** The Amazon border is subject to an intensive drug and arms smuggling and requires intensive patrolling. Also the frontier with Paraguay is requiring increasing control due to an increase flow of illegal immigration, smuggling and terrorism threats. Given its vital importance for Brazil a national strategy has been developed (*Estratégia Nacional de Segurança nas Fronteiras (ENAFRON)*) by the Ministry of Justice. Moreover, the strategic border plan (*Plano Estratégico de Fronteiras*) was jointly created by the Ministries of Justice and Defence with the goal of integrating security agencies and police forces to protect Brazilian borders against drug trafficking, arms smuggling, theft of livestock and other crimes (Blog Ministry of Justice, January 2013). Investments of *ENAFRON* in the period 2009-2012 amount to €0.8 billion (R\$ 0.2 billion). Quite large investments are also being made to create the

⁹⁶ Guardian datablog, Simon Rogers, 22 July 2012.

⁹⁷ Julio Jacobo Waiselfisz, Mapa da Violência 2013: Mortes matadas por armas de fogo, Faculdade Latino-Americana de Ciências Sociais (FLACSO), Brazil 2013.

⁹⁸ National Confederation of Industry (CNI).

⁹⁹ Visiongain (2012): The Homeland Security Market 2012-2022.

¹⁰⁰ SIA (2012) "Brazil Security Market Report 2012".

¹⁰¹ Developments in the aviation security sector are described under the sub-heading 'Aviation screening market'.

SisGAAz (*Sistema de Gerenciamento da Amazônia Azul*) program for surveillance of the Blue Amazon;

- **Large events.** The security aspects of the organisation of the coming large events have become such a pressing issue that the Ministry of Justice created a special Secretariat for this purpose (*Secretaria Extraordinária de Segurança para Grandes Eventos, SESGE*). The SESGE is responsible for the security of the 2014 World Cup, the Confederations Cup and 2016 Olympic Games and has a budget of €0.45 billion (R\$ 1.17 billion), while €266 million (R\$700 million) will also be invested by the Ministry of Defence. Recently SESGE invested €33 million (R\$ 87.3 million) in the acquisition of Mobile Integrated Command and Control Centres;
- **Public security.** High levels of criminality and violent crime are a pressing issue for authorities and private individuals to invest in security. The Brazilian Yearbook of Public Safety report of 2012 shows that the total expenditure in the country with public safety increased by 14% between 2010 and 2011 to reach €19.6 billion (R\$ 51,55 milliard);
- **Protection of infrastructures:** The importance of (physical) protection of critical infrastructures is reflected in the recent White Paper National Defence 2012. The allocation of a budget of €5 billion (R\$ 13.23 billion) in the period 2011-2035 to this area portrays this importance;
- **Cyber and information security:** Cyber attacks have emerged as one of the leading dangers to infrastructure security. Accordingly, the White Paper National Defence 2012 has considered cyber defence a priority sector and focus now on ensuring that the country has a cyber -defence and counter-attack mechanisms by increasing the scientific and technological capacity of the country and human resources in this area (White Paper National Defence 2012). Here an investment of €319.8 million (R\$ 839.9 million) is expected in the period 2011-2033 (National Defence Strategy). Besides this defence investment, according to the International Data Corporation (IDC), Brazil is about to reach the significant milestone of €0,77 billion (US\$ 1 billion) in the Information Security market segment. In 2011, the market reached €596 million (US\$ 779 million), of which 32% for the software, 25% hardware and 43% for services (Biajante 2013).

Although port security is not been included in the above list, it is expected to become more important in the period after the forthcoming major international events. Large investments in port infrastructures have been pursued by the National Commission on Public Safety in Ports, Terminals and Waterways (CONPORTOS) in the areas of security (implementation of the international legislation against terrorism). However it appears that effort in this area has shifted to expansion of the port capacity for trade vessels and tourist cruise ships (due to upcoming large events) rather than reinforcing security.

Situation of the security industry

The private security industry in Brazil emerged during the 1960s and has been growing steadily since then. However, only in 1983 was specific legislation introduced to regulate this market (Picini 2004). Currently, the number of private security personnel is already larger than the total of federal, military and state police¹⁰². According to this source, there are 2,000 private security companies operating in Brazil generating approximately €1,37 billion (R\$ 3,6 billion) in 2011. It is expected that private security will grow further due to the upcoming major events.

Based on media reports and company information, some of the companies that are active in the Brazilian security market in the areas of fire fighting, integrated security systems and private security, are:

- **Iveco Magirus Brandschutztechnik GmbH:** A German based company that produces a range of firefighting and civil protection vehicles. They were awarded in 2013 the contract to equipping

¹⁰² <http://www.defesanet.com.br/seguranca/noticia/6876/Governo-quer-nova-lei-para-vigilancia-privada>.

27 Brazil's airports with 80 units of high-end Airport Rescue and Firefighting Vehicles with worth of €53 million (R\$ 141 million)¹⁰³;

- **Johnson Controls:** A USA based company active in three segments, one of them being building efficiency. In this area they provide equipment, controls and services for heating, ventilating, air-conditioning, refrigeration and security systems. Johnson Controls will provide security systems for 2014 Soccer World Cup in Brazil. This project consists of the design and installation of advanced and integrated security systems for 12 major soccer stadiums throughout Brazil. The €22 million (US\$ 29 million) project includes mass access control systems designed to quickly provide access to large numbers of people; video surveillance, ticket systems and a communications network for the stadiums¹⁰⁴;
- **Sagem Sécurité** (Safran group): A European company of the Safran group that provides solutions and services in optronics, avionics, electronics and critical software for the civilian and military markets. In 2010 they were chosen to provide a key security solution for the Minas Gerais State Administrative Centre in the capital city of Belo Horizonte, in partnership with Task Sistemas (a Brazilian company)¹⁰⁵. Optovac Mecânica e Optoeletrônica Ltda (Brazilian company) was acquired by Sagem in 2012 to handle the marketing, production and support of Sagem's product range for its customers in Brazil¹⁰⁶;
- **SISGRAPH:** Sisgraph markets solutions for Intergraph Security, Government & Infrastructure and Intergraph Process, Power & Marine in South America and is part of the Swedish Hexagon Group. They have been present in Brazil 30 years and are active in the areas of geographic information systems, engineering and processes, information management, traffic management, utilities and telecom, public safety and crisis management. They provided an integrated security system for the Pan American Games 2007 in Rio de Janeiro¹⁰⁷, and have been delivering integrated security systems for several states in Brazil over the previous last years, including border control;
- **Condor:** Condor is a Brazilian company founded in 1985 that is active in manufacturing Non-Lethal and Pyrotechnics high-tech Equipment for disturbance situations, military and rescue signalization. In 2013 they provided the non-lethal electric device Spark to the Coordination of Special Resources (*Coordenadoria de Recursos Especiais CORE*) national civil police unit of the State Rio de Janeiro¹⁰⁸;
- **Prosegur Brasil:** Prosegur Brasil was installed in Brazil in 1981 as part of the Argentinian group Juncadella. In 2001 the company was bought by Prosegur Spain Brazil. In 2009 Prosegur acquired the Brazilian company Setha Indústria Eletrônica, focused on the development and manufacture of electronic security systems and industrial communication. This company operates in the area of public security offering among others, surveillance services, logistics and cash in transit services, alarms, training of security professionals, etc. According to the company website the company has 52,000 employees and turnover in 2012 of €1.03 billion (R\$ 2.7 billion). Moreover, they are active in 25 states and also in the Federal District and are the largest group of private security in Brazil¹⁰⁹. During Rock in Rio in 2011, Prosegur was responsible for the security in partnership with Bosch Security Systems that supplied state-of-the-art surveillance technology¹¹⁰.

¹⁰³ http://www.airport-suppliers.com/supplier/lveco_Magirus_Brandschutztechnik_ http://www.airport-suppliers.com/supplier/lveco_Magirus_Brandschutztechnik_GmbH/press_release/Airport_Rescue_and_Firefighting_Vehicles_ARFF_2/.

¹⁰⁴ http://www.johnsoncontrols.com/content/us/en/about/our_company/featured_stories/world_cup_2014.html.

¹⁰⁵ <http://www.safran-group.com/site-safran-en/press-media/press-releases/2010-698/article/sagem-securite-access-control?10324>.

¹⁰⁶ <http://www.safran-group.com/site-safran-en/press-media/press-releases/2013-920/article/optovac-sagem-s-brazilian?12797>.

¹⁰⁷ http://www.sisgraph.com.br/press/email/2007/BI_SGI_setembro_2007.htm.

¹⁰⁸ <http://www.condornaoletal.com.br/images/stories/corenaolet.jpg>.

¹⁰⁹ <http://www.prosegur.com.br/BR/ProsegurNoBrasil/index.htm>.

¹¹⁰ <http://www.prosegur.com.br/BR/SalaPrensa/PRWEB009481>.

Airport screening market

Currently several modernisation projects are taking place in order to extend and modernize the airport infrastructure in order to deal with the current increase of air passengers and to cope with the current and expected increase of air passengers flow (due to the upcoming large events like the Football World Cup and Olympic Games). For instance, in 2012 the Ministry of Tourism announced an investment of € 1.14 billion in infrastructure projects across the country. Moreover, the federal government approved a plan to invest € 2.13 billion in 13 airports between 2011 and 2014.

It can be noted that due to the recent granting of airport concessions, new equipment for passenger and baggage screening has been acquired. The following three concessions have recently been awarded:

- São Paulo airport /Guarulhos was awarded to the consortium “Aeroporto Internacional de Guarulhos”, formed by Invepar, OAS, and South African operator ACSA for €6.17 billion (R\$16,2 billion) for a 20 year period;
- Campinas airport / Viracopos airport was awarded to the Consortium Aeroportos Brazil comprising of Brazilian toll road operator Triunfo Participações and France's Egis Airport Operation for €1.45 billion (R\$3.8 billion) for a period of 30 years;
- Brasília airport concession has been awarded to a consortium comprising of Brazil's Grupo Engevix and Argentina's Corporación America, led by Inframérica group for €1.71 billion (R\$4,5 billion) for a period of 25 years.

Also for smaller airports, like the airport of Fernando de Noronha, investments of €1.26 million (R\$ 3.3 million) are planned for its modernisation, which includes a system of x-ray and metal detector portal for the luggage.

The National Civil Aviation Agency (ANAC) is the regulatory agency responsible for the regulation, safety and security oversight of Brazilian civil aviation. The public airport operator Infraero is responsible for promoting and coordinating the installation and permanence of the security services, as well as police customs, justice and health services at airports. Infraero administrates a total of 66 airports, including international as well as small regional airports. These airports accounted for 97% of Brazil's air transport movements in 2011 (Hochstrasser, Matter 2013). Finally, the Secretariat of Civil Aviation, organ of the Presidency (SAC/PR), was established in March 2011, to formulate, coordinate and supervise the development of policies for the civil aviation industry and airport infrastructure and civil aviation.

Given the increase in passenger numbers, (ANAC website – Estatísticas), it is expected that the demand for security technologies will grow significantly in the coming five years. For instance, in 2012 Infraero opened a bidding process for the procurement of 180 hand luggage x-ray equipment to be placed at 63 airports, from which the following will receive the largest number of equipment: Porto Alegre (RS) with 19, Galeão (RJ), with 17, Curitiba (PR), with 11, and Confins (MG), with 10 equipment, Website Infraereo 14 March 2012.

Other Infraereo investments in airport security equipment are:

- Acquisition for the International Airport of Guarulhos, Campinas (SP), a new TV system and surveillance with cameras (about 640 cameras), about € 4,6 million (R\$ 12 million). This new system enables monitoring from different stations, and has a large storage capacity and a higher quality of image capture compared to the previous system composed of analog cameras (Website SESVESP - Transporta brasil, 16 February 2012);
- Acquisition of 1,500 new security equipment (among others, digital cameras) with an investment of about € 0.57 million for six airports in the Northeast (Recife e Petrolina (PE), Fortaleza e

Juazeiro do Norte (CE), Teresina e Parnaíba (PI), João Pessoa e Campina Grande (PB) e Natal (RN)), World Cup Portal, 1 March 2013;

- Acquisition of 17 x-ray systems for the airport of Fortaleza, Website Infraereo, 20 March 2013;
- Installation of three new passenger screening portals for Natal airport (about € 102 million), Website Infraereo, 13 February 2013.

Given the increase in passenger numbers, it is expected that the demand for security technologies will grow significantly in the coming five years. According to Visiongain (2012)¹¹¹ the Brazilian aviation security market amounted to \$210 million (€160 million) (US) in 2011. From 2012 to 2022, the Brazilian aviation security market is projected to record a Compound Annual Growth Rate (CAGR) of 6.5%, resulting in 2022 in an aviation security market worth around \$ 400 million (€306 million).

The main companies identified as active in this market segment include:

Smiths Detection Brazil

The Smiths group, based in London, has identified Brazil as a potential market, and as such the Smiths Detection Group acquired its distributor in Brazil, EBCO Systems Lda, to take full control of its routes to market. EBCO, based in São Paulo, was the exclusive distributor for Smiths Detection in Brazil since 1994, selling and servicing a wide range of X-ray and trace detection systems to customs authorities, airports, and prisons and also during large events. The new company, called Smiths Detection Brasil, employs approximately 55 people and operates a subsidiary of Smiths Detection Group Limited. Smiths Detection systems are vastly used all across Brazil and were the suppliers of the main security systems to protect the United Nations Conference on Sustainable Development, held in Rio de Janeiro 2012¹¹². Some of their activities in the area of airport security are:

- The B-SCAN, security equipment to detect concealed objects in the human body, is being used in Galeão (RJ), Cumbica (SP) and Brasília (DF)¹¹³;
- The 02PN20, metal detector reinforced to inspect people in transit is deployed at Hercúlio Luz (SC) and Viracopos (SP) national airports and in international airports¹¹⁴;
- The Ceia SMD600, a portal metal detector with ultra-high sensibility to all kinds of metal, made by CEIA¹¹⁵ and sold in Brazil exclusively by Smiths Detection, is now being used at national Brazilian airports such as Congonhas (SP), Viracopos (SP), Cumbica/Guarulhos (SP) and Galeão (RJ), as well as in international ones¹¹⁶;
- The IONSCAN 500DT, portable equipment that can detect and identify simultaneously narcotics and explosives traces is present in national airports; Pampulha (MG), Galeão (RJ), Congonhas (SP)¹¹⁷.

This company has more than 1,200 inspection equipment for X-ray and trace detection systems and chemical identifiers operating in Brazil¹¹⁸. According to the CEO, Danilo Alves, the company holds 85% of the ports market share and holds a strong presence in the airport security market

¹¹¹ Visiongain (2012): The Aviation Security Market 2012-2022.

¹¹² http://www.smithsdetection.com/1025_6447.php.

¹¹³ http://airportnews.com.br/novo_site_eng/noticias_interna.php?ID=125&type=EMPRESA.

¹¹⁴ http://airportnews.com.br/novo_site_eng/noticias_interna.php?ID=149&type=EMPRESA.

¹¹⁵ CEIA is a world leading manufacturing company specialized in the design, engineering and production of Metal Detectors and Electromagnetic Inspection Devices.

¹¹⁶ http://airportnews.com.br/novo_site_eng/noticias_interna.php?ID=133&type=EMPRESA.

¹¹⁷ http://airportnews.com.br/novo_site_eng/noticias_interna.php?ID=183&type=EMPRESA.

¹¹⁸ <http://www.alide.com.br/joomla/capa/36-noticias/3605-aeroportos-de-sao-paulo-receberao-equipamentos-de-inspecao-de-raio-x-da-smiths-detection>.

(currently 500 security equipment is being used in Brazilian airports)¹¹⁹. Moreover, Smiths Detection Brasil ambition is to contribute with 10% of the sales of the international Smiths Group.

VMI Security Systems

The VMI Group, a Brazilian company, started in 1985 with the development of technologies for imaging through x-ray. VMI developed the first baggage scanner, Spectrum 150, fully designed and manufactured in Brazil, in partnership with Infraero. Due to the increasing need for security VMI Security Systems was created in 2010 and established alliances with the international companies Nuctech Company Limited and Gilardoni Italian Scientific Industry. Currently VMI Security Systems is a company focused on solutions for inspection systems for both aviation, rail, maritime and environmental protection. The inspection systems are aimed at both baggage, cargo and containers and safety inspection of liquids. Its main customers include Federal and State Departments, Ministry of Justice of Brazil, Penitentiary institutions, Airports, Stadiums, Ports, etc. VMI security systems ended first on Infraero bidding process for the procurement 180 hand luggage x-ray equipment to be placed at 63 airports¹²⁰.

Detronix Detectores de metais

Brazilian company working in the development, production and commercialization of metal detectors, covering mainly safety doors, walk-through, manual detectors and industrial detectors. Provided in 2012 the MettlerMNI metal detectors for the new sport complex Grêmio Football Porto Alegre Arena¹²¹.

Alarms system (and electronic security) market

According to the SIA Brazil Security Market Report 2012, the electronic security market is expanding in Brazil. This is partially due to the upcoming large events, large number of major infrastructure projects, to the high criminality levels and perception of security. Moreover, it is expected that the upcoming large events will stimulate the access control and video surveillance market segments, including intelligent video surveillance. In particular, the video surveillance segment is quite relevant, since Brazil is still in the transition from analogue to network video equipment (a large proportion of the market is still analogue). This report also mentions that the Brazilian market for (physical) electronic security equipment totals € 453 million (US\$ 592 million). Moreover, it is expected that this market segment will at least triple up to € 1.38 billion (US\$ 1.8 billion) by 2017. Part of this growth can be explained by the increasing need for integrated security systems in high-end developments and of the use of electronic equipment instead of traditional use of personnel for security purposes. Also, governmental institutions and companies are responsible for 90% of the market demand in this area. It should be noted that this survey gathered data from the Brazilian formal market and used manufacturer prices, without accounting for taxes and other services.

On the other hand, according to ABESE (Brazilian Association of Suppliers of Electronic Security Systems) the electronic security sector generated in 2010 approximately € 1.2 billion¹²², which provided an increase of 12% compared to the previous year. Over the past nine years, this market has been growing at rates averaging 13% annually. In 2012 the market reached € 1.6 billion and a growth of 11% is expected in 2013. Data gathered by this association also points out that only 12% of electronic security equipment is placed at condominiums and residences. Therefore, this area

¹¹⁹ http://airportnews.com.br/php/noticias_interna.php?ID=321&type=NOTICIA.

¹²⁰ <http://www.infraero.gov.br/index.php/br/imprensa/noticias/4788-143-infraero-abre-licitacao-para-compra-de-aparelhos-de-raio-x-de-bagagem-de-mao.html>.

¹²¹ <http://www.detrnix.com.br/Noticias/ARENA-DO-GREMIO-PROTEGIDA-PELA-DETRONIX/17>.

¹²² ABESE estimate of the market segment size is larger than reported by SIA. A possible explanation for this difference resides, as mentioned, in the scope of activities considered (physical equipment) and also to the fact that only the formal market segment was considered.

has good possibilities to expand, since only 11% of the condominiums, with possibility of receiving monitored alarm systems, are currently monitored. ABESE provided the following market breakdown in 2012: share of video surveillance and monitoring 44%, access control 23%, alarm systems 23% and fire detection and suppression 10%. It is worthwhile mentioning that currently 18,000 companies are active in the area of electronic security, generating more than 200,000 jobs. It should be noted that in Brazil an informal mark in this area still exists (although the establishment of the Law 1759/200 provides regulation for electronic security companies).

The Brazilian electronic security industry is made up of small and micro businesses (about 84%)¹²³. These small companies are often focused on products with low cost and technological complexity. Moreover, foreign electronic security products account for approximately 50% of the total market share, with U.S. products representing half of these imports. Israel, Korea and Japan, are each responsible for 10 to 15% of the import market share.

Some of the main companies identified as active in this market segment include:

Bosch Security Systems

Bosch Security Systems is a global manufacturer and distributor active in the areas of video surveillance systems incl. video over IP and intelligent video analysis, Intrusion detection systems, Access control systems, Fire alarm system, etc.

The Brazilian branch of Bosch started in 1954, having in 2012 more than 9000 employees and € 1.6 billion (\$R 4.1 billion) sales¹²⁴. Bosch Security Systems division is structured to provide full support to its customers' projects before, during and after the sale. For instance, together with Astech Sistemas Integrados de Segurança they installed an integrated security system in the Shopping Mall of *Parque das Bandeiras*, in Campinas¹²⁵.

GSN Brasil (Global Security Network)

A Brazilian based company with 18 years experience that offers services and equipment in the areas of electronic alarms, video surveillance, access control and telemetry¹²⁶. This company introduced the alarm system PARADOX in Brazil, according to the Journal of Security (Revista Segurança & Cia, 2012).

JFL Alarmes

A Brazilian company founded in 1994 and specialised in the area of alarm systems and electric fences. They have won several prizes in this area over the last years. Among them the "Brand Prize Brazil (*Marca Brasil*) 2013 for alarms, electric fences, VTC systems, etc."¹²⁷.

SWOT analysis

The following key findings emerge from a SWOT analysis for the Brazilian security industry. The high levels of crime and vast border areas imply a consistently high demand for security, both from new and traditional threats. Government support for homeland security programs further strengthen the base for the industry. The industry itself has some areas of expertise related mostly to spill-overs from the defence sector. However, the market remains fragmented and difficult regulatory conditions may prevent the market from reaching its potential integration at national level.

¹²³ Mello (2012), "Introduction to the Security Industry in Brazil"; article from The Brazil Business, available at: <http://thebrazilbusiness.com/article/introduction-to-the-security-industry-in-brazil>.

¹²⁴ http://www.brasil.bosch.com.br/pt/br/br_main/about_bosch_home_1/about-bosch-in-brazil.php.

¹²⁵ http://www.boschsecurity.com.br/acerca/noticias_y_eventos_prensa/shopping.asp.

¹²⁶ <http://www.gsnbrasil.com.br/>.

¹²⁷ <http://www.jfl.com.br/institucional-marca-brasil-2013>.

Currently, the economic environment is conducive to a high growth in private demand. The public investment in R&D and procurement in security are also growing, to face new threats related to border security, civil protection and infrastructure protection. These demand growth prospects present the main opportunities for development of the industry.

On the downside, the industry faces an environment of persistent barriers to entrepreneurship, and the lack of innovation may threaten future competitiveness. At the same time, the abundant number of local regulations and subsidy schemes support a protectionism, e.g. the law No. 12,349, December 15, 2010 (U.S. & Foreign Commercial Service and U.S. Department of State 2011). Also the lack of transparency of the certification of equipment poses additional constraints. Moreover, often technical literature of equipment has to be translated into Portuguese. The physical dimensions of the country also often demands that a company has to open branches at several states, or work with local suppliers.

Finally, the focus of local industry of electronic security equipment is often on products with low cost and technological complexity, which can be partially explained by the lack of qualified personnel, and the lack of commitment in R&D by the industry. On the other hand, initiatives to stimulate the embedding of R&D in industry have been defined as well as several programs to train qualified personnel. Moreover, strengthening security is more than ever a relevant issue also due to the upcoming large events.

Therefore, the main opportunities for EU security industry reside in the development of high-end technological innovation products and training of personnel, possibly in cooperation with local partners/industries in order to counter the protectionism attitude and deal with the difficult business environment.

Table 2.31a Brazil the security industry (general) SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> Continuing and emerging new security threats; National Initiatives in security programs; Available expertise and know-how in some areas (especially defence-related). 	<ul style="list-style-type: none"> Fragmented market; Difficult certification environment and unclear policies; Informal market; Protectionism: Preference given to local companies; Lack of qualified personnel.
Opportunities	Threats
<ul style="list-style-type: none"> Upcoming large events; Large and many infrastructure projects; Increasing government investment in security & defence R&D; Government stimulation to international technology alliances. 	<ul style="list-style-type: none"> Difficult business environment; Brazilian private sector commitment to innovation is weak.
Opportunities for the EU	Challenges for the EU
<ul style="list-style-type: none"> Need for qualified personnel and high end technology; The National Science and Technology Strategy focus on technological innovation. 	<ul style="list-style-type: none"> Dealing with the Brazilian security frameworks and protectionism.

Table 2.31b Brazil airport screening sector SWOT analysis

Strengths		Weaknesses	
<ul style="list-style-type: none"> • Numerous and large airport infrastructures; • Continuing security threat. 		<ul style="list-style-type: none"> • Fragmented market; • Difficult certification environment and unclear policies; • Informal market; • Protectionism: Preference given to local companies; • Lack of qualified personnel. 	
Opportunities		Threats	
<ul style="list-style-type: none"> • Several programs for extension and modernization of airports; • Government stimulation to international technology alliances; • The National Science and Technology Strategy focus on technological innovation. 		<ul style="list-style-type: none"> • Difficult business environment; • Brazilian private sector commitment to innovation is weak. 	
Opportunities for the EU		Challenges for the EU	
<ul style="list-style-type: none"> • Need for qualified personnel and high end airport screening technology (like body scanners, liquid detectors, etc.); • Government stimulation to international technology alliances; • The National Science and Technology Strategy focus on technological innovation. 		<ul style="list-style-type: none"> • Dealing with the Brazilian security framework and protectionism. 	

Table 2.31c Brazil electronic security (alarm) systems SWOT analysis

Strengths	Weaknesses
<ul style="list-style-type: none"> • Active sector; • Continuing and emerging new security threats; • National Initiatives in security programs; • Available expertise and know-how in some areas (especially defence-related). 	<ul style="list-style-type: none"> • Fragmented market; • Difficult certification environment and unclear policies; • Informal market; • Protectionism: Preference given to local companies; • Lack of qualified personnel.
Opportunities	Threats
<ul style="list-style-type: none"> • Upcoming large events; • Large and many infrastructure projects; • Increasing government investment in security R&D; • Government stimulation to international technology alliances; • The National Science and Technology Strategy focus on technological innovation; • Increasing need for personnel (and residence) protection; • Increasing need for video surveillance high end integrated electronic security equipment (like network video equipment, etc.). 	<ul style="list-style-type: none"> • Difficult business environment; • Brazilian private sector commitment to innovation is weak.
Opportunities for the EU	Challenges for the EU
<ul style="list-style-type: none"> • Need for qualified personnel and high end integrated electronic security equipment (like network video equipment, intelligent video surveillance, etc.); • Government stimulation to international technology alliances; • The National Science and Technology Strategy focus on technological innovation. 	<ul style="list-style-type: none"> • Dealing with the Brazilian security framework and protectionism.

2.4 Competitive position of the airport screening and alarm systems industries

2.4.1 Introduction

This section provides a competitiveness analysis of two segments of the security industry: 'alarm systems' and 'airport screening equipment'. Alarm systems represent part of what may be considered the 'traditional' security industry while 'airport screening equipment' is part of what may be considered the 'new' security industry that has developed particularly in response to terrorism threats. The analysis draws on previous studies that have been undertaken on behalf of the Commission, which has been supported through additional background research and contacts with industry stakeholders. In addition, a specific analysis has been undertaken of international trade in intruder and fire alarms. Concerning specific estimates of relevant cost items and cost impacts associated to conformity assessment and certification, these are described in Chapter 3.

2.4.2 Overview of the airport screening sector¹²⁸

Industry structure

The supply of security inspection and screening equipment for the transport sector is concentrated among a few international players, mainly from the US and Europe. These include companies such as Morpho (Safran), Smiths Detection and Rapiscan in the EU, and L3, SAIC and AS&E in the US. The table below shows the main players in this industry, EU as well as non-EU.

Table 2.32 Main Players security screening equipment industry (EU and non-EU)

Manufacturer	EDS	LEDS	SSC	EU	Non-EU
Analogic	O	X			X
CEIA		X		X	
Cobalt		X		X	
FLIR		X			X
Gilardoni	O	X		X	
L3	X	X	X		X
Morpho	X	O	O	X	
Nuctech	X	X	O		X
Optosecurity	O	X	O		X
Rapiscan	X	X	O		X
Reveal	X	X			X
Smith Detection	X	X	X	X	
X → Available // O → Development					

Source: information from industry expert.

Note: EDS: Explosive Detection System; LEDS: Liquid Explosive Detection System; SSC: Security Scanners.

Below tables provide an overview of financial and product line information for some of these main players.

The development of the sector has been characterised by strategic acquisitions, notably by several companies strongly connected to the defence sector that have sought to strengthen their position in the civil security sector.¹²⁹ Alongside the handful of leading players are a few medium and smaller

¹²⁸ For additional background information on the airport security screening equipment sector see "Study on the competitiveness of the EU Security Industry" and the SECERCA study.

¹²⁹ Examples of M&A activity in the transport security sector include: SAIC acquisition of Reveal Imaging in 2010; Safran (Morpho) acquisition of GE Homeland Protection in 2009; L3 acquisition of Perkin Elmer's Detection systems business in 2002; Smiths Detection acquisition of Heinemann Systems in 2002; OSI acquisition of Rapiscan Security Products in 1993.

companies that tend to focus on the development of specialised niche products or specific technologies. It may be noted, also, that some companies maintain linkages to the health sector (i.e. through the use of similar technologies required for health imaging) while other companies have been set up to commercialise technologies resulting from academic research.

Main players in the industry: detailed information

Table 2.33a - SMITHS DETECTION (UK)

Main indicators	Smiths Group		Smiths Detection	
	2011	2012	2011	2012
Turnover	€ 2,466.6m	€ 2,476.8m	€ 442.6m	€ 423.1m
Profit	€ 448.7m	€ 451.7m	€ 57.3m	€ 56.3m
R&D budget	€ 96.3m	€ 95.4m	€ 30.4m	€ 30.2m
Number of employees	22,900	23,200	2,500	2,300
Description of the company				
<p>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 (47% 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.</p>				
Main products and technologies				
<ul style="list-style-type: none"> • 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. 				
Location of production				
Smiths Detection: United Kingdom, Singapore, United States				

Sources: www.smithsdetection.com, Smiths Group 2011 Annual Report and Smiths Group 2012 Annual Report.

Table 2.33b - SAFRAN (FR)

SAFRAN (former GE Security)		
Main indicators*	SAFRAN (former GE Security)	
	2011	2012
Turnover	€ 11.7bn	€ 13.6bn
Profit	€ 669m	€ 1bn
R&D budget	€1.3bn	€1.6bn
Number of employees	60,000	62,500
Description of the company		
<p>Former GE Security has been bought by SAFRAN Group in April 2009. SAFRAN Group is a leading high-technology group and Tier-1 supplier of systems and equipment for aerospace, defence and security. Operating worldwide, Safran has 62,500 employees and generated sales of 13.6 billion euros in 2012. Through Morpho, Safran masters all technologies needed to address security requirements in airports: explosive detection, identification, secure travel documents, border control and access control for secure zones.</p>		
Main products and technologies		
<ul style="list-style-type: none"> • Its products are mainly related to X-ray (CT) based EDS equipment (EntryScan, CTX and XRD series) and ETD equipment (Itemiser, VaporTrace, MobileTrace models); • SAFRAN developed a new system (CAT/BPSS) that will automatically check driver's licenses, passports and other routine ID documents and ensure that the passenger matches his or her boarding pass. 		
Location of production		
<p>Safran: France, United Kingdom, Belgium, Germany, Russia, United States, Mexico, Canada, Brazil, Morocco, South Africa, United Arab Emirates, India, China, Singapore, Australia</p>		

Source: Safran Annual Report 2012 and General Electric 2012 Annual Report.

Table 2.33c - L3 SECURITY & DETECTION (US)

Main indicators	L3 Communications		L3 Security & Detection	
	2011	2012	2010	2011
Turnover	€ 10,897.3m	€ 10,231.9m	€ 238.8m	€ 265.1m
Profit	€ 1,148.0m	€ 1,051.5m	N/A	N/A
R&D budget	€ 52.4m	€ 68.5m	N/A	N/A
Number of employees	61,000	51,000	N/A	N/A
Description of the company				
<p>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.</p>				
Main products and technologies				
<ul style="list-style-type: none"> • 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 millimetre wave imaging and energetic materials detection. 				
Location of production				
Australia, Canada, Germany, Italy, Korea, Norway, United Arab Emirates, United Kingdom, United States				

Source: L3 Communications 2011 Annual Report and L3 Communications 2012 Annual Report.

Table 2.33d - RAPISCAN SYSTEMS (US)

Main indicators	OSI Systems, Inc.		Rapiscan Systems	
	2011	2012	2011	2012
Turnover	€ 475.7m	€ 619.3m	€ 213.7m	€ 281.3m
Profit (operating)	€ 24.2m	€ 32.7m	N/A	N/A
R&D budget	€ 32.9m	€ 35.6m	N/A	N/A
Number of employees	N/A	3900	N/A	N/A
Description of the company				
<p>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 ten locations and supported by a global support service network.</p>				
Main products and technologies				
<ul style="list-style-type: none"> • 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. 				
Location of production				
<p>Rapiscan: United States, Australia, Cyprus, United Arab Emirates, Hong Kong, Mexico, United Kingdom, Finland, Singapore, Malaysia</p>				

Source: OSI Systems, Inc. 2012 Annual Report.

Table 2.33e - SAIC (US)

Main indicators	SAIC	
	2011	2012
Turnover	€ 7,917.7m	€ 7,601.5m
Profit (operating)	€ 448.8m	€ 42.4m
R&D budget	€ 39.9m	€ 66.8m
Number of employees	42,000	41,100
Description of the company		
<p>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. Since 2010 is Reveal Imaging Technologies, Inc. part of SAIC. It belongs to the Transportation Technology Unit, part of SAIC's Infrastructure, Energy, health and Product Solutions Group.</p>		
Main products and technologies		
<ul style="list-style-type: none"> • 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; • SAIC is provider of the Explosive Detection System (EDS) and automated threat detection technologies, including inspection systems that check baggage for explosives. 		

Source: SAIC Annual Report 2012.

Table 2.33f - AMERICAN SCIENCE & ENGINEERING (US)

Main indicators		
American Science & Engineering		
	2011	2012
Turnover	\$278.6m	\$ 203.6m
Profit	\$42.8m	\$21.4m
R&D budget	\$22.2m	\$25.5m
Number of employees	420	415
Description of the company		
<p>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 defence, 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 34% of total company sales in 2012. Europe accounts for 6% of international company's revenue during 2012.</p>		
Main products and technologies		
<ul style="list-style-type: none"> 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). 		
Location of production		
AS&E: United States, Mexico, Brazil, Netherlands, Hong Kong, Singapore		

Source: AS&E 2012 Annual Report.

Table 2.33g - GILARDONI (IT)

Main indicators		
Gilardoni		
	2011	2012
Turnover	N/A	€ 38.1m
Profit	N/A	N/A
R&D budget	N/A	N/A
Number of employees	N/A	±200
Description of the company		
<p>Gilardoni is among the main European suppliers of X-ray and ultrasonic equipment's, 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.</p>		
Main products and technologies		
<ul style="list-style-type: none"> • 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.

Production activities

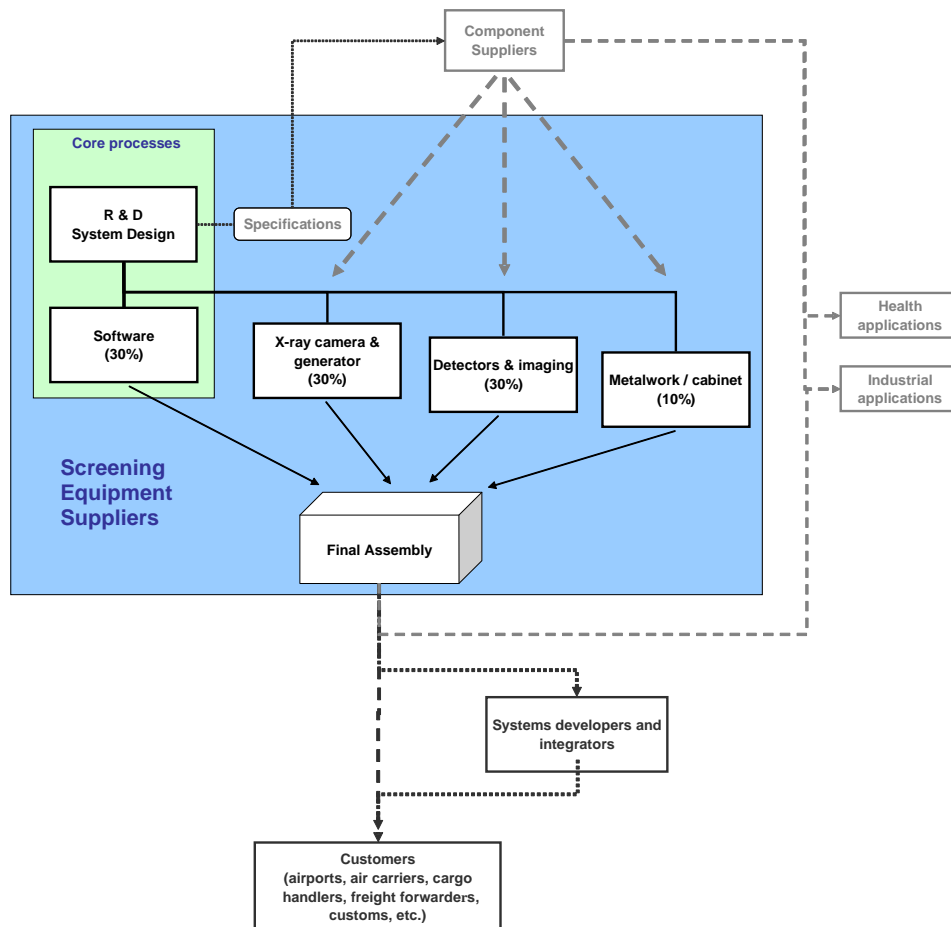
In terms of technology development and upstream linkages to component suppliers, the situation of providers of security inspection and screening equipment (OEMs) can differ depending on the technology expertise within the company (or other companies within the same group). Depending on this expertise, main components 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 of value added for security screening equipment.¹³⁰ A consequence of this situation is 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.¹³¹

¹³⁰ 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).

¹³¹ This may be mitigated somewhat when the company (or company group) is engaged in supplying technologies/equipment to markets other than security (e.g. health, or industrial applications). 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.

Typical manufacturing activities – which increasingly relates to final assembly – is undertaken ‘in-house’ and at the main business locations of equipment suppliers (i.e. US, Western Europe). This reflects the need for close oversight of product assembly and for maintaining proximity between manufacturing activities and technical and systems development activities.¹³² Smaller companies (e.g. producers of specialised equipment) may outsource manufacturing/assembly activities but this is generally not the case.¹³³ There is, however, the possibility that manufacturing and assembly activities may be relocated outside of US/Europe, partly to reduce costs but also in response to market opportunities.¹³⁴ Another aspect of production that may eventually become subject to outsourcing and/or off-shoring is software development, which can be extremely labour intensive¹³⁵. 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).

Figure 2.6 Stylised supply/value chain for aviation security screening equipment¹³⁶



¹³² 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.

¹³³ 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.

¹³⁴ For example, in 2006 Smith’s detection opened an x-ray production/assembly site in St Petersburg to serve the growing Russian market.

¹³⁵ 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>.

¹³⁶ Based on the example of x-ray based systems. Numbers in parentheses indicate the approximate breakdown of cost elements in final equipment.

Competitive position of EU suppliers¹³⁷

The major American 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. 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 global players are US-based companies. Even for the main EU-based companies, it is evident that access to the US market has been a crucial factor in enabling them to occupy their current market position.

Unfortunately, it is difficult to quantitatively assess the competitive position of EU suppliers of airport screening equipment. Information on the global market position of EU suppliers is not readily available and estimates, where they exist, are subject to wide differences. Even for the aviation security market as a whole, estimates differ substantially across sources. The estimated market size presented in this study (see Section 2.2.3) is about 80% higher than the forecast presented in HSRC (2008).¹³⁸ Moreover, security inspection and screening equipment is not identifiable from existing product classification used for the collection of international trade data. This implies that there are no export and import data at country level for the airport screening equipment segment.

To provide a quantitative impression of the competitive position of EU suppliers, this study makes use of the annual reports for some of the main players identified above. Insofar data are available, the annual reports give information about sales revenues by geographic market area. Table 2.33 shows the share of revenues by main market for six of the main companies active in the airport screening sector. The last line reports estimated total revenues in 2012 in million euro, based on the reported information on the share of security and detection in total revenues.

Table 2.33 Revenues of main companies in airport screening equipment by geographical market area (2012, percentage of total revenue)

	Smiths (UK)	Safran (FR)	L3 (US)	Rapiscan (US)	FLIR (US)	Analogic (US)
Europe	26%	46%	6%	19%	24%	24%
Americas				68%		
North America	50%	30%	84%		51%	39%
Asia	7%	16%	1%	12%	-	16%
Oceania	-	-	1%	-	-	-
Other	17%	8%	8%	0%	25%	21%
Total revenues (million euro)	635	1492	256	302	66	48

Source: annual reports; Ecorys. Notes: Analogic's figures for Europe include Germany, the Netherlands and Denmark, and Asia refers to Japan only. "Other" includes the rest of Europe, Canada and China for example. The Netherlands accounts for 12% of revenue, but most likely this is mostly in medical appliances. In security, this share is likely an overestimate. The figures for Rapiscan refer to the Americas, including the North American and Latin American markets.

The figures in the table show that the EU based main companies are less focused on their home market than most of their US based counterparts. A substantial share of revenues accrues from activities in the US market, as explained above. The US market is even the main market for the UK based company Smiths. Competitiveness of the EU suppliers on the global and US market appears to be strong. In terms of global sales estimates, Safran and Smiths exceed the US based companies, of which Rapiscan has become the largest competitor as of 2012. The share of revenues that sources from outside of the EU and US market is about 25% for the EU suppliers.

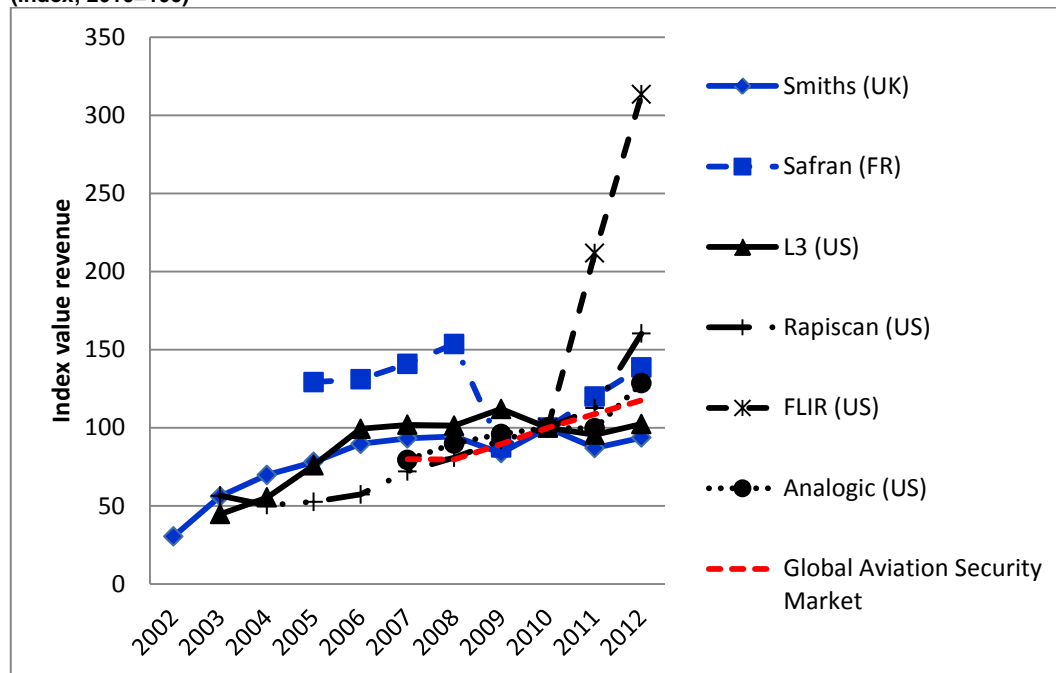
¹³⁷ Information on the global market position of EU suppliers of security inspection and screening equipment is not readily available and estimates, where they exist, are subject to wide differences. Moreover, security inspection and screening equipment is not identifiable from existing product classification used for the collection of international trade data.

¹³⁸ HSRC (2008) Global Homeland Security, Homeland Defense and Intelligence Markets Outlook 2009-2018.

This is higher than for L3 and Rapiscan, which focus on the (North) American markets. The two smaller US suppliers appear to be more focused on external markets than their larger US counterparts, although it should be noted that the other markets for Analogic include many EU countries and Canada.

Though still in a strong position, there is some evidence to suggest that main EU suppliers have lost some ground in terms of market shares over time since about 2007 (see Figure 2.7).

Figure 2.7 Development of total revenue for main companies in airport screening equipment over time (index; 2010=100)



Source: annual reports; HSRC (2008); Ecorys. Notes: The development for the global aviation security market is based on forecasts from 2009 onwards. Figure for L3 in 2009 may be somewhat overestimated, as the 2012 annual report has adjusted values for 2009-2011 downwards.

Particularly in the period 2009-2010, both Safran and Smiths appeared to do less well than Rapiscan and to a lesser extent L3. In 2011 and 2012, revenue performance recovered for Safran, but both companies have lost market share to US firms such as Rapiscan and the relatively smaller companies FLIR and Analogic.

Table 2.34 compares the growth in total revenues since 2007 across the main companies. It also reports the difference in percentage points growth between the mature markets in the US and EU and the emerging markets in Asia and the rest of the world.

Table 2.34 Growth performance across markets for the main companies in airport screening equipment (2007-2012)

	Growth difference emerging vs. mature markets	Growth total revenues
Smiths (UK)	25%	1%
Safran (FR)	28%	-2%
L3 (US)	31%	0%
Rapiscan (US)	105%	122%
FLIR (US)	13%	213%
Analogic (US)	-23%	47%
Overall markets	12%	47%

Source: annual reports; HSRC (2008); Ecorys. Notes: Mature markets are the EU and North America. Emerging markets are all other markets. For growth difference between the overall geographical market areas, the 10 year growth forecast for 2008-2018 based on HSRC (2008) is used and split in halves to attain a 5 year growth forecast 2008-2013. The growth of the global market may be an overestimate, due to the economic crisis largely occurring after the source publication. For example, Visiongain forecasted a 5.5% annual growth in aviation security for 2012. Against the backdrop of expected recovery in 2012, this suggests annual growth has been lower in the period 2007-2011.

Both the main EU suppliers and US suppliers show a faster increase of revenue in emerging markets than in the EU and North America combined since 2007. In comparison to the growth of the global market expected for the 2007-2012 period in 2008, EU companies appear to have been hit more by the economic crisis. Their performance in markets other than the mature US and EU has however been better than expected on the basis of market forecasts.

Overall, the better sales performance of Rapiscan and recently FLIR suggests that US companies are forging ahead in terms of international competitiveness. Growth in total revenue has reached double digits for these two firms, while Analogic shows a very strong growth in the US and its key EU markets. There is some variation, though, as L3 shows similar growth performance as the EU suppliers.

The loss in market share in emerging markets and in mature markets to these US suppliers may be related to the general framework conditions discussed below. In particular, the regulatory environment in the US may be more conducive to development and certification of airport screening equipment. This could be important for growth perspectives, also for relatively smaller and more specialized companies that introduce new technology to the market. The figures on total revenues presented above seem to provide support for this.

On top of the general regulatory environment, the adoption of a harmonised US certification systems administered by TSA in 2007 may have provided a marketing advantage to US suppliers. Clients in various emerging markets require equipment to have a US certificate as proof of its performance up to high standards meeting essential and technical requirements. Though main EU companies also have the US certificates for their key equipment, given the importance of the US market, there is evidence that the process to acquire certificates for new equipment can be handled more effectively by US based suppliers. While EU suppliers are performing well in emerging markets in their own right, the development of revenues in these markets since 2007 lags behind that for US suppliers such as Rapiscan and FLIR.

Though regulation and other framework conditions are not the only determinants of business success, the monetary equivalent of the growth in total revenues can provide an indication for the competitive advantage developing for US suppliers. The estimated value of growth in total revenues of Rapiscan and Analogic over the 2007-2012 period and of FLIR since 2010 amounts to about €230 million. As the revenue for the main EU companies was roughly stable over the period mentioned, this monetary value could be regarded as an upper bound for the value of the loss in

market share due to reduced competitiveness vis-à-vis US suppliers. Of this amount, roughly €35 million can be attributed to the introduction of the US certification system as of end 2007, which amounts to around €10 million per year on average. This amount reflects the percentage growth in revenues from emerging markets – where the marketing advantage would mostly apply, in so far as it exceeds the average percentage growth in these markets attained by the main EU suppliers Safran and Smiths. A similar analysis for the European market provides a figure of €42 million for the entire period, which amounts to €12 million per year on average. These amounts should be treated with care, as they arise from the use of incomplete data for the purpose at hand. First, only the major suppliers are included. This may not be too much of a problem, as SMEs are likely to be more fragmented in terms of their market reach. Second, we rely only on annual reports for industry data. These main companies are MNCs and they are active in various production and distribution locations. Hence, revenue figures do not relate one-to-one with EU production and employment, for example. This implies that costs or benefits to the industry are not only accruing to EU citizens. On the other hand, the geographical dispersion of activities also implies that the competitiveness of the main EU suppliers is less affected by US harmonised certification, as they tend to shift more towards development in the US to benefit from the same certification advantages in third markets. As a result, EU suppliers may gain less from EU harmonization due to the mobility of US suppliers, but the EU industrial base may gain more than expected purely on the basis of revenue figures.

Looking below the first-tier of what are essentially global players, the European inspection and screening equipment sector industry appears somewhat fragmented and fragile. The remainder of the sector is characterised by companies of relatively limited size, focussed on the development of specific technologies and/or offering specialised or niche products to the market. However, they have neither the size nor the capability to compete with the major players, with whom they must often develop partnerships to have access to broader market segments.

In terms of other international competitors, the only significant company in the aviation security inspection and screening equipment sector is the Chinese company Nuctech¹³⁹. Nuctech is able to build on its direct linkage into the research capacity and network of the University of Tsinghua, while taking advantage of lower production costs than its main rivals. The company has had some success in obtaining contracts in Europe and notably in geographical markets that are of strategic interest to the Chinese state. 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. Price competitiveness is an important factor in the overall competitive position of suppliers but, given the limited scope to compete on price alone, American and European suppliers need to maintain and protect their technological lead – and also reputation and service quality – to remain competitive. This is especially the case in the broader international marketplace, notably in markets such as Asia and the Middle East where aviation demand and, hence, security requirements are expected to grow rapidly in the future.

Among the elements identified as important for the development and future competitiveness of the sector in the EU the following may be noted:

- **Regulatory environment.** The regulatory environment at international, EU and national level plays an important role in shaping demand for aviation security inspection and screening equipment. EU legislation provides an overall framework for aviation security that aims to impose common standards for security requirements across all Member States but the responsibility for implementation and for setting specific requirements within this framework remains with the Member States. Disparities in legislation across Member States mean that demand side actors (e.g. airports, air carriers, and freight forwarders) are unable to adopt

¹³⁹ 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.

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 in case their activities are cross-border and internationally oriented. This implies, for instance, that airlines may have to purchase and utilise different sets of screening technology and equipment depending on the country in which they are operating. The regulatory framework can also present a barrier to the introduction of new technologies. The present EU regulatory framework defines a list of eligible methods and technologies for passenger screening and airports are not permitted to replace systematically any of the recognized screening methods with alternative technologies until they are added to the legally binding list of eligible methods;

- **Security standards and certification.** EU regulations define minimum performance standards for a number of screening technologies used in the aviation sector but Member States retain both the right to choose the technologies they employ and, where warranted by the security situation of the individual Member State, the prerogative to set more stringent performance requirements. Although the European Commission, in collaboration with ECAC has made strides towards the development of common performance standards for several categories of aviation security equipment, and ECAC has put in place a framework for the evaluation of security equipment used in the aviation sector (ECAC Common Evaluation Process (CEP)), approval (certification) of equipment remains at a national level and does not preclude national authorities from subjecting screening equipment to their own national testing and validation procedures. Thus, despite a common overall EU framework for aviation security, differences in national approaches and requirements persist. These differences can be particularly pronounced when they concern the evaluation and introduction of new security technologies and solutions. 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 the 'hands on' approach taken by the Transportation Security Administration is seen as more conducive to the development and eventual adoption and certification of security technologies/equipment. The air transport industry and related stakeholders consider that international standards for the screening of passengers, their cabin and hold baggage and, eventually, air cargo would have the potential to increase security, while also driving down costs for users. The lack of common international standards and certification (or, alternatively the multiplicity of standards and certification systems within the EU) is seen as having an unnecessary negative impact on the global outreach of EU security equipment manufacturers. On the one hand, suppliers serving the EU market incur 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. Accordingly, the absence of common EU certification – or, more broadly, accepted common international standards/certification – place EU equipment providers at a competitive disadvantage;
- **Public procurement approaches.** National responsibilities for the procurement and use of aviation security vary throughout the EU. Typically, subject to the general EU regulatory framework, national authorities set out aviation security requirements but are not responsible for procuring security equipment, which remains with the private sector (airport operators, airlines, freight-forwarders etc.) Accordingly, procurement of aviation security equipment and systems is primarily a concern for the private sector. The extent to which costs associated to security requirements should be borne by public authorities or by the private sector is, however, an issue of broader debate for the aviation sector;

- **R&D support.** Under the EU Framework Programme (FP7) a separate security research programme was created that has supported some projects involved in the field of aviation security. However, stakeholders from the aviation sector and security equipment providers argue that much of the funded research prioritises 'blue sky' and 'multi-national collaboration' projects that are not sufficiently end user-oriented and whose applicability in a 'real world' commercial environment is limited. This is in contrast to the situation in the US where support for R&D and innovation initiatives for US companies are seen to have had a direct impact in raising demand for new types of products and equipment in the United States;
- **Societal acceptance.** The aviation security equipment market is also clearly influenced by public attitudes towards the acceptability of security technologies. The debate surrounding the use of 'security scanners' (otherwise known as 'body scanners' or 'advanced imaging technology') for screening passengers in the aviation sector provides a clear example of the kinds of ethical concerns that may be raised by the use of security equipment/technologies. While the EU is moving towards the deployment of 'security scanners', it has been made clear that in case security scanners are to be deployed "*health and fundamental rights must be safeguarded along with personal data, dignity and privacy*" ¹⁴⁰ and passengers should be given the right to refuse body scanning and submit to alternative screening methods. This situation leaves open the possibility that national authorities may adopt quite different positions when addressing 'ethical' issues. In turn, this may further contribute to the fragmentation of the EU market. The hesitant EU approach is in contrast with that of the USA where they have pushed forward development (e.g. support for R&D) of the 'body scanners' and where the TSA began deployment in 2007. Currently, there are approximately 510 advanced imaging technology units at more than 90 airports. ¹⁴¹

The aforementioned characteristics of the EU market are applicable to all suppliers of screening technologies used in the aviation sector whether they be EU based, American or from elsewhere. However, they disproportionately affect those companies that are orientated towards the EU marketplace. Consequently, they imply that EU suppliers of aviation security equipment incur higher market access costs and risk 'premiums' on investment activities than, for example, their main competitors from the US. These 'additional' costs have a negative impact on the sector's competitiveness and may, in a negative future scenario, contribute to weakening of the EU's competitive position and to an eventual relocation of activities outside the EU, either to the US or to locations with high market growth potential.

2.4.3 Overview of the intruder and fire alarms sector

Industry structure

A relatively small number of major players dominate both the US and the EU market for electronic security products, including intruder and fire alarms. Tyco, UTC, and Honeywell are the main manufacturers of product systems that are marketed worldwide. ¹⁴² Since the mid-90s the major players led an 'acquisition crusade', buying up medium and small security products manufacturers. ¹⁴³ This resulted in considerable consolidation and rationalization within the sector. Bosch and Siemens ¹⁴⁴ are the largest players in the European market and both companies pursued an acquisitions led approach to enter the market for electronic security (and fire) equipment. With the major players focused on products and systems that can be marketed worldwide, there remain

¹⁴⁰ European Parliament's Transport Committee. See: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20110523IPR19946+0+DOC+XML+V0//EN&language=EN>.

¹⁴¹ Source: <http://www.tsa.gov/approach/tech/ait/index.shtm>.

¹⁴² GE Security, another market leader was acquired by UTC in 2010.

¹⁴³ An important motivation for these major companies was that the belief that security/fire equipment markets are relatively stable and not as cyclical and other markets for their products.

¹⁴⁴ An important share of EU fire detectors – mainly automation devices - are made by Siemens in Switzerland.

many niche markets that are very attractive for SMEs, either directly or through the supply of specialized products and components to major manufacturers and integrators, and to the installation service market.

The tables below provide further information on some of the main global players on this market.

Main players in the industry: detailed information

Table 2.36a - Bosch (DE)

Main indicators	Bosch		Energy and Building Technology	
	2011	2012	2011	2012
Turnover	€ 51,494m	€ 52,464m	€ 13,029m	€ 13,358m
Profit	€ 1,820m	€ 2,342m	N/A	N/A
R&D budget	€ 4,190m	€ 4,787m	N/A	N/A
Number of employees	302,519	305,877	N/A	N/A
Description of the company				
The Bosch Group is a leading global supplier of technology and services. In fiscal 2012, its roughly 306,000 associates generated sales of 52.5 billion euros. Since the beginning of 2013, its operations have been divided into four business sectors: Automotive Technology, Industrial Technology, Consumer Goods, and Energy and Building Technology. The Security Systems division is part of the Energy and Building Technology sector.				
Main products and technologies				
<ul style="list-style-type: none"> • The Security Systems division supplies video surveillance, intruder alarms, evacuation systems, and fire alarms; • They also provide public address systems, and access control. 				
Location of production				
Security systems: France, Italy, Netherlands, Portugal, Spain, United Kingdom, United States, China, Australia, New Zealand				

Sources: BOSCH Annual Report 2012.

Table 2.36b - Siemens (DE)

Main indicators	Siemens		Infrastructure & Cities	
	2011	2012	2011	2012
Turnover	€ 73,275m	€ 78,296m	N/A	€ 17,585m
Profit	€ 4,590m	€ 6,321m	N/A	€ 1,102m
R&D budget	€ 3,899m	€ 4,238m	N/A	N/A
Number of employees	402,000	410,000	N/A	N/A
Description of the company				
Siemens is divided over six sectors: Energy, Healthcare, Industry, Infrastructure & Cities, Equity Investments, and Financial Services. The Infrastructure & Cities Sector offers a wide range of sustainable technologies for metropolitan centres and urban infrastructures worldwide, such as integrated mobility solutions, building and security systems, power distribution equipment, smart grid applications and low- and medium-voltage products.				
Main products and technologies				
<ul style="list-style-type: none"> The Building Technologies Division (part of the Infrastructure & Cities Sector) offers products, services and solutions for commercial, industrial, public and residential buildings, including heating and ventilation controls, security systems and devices such as intruder detection, video surveillance and building access control, fire safety solutions such as fire detection, protection alarm systems and non-water based fire extinguishing. 				
Locations				
Active in 190 countries.				

Sources: Siemens Annual Report 2012.

Table 2.36c - Tyco (CH)

Main indicators	Tyco		Security Products	
	2011	2012	2011	2012
Turnover	€ 7,653.8m	€ 8,124.7m	N/A	€ 390.5m
Profit	€ 1,246.3m	€ 368.6m	N/A	N/A
R&D budget	€ 106.6m	€ 164.0m	N/A	N/A
Number of employees	102,000	70,000	N/A	N/A
Description of the company				
<p>Tyco is divided in two main businesses: Installation and Services, and Global Products. The division Security Products is part of the Global Products business. The division Security Products is a leading global developer and manufacturer of access control, video, real-time location solutions and intrusion products. The division delivers a comprehensive range of premium security solutions and has a strong market position with large installed base and brand loyalty.</p>				
Main products and technologies				
<p>Security Products designs and manufactures a wide array of electronic security products, including integrated video surveillance and access control systems to enable businesses to manage their security and enhance business performance. Our global access control solutions include integrated security management systems for enterprise applications, access control solutions applications, alarm management panels, door controllers, readers, keypads and cards. Our global video system solutions include digital video management systems, matrix switchers and controllers, digital multiplexers, programmable cameras, monitors and liquid crystal interactive displays. Our security products for homes and businesses range from basic burglar alarms to comprehensive interactive security systems including alarm control panels, keypads, sensors and central station receiving equipment used in security monitoring centres.</p>				
Location of production				
N/A				

Sources: Tyco Annual Report 2011 and Tyco Annual Report 2012.

Table 2.36d - Honeywell (US)

Main indicators	Honeywell		Automation and Control Solutions	
	2011	2012	2011	2012
Turnover	€ 26,483.5m	€ 29,416.4m	€ 11,262.9m	€ 12,402.3m
Profit	€ 1,498.6m	€ 2,285.2m	€ 1,510.2m	€ 1,743.2m
R&D budget	€ 1,304.3m	€ 1,442.5m	N/A	N/A
Number of employees	132,000	132,000	N/A	N/A
Description of the company				
<p>Honeywell globally manages their business operations through four businesses that are reported as operating segments: Aerospace, Automation and Control Solutions, Performance Materials and Technologies, and Transportation Systems. Honeywell's Automation and Control Solutions segment is a leading global provider of environmental and combustion controls, sensing controls, security and life safety products and services, scanning and mobility devices and process automation and building solutions and services for homes, buildings and industrial facilities.</p>				
Main products and technologies				
<p>Two components of the segment Automation and Control Solutions with their main products are:</p> <ul style="list-style-type: none"> • Environmental and combustion controls: E.g. Sensors, measurement, control and industrial components; • Security and life safety products and services: E.g. Security products and systems, Fire products and systems, Access controls and closed circuit television 				
Location of production				
Automation and Control Solutions: USA, China, Czech Republic, Germany, India, Mexico, Netherlands, Scotland				

Sources: Honeywell Annual Report 2011 and Honeywell Annual Report 2012.

Table 2.36e - ADT (US)

Main indicators	ADT	
	2011	2012
Turnover	€2,254.8m	€2,521.1m
Profit	€272.6m	€307.7m
R&D budget	N/A	N/A
Number of employees	N/A	16,000
Description of the company		
<p>ADT is a leading provider of electronic security, interactive home and business automation and monitoring services for residences and small businesses in the United States and Canada. ADT serves more than six million residential and small-business customers, making them the largest company of its kind in both the United States and Canada. ADT delivers an integrated customer experience by maintaining the industry's largest sales, installation and service field force and most robust monitoring network, all backed by the support of 16,000 team members.</p>		
Main products and technologies		
<ul style="list-style-type: none"> • Business protection: Burglar Alarm Monitoring, Fire & Smoke Monitoring, Carbon Monoxide Monitoring, Panic Button, Video; • Home protection: Intrusion Detection & Monitoring, Access Control Systems & Management, Video Surveillance; • In 2010, ADT launched ADT Pulse, the first home and business automation platform available for the mass market nationwide. Today, Pulse customers across the U.S. and Canada are able to adjust thermostats and lighting, lock and unlock doors, and view real-time video from security cameras, all from their smartphone, laptop or tablet. 		
Location of production		
Sale and service are only located in the U.S. and Canada. Production facilities are also in the U.S. and Canada.		

Sources: The ADT Corporation 2012 Annual Report.

Table 2.36f - UTC (US)

Main indicators	UTC		Climate, Controls & Security	
	2011	2012	2011	2012
Turnover	€ 40,421.7m	€ 45,070.0m	€ 13,676.4m	€ 13,347.3m
Profit	€ 3,781.6m	€ 4,061.2m	€ 1,603.7m	€ 1,893.9m
R&D budget	€ 2,465.0m	€ 3,124.0m	N/A	N/A
Number of employees	199,900	218,300	65,741	61,272
Description of the company				
UTC Climate, Controls & Security, a division of United Technologies Cooperation, is a combination of the former divisions Carrier and UTC Fire & Security businesses. This division UTC Climate, Controls & Security delivers solutions to customers worldwide from leading brands such as Carrier, Automated Logic, Lenel, Chubb, Det-Tronics, Edwards, Fenwal, Interlogix, Kidde, Marioff and Supra. UTC Climate, Controls & Security sells directly to customers as well as through manufacturer representatives, distributors, dealers and U.S. retail distribution.				
Main products and technologies				
<ul style="list-style-type: none"> • UTC Climate, Controls & Security provides electronic security products such as intruder alarms, access control systems and video surveillance systems and designs and manufactures a wide range of fire safety products including specialty hazard detection and fixed suppression products, portable fire extinguishers, fire detection and life safety systems, and other fire fighting equipment. Services provided to the electronic security and fire safety industries include systems integration, video surveillance, installation, maintenance, and inspection; • Interlogix is the firm that delivers everything what is needed for Electronic security systems, e.g. cameras, monitors, recorders, software, control systems, etc. 				
Locations in Europe				
Climate, Controls & Security: Belgium, Czech Republic, Denmark, Finland, France, Germany, Hungary, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Romania, Slovak, Spain, Sweden, United Kingdom				

Sources: United Technologies Annual Report 2012.

Production activities

Consolidation and internationalisation within the electronic security products sector has promoted the shift of hardware production to Asia; firstly Hong Kong and Taiwan, with China now having a dominant position. All the major players now have (contract) manufacturing facilities in China, which allows them to reduce labour/production costs. By contrast, significant activities connected to the related software systems are still undertaken globally.¹⁴⁵

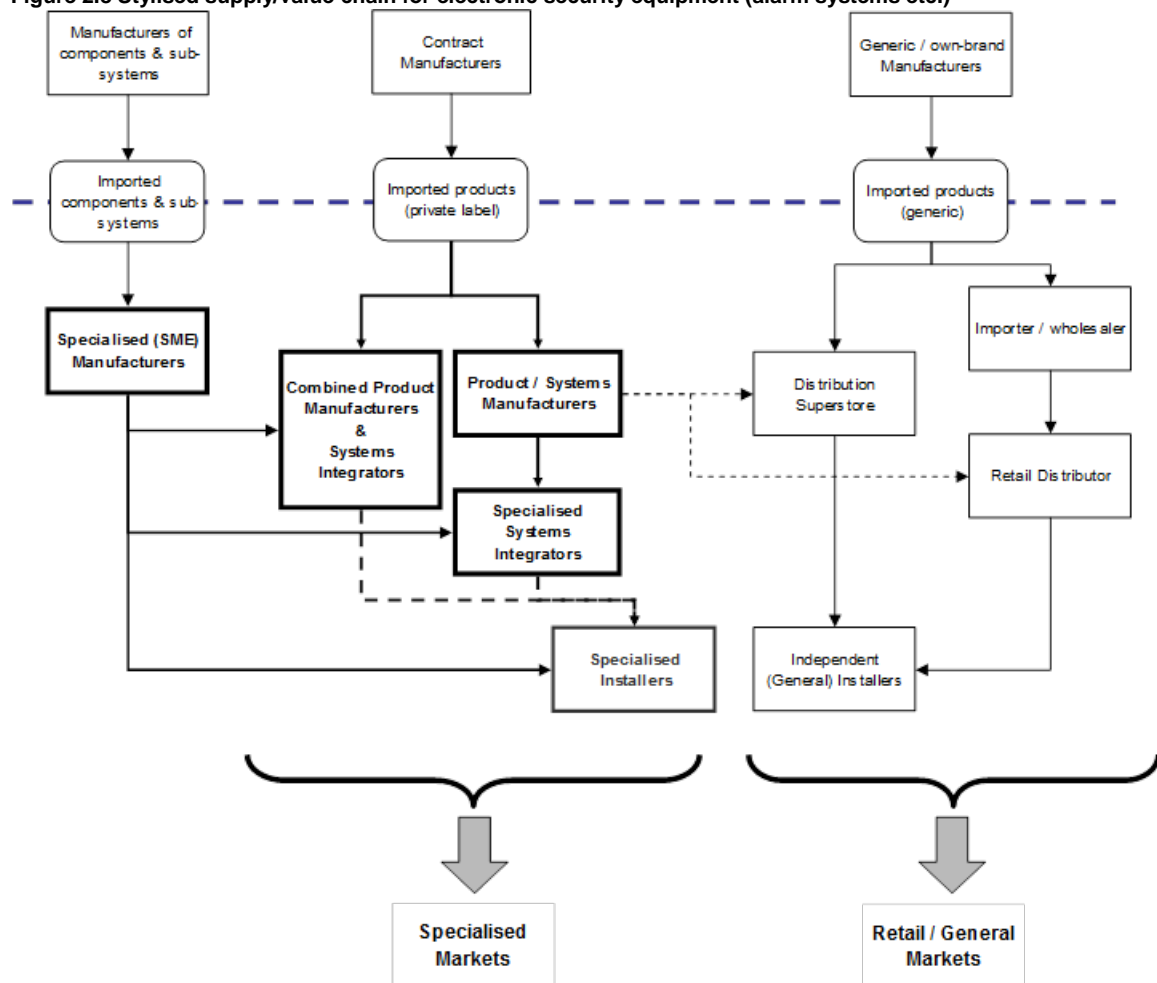
By and large, while the major players may still be manufacturers – albeit that they contract Asian manufacturers to supply products and sub-systems under ‘private labels’ – the main focus of their activities is on systems integration. Other companies, which include most of those in the EU, are more focussed on ‘services’, including research and innovation to develop new high-tech products and product customisation for specialised ‘high end’ market segments.¹⁴⁶

¹⁴⁵ Software development which remains a ‘global’ activity is of particular relevance for surveillance systems. Eventually, more development of ‘soft’ components is expected to move towards the sites for hardware production, particularly with the increasing integration of intelligent systems within surveillance cameras themselves. This development may be accelerated by a skills shortage in software development (e.g. signal analysis) within the EU.

¹⁴⁶ EU companies are also specialising in the following fields or niche markets: perimeter security; interface (e.g. locks); signalling (e.g. sirens); alarm transmission; and wireless equipment.

In terms of the factors shaping competitiveness, it is relevant to note that security equipment is not only characterised by its sophistication but also by its reliability. Accordingly, having the newest technology can be a less important issue than reliability. As a result, in order for technology developments to be adopted in the market they often need to be tied to functionality improvements in equipment/systems. At the same time, the electronic security products sector in general has been characterised by increasing customer requirements for integrated security solutions, both for security products and also accompanying services. This implies that competitiveness of suppliers places less emphasis on performance of individual product categories and more on the supply and integration of a system of products.

Figure 2.8 Stylised supply/value chain for electronic security equipment (alarm systems etc.)



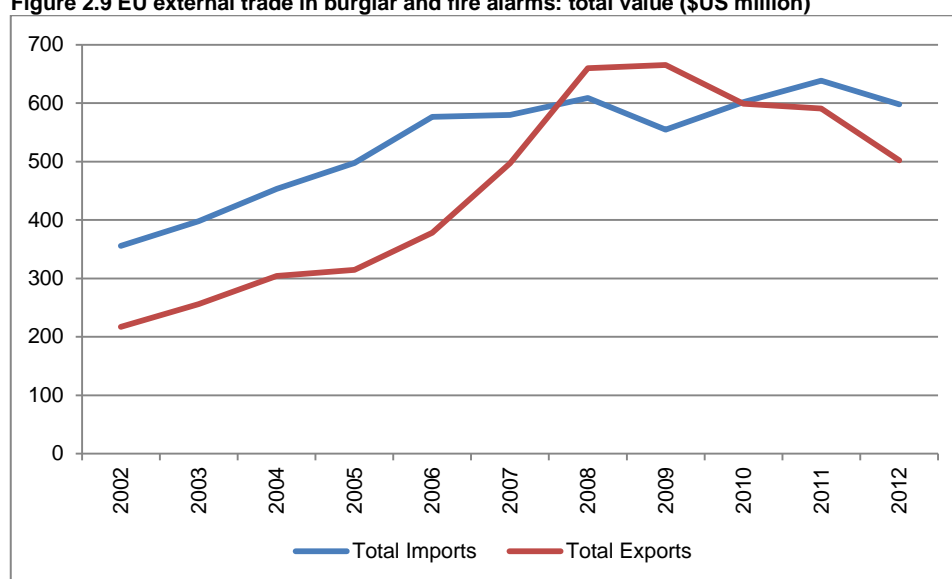
Competitiveness position of EU suppliers – analysis of international trade data

International trade data¹⁴⁷ indicates a strong development of the position of European suppliers in the international market for intruder and fire alarms. Over the past decade, growth in the value of EU exports of intruder and fire alarms significantly outstripped that of imports, such that the EU moved from a negative trade balance to record a positive trade balance in 2008 and 2009 of \$US 51.5 million and \$US 110.5 million respectively. However, this pattern reversed again over the 2010-2012 period, where the EU position substantially worsened over the period of crisis and economic recession. Exports basically returned to pre-crisis levels.

¹⁴⁷ The analysis reported in this section is based on trade data taken from UN COMTRADE database. All data refer to the product code 853110 (HS2002 and HS2007) 'Burglar or fire alarms and similar apparatus'.

Table 2.37 - EU external trade in burglar and fire alarms: total value (\$US million)

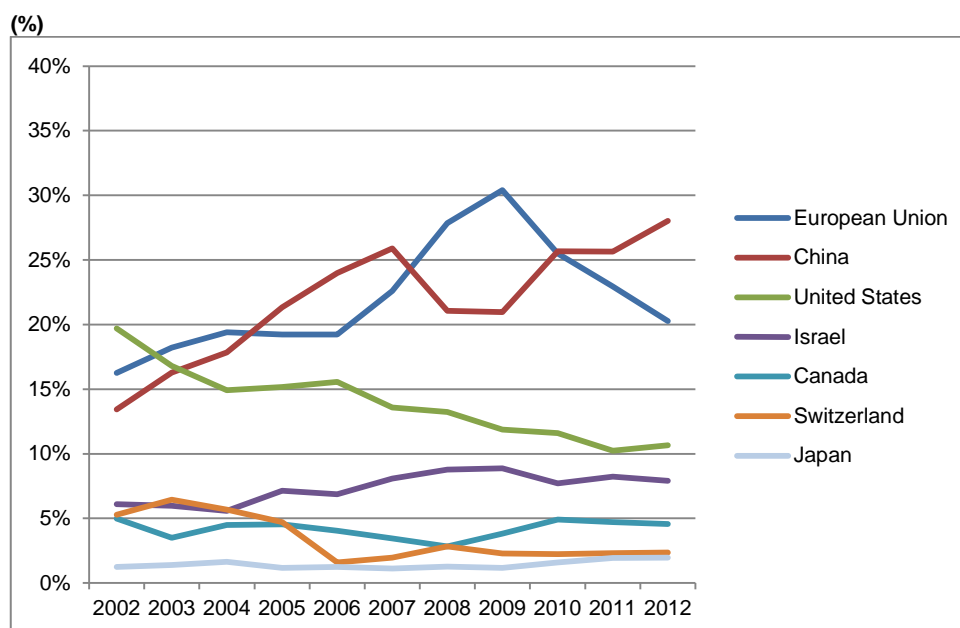
Year	Total Imports	Total Exports	Net balance
2002	355,6	217,4	-138,2
2003	398,0	256,0	-142,1
2004	453,3	304,0	-149,3
2005	497,5	314,7	-182,8
2006	576,5	378,0	-198,5
2007	579,9	497,3	-82,6
2008	608,6	660,1	51,5
2009	554,8	665,3	110,5
2010	602,0	599,1	-2,9
2011	638,6	590,9	-47,7
2012	597,7	502,1	-95,6

Figure 2.9 EU external trade in burglar and fire alarms: total value (\$US million)

Further, the EU has been successful in increasing its share in the value of world trade of intruder and fire alarms, which is shown to have grown markedly from 2005 onwards¹⁴⁸. The data indicate that the share of imports originating from the EU in the value of total world imports of burglar and fire alarms increased from less than 20% in 2002 to about 30% in 2009; though this share appears to have fallen back sharply again during the 2010-2012 period. By contrast the share of the USA has steadily declined over the period (see the Figure below).

¹⁴⁸ For the analysis of aggregate world trade, the estimates are based on reported imports ('mirror' export data) rather than export data. For data concerning the EU, the total value of reported EU exports is closely in line with the total value of imports from the EU reported by receiving countries. The main observed difference between the value reported exports and the value of recorded imports relates to China. Specifically, the total value of reported exports from China is significantly lower than the total value of imports reported as coming from China by receiving countries. This is particularly the case for the earlier years covered by the analysis. Notwithstanding the difference between reported export and import data, the general pattern in the evolution of country shares in total world trade are similar whichever approach is used.

Figure 2.10 Shares of global trade in burglar and fire alarms: share of world imports by source country



The EU's export performance is also reflected in the development of the EU's revealed competitive advantage (RCA) index for burglar and fire alarms, which indicates that the EU has moved from a revealed competitive disadvantage prior to 2007 to a revealed competitive advantage thereafter (see below). In recent years, the upward trend appears to have been broken, in line with the patterns in export performance described before.

Revealed Comparative Advantage (RCA)

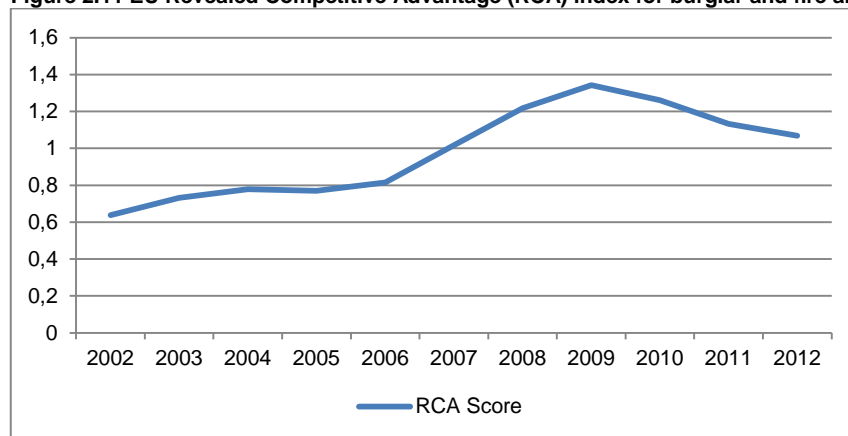
The RCA of a country is defined as follow:

'The RCA index of country i for product j is measured by the product's share in the country's exports in relation to its share in world trade:

$$RCA_{ij} = (x_{ij}/X_{it}) / (x_{wj}/X_{wt})$$

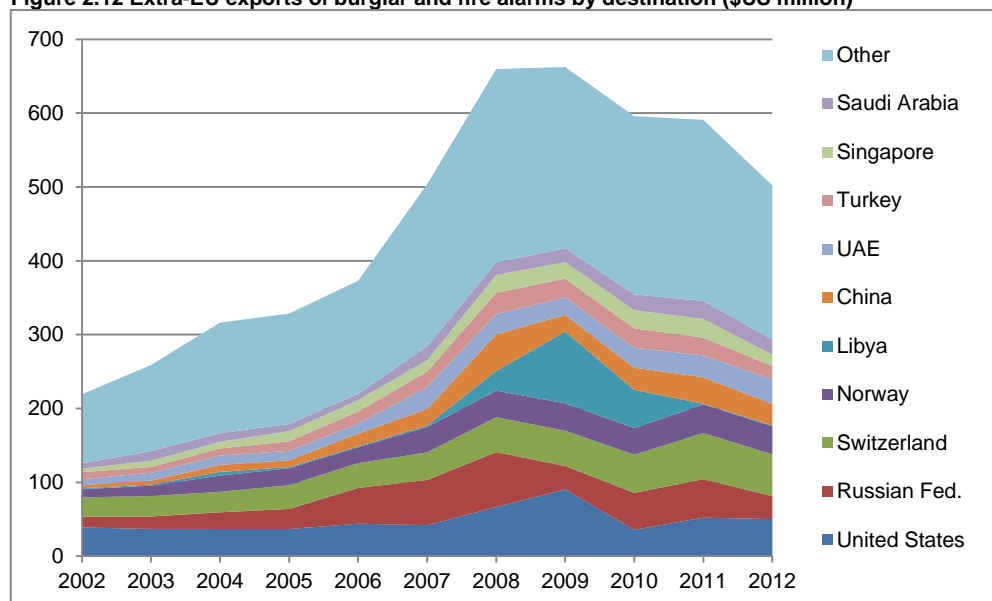
Where x_{ij} and x_{wj} are the values of country i 's exports of product j and world exports of product j and where X_{it} and X_{wt} refer to the country's total exports and world total exports. A value of less than unity implies that the country has a revealed comparative disadvantage in the product. Similarly, when the index exceeds unity, the country is said to have a revealed comparative advantage in the product' (WITS, 2011)

Figure 2.11 EU Revealed Competitive Advantage (RCA) index for burglar and fire alarms



The main markets for EU exports are the USA and the Russian Federation, together with the near neighbours of Switzerland and Norway (see the chart below). Beyond these countries, EU exports are characterised by a wide geographical spread with, it appears, an increasing importance of the Middle East, North Africa and a number of Asian markets (including China). These markets, together with Latin America, are expected to be the main drivers of growth in global demand, particularly given growth expectations for Europe and other developed markets and a probable slump in new construction demand.

Figure 2.12 Extra-EU exports of burglar and fire alarms by destination (\$US million)



The main supplier of EU imports of burglar and fire alarms is (mainland) China, which increased its share of EU imports from 21.7% in 2002 to 41% in 2012¹⁴⁹ (see below). A further 4% for imports originating from Hong Kong may be added to this figure, indicating that nearly half of EU imports of burglar and fire alarms come from China. With the exception of Israel, most of the other main suppliers to the EU market have seen their share of total EU imports fall between 2002 and 2012.

¹⁴⁹ It should be noted that the recorded value of total EU imports of burglar and fire alarms exceeds the sum of recorded values of EU imports from individual (source) countries. The difference between these values is treated as non-specified (N.S). Estimated country shares are based on the share in the sum of recorded values recorded by source country.

Figure 2.13 Extra-EU imports of burglar and fire alarms by source country (\$US million)

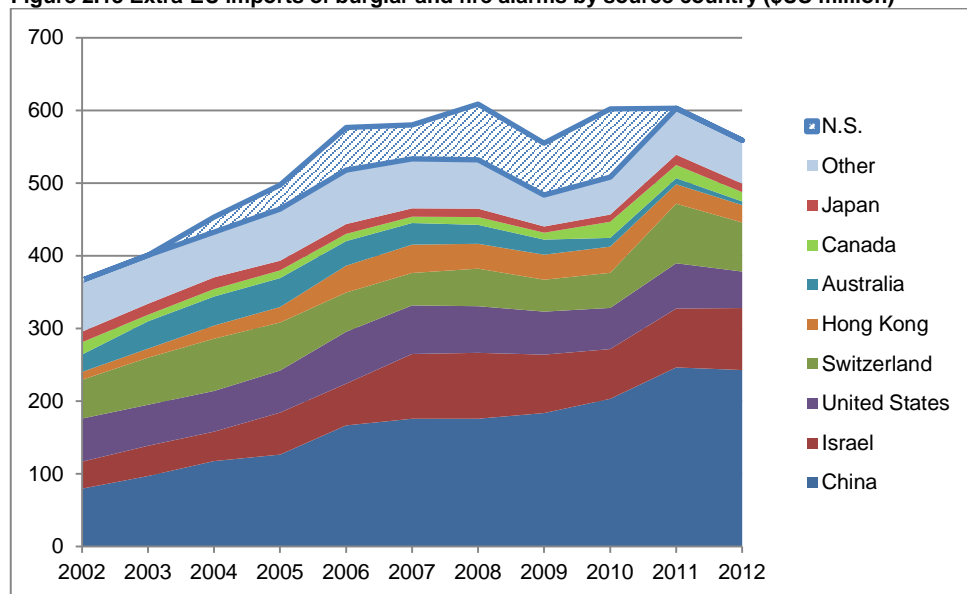
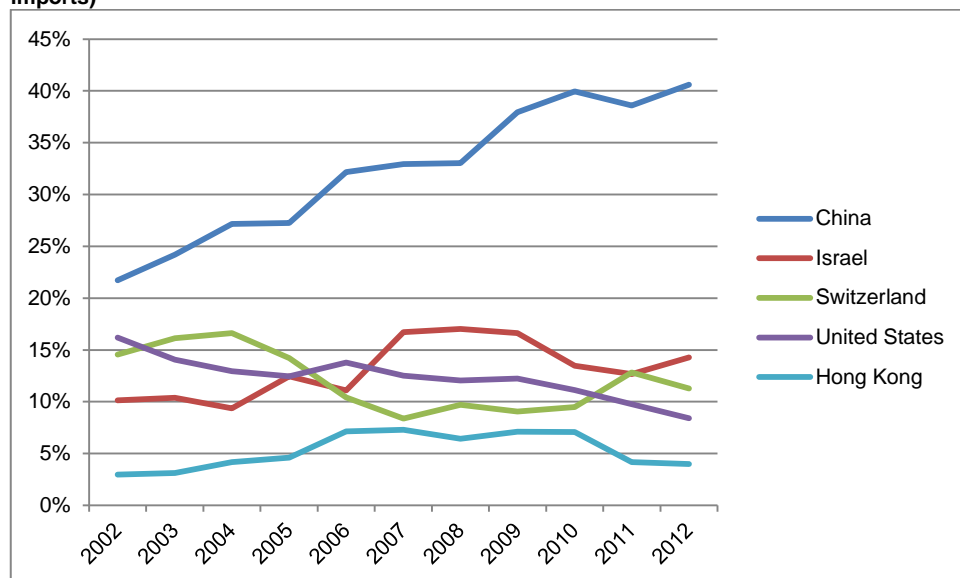


Figure 2.14 Extra-EU import shares of leading supplier countries of burglar and fire alarms (% of imports)



China's position of the main supplier to the EU reflects its role as the dominant location for the basic manufacturer of alarms, with the major global players operating (contract) manufacturing facilities in the country. In this respect, imports of alarm products from China and other low-cost Asian suppliers can be viewed primarily as inputs into the production processes of European and other 'advanced' country suppliers, as opposed to imports that are directly competing with locally manufactured products. This is also indicated by the difference in the relative 'price' (unit value) of Chinese imports which approaches a tenth of the 'price' of products from the EU and other 'advanced' country suppliers (see the next table).

Table 2.38 Estimated average unit value of imports by source country

Country	Unit value (\$US – average for 2009 to 2010)
Canada	54.6
Switzerland	52.6
European Union	37.7
Israel	32.9
United States	30.6
Japan	8.0
Hong Kong, China	4.1
China	3.9

A further feature of the development of EU trade in burglar and fire alarms is the increase in the relative importance of extra-EU trade vis-à-vis trade within the EU. Intra-EU trade, which was worth in excess \$US 1 billion in 2012, remains significantly higher than EU external trade at approximately \$US 500 million in the same year. However, growth in extra-EU exports has tended to significantly outstrip growth in intra-EU trade. Prior to the onset of the financial and economic crisis, which appears to have significantly dampened trade growth, extra-EU exports of fire and burglar alarms grew at an average annual rate of 20% (CAGR)¹⁵⁰ compared to 11% for intra-EU exports. Consequently, over this period the ratio of intra-EU exports to extra-EU exports fell from 3.7 to 2.3 (i.e. the value of internal trade within the EU was 3.7 times that of EU exports in 2002 compared to only 2.3 times in 2008). This trend flattened off since 2008 and the ratio of intra-EU exports to extra-EU exports fell to 2.0 in 2012 (i.e. the value of extra-EU exports rose to half the value of intra-EU trade).

To the extent that intra-EU trade provides an indicator of the underlying growth of demand for burglar and fire alarms within the EU, the relatively slow growth in intra-EU trade compared to extra-EU exports suggests that the ability of the EU burglar and fire alarm producers to maintain and enhance their international competitiveness will be of crucial importance for the sectors future growth performance.

2.5 Summary and conclusions

This chapter has attempted to provide an overview of the situation of security markets and security industries in selected third countries and in the EU. This has covered a general overview for the security sector as a whole, together with a more specific focus on the aviation screening and alarm systems (hereafter referred to as 'electronic security') segments.

2.5.1 Competitive position of selected countries

Broadly speaking, Europe and the USA continue to be the global leaders in the security industry and are generally occupy a position of technological frontrunners in high-end security equipment. However, the global supply-side situation differs across market segments, as is illustrated by the two segments assessed in more detail for this report. In the case of screening equipment for the aviation sector – and more broadly for other market segments such as maritime – the supply of main categories of equipment (passenger screening, carry-on and checked baggage, and cargo screening) is dominated by a handful of main global players, mainly from the EU and US. By contrast, the segment of security alarms – and, more broadly, 'electronic security' including access control and video surveillance – is far more fragmented. On the one hand, leading European and

¹⁵⁰ Compound annual growth rate.

American suppliers of alarm systems (e.g. Tyco, UTC, Honeywell, Siemens, Bosch, Stanley, etc.) probably account for no more than 25% of the global market. On the other hand, there are a multitude of smaller local and regional players active both as suppliers of products and, even more importantly, in installation and maintenance of equipment.

Looking beyond Europe and the USA, Israeli and Japanese companies occupy strong positions in some – typically high-end – niche market segments, notably for IT and communication systems. Neither country has a significant position in the main categories of aviation security screening equipment, though Israel has a number of innovative technological solutions on offer. Both countries are, however, relatively important players in the electronic security field – specifically in video surveillance in the case of Israel – where they are able to offer sophisticated products and systems that are competitive with those from the EU and US. The two countries provide an interesting contrast in terms of the origins and development of the security industry. On the one hand, the Israeli security industry is closely linked to the defence industry (through which it also maintains strong connections with the USA) and its competitive position is based on the development of innovative technologies with proven operational effectiveness. On the other hand, the Japanese security industry is more closely rooted to the country's traditional strengths in consumer electronics and engineering. This is reflected in a focus on networked solutions, intelligent performance and component miniaturisation.

Presently, the bulk of the Chinese security industry is positioned in low to medium-end equipment segments, specifically in relation to products such as alarm systems, access control and video surveillance equipment. The relatively fragmented nature of the domestic electronic security sector (compared to screening technologies, see below) is one of the factors that has allowed foreign players to develop a significant position in the Chinese market, particularly for higher-end products and more complex systems and solutions. However, although foreign companies are expected to benefit from the fast growing Chinese market – driven by factors such as urbanisation, major infrastructure development etc. – their overall share of the market is expected to diminish over time. With respect to the security screening segment, a small number of Chinese companies are active in the market. Most notable is Nuctech, a spin-off from National Tsinghua University in Beijing, which claims to be the leading global supplier of high-energy (cargo) security inspection systems. The company has already been able to make significant inroads into the EU market, with contracts to supply products to, among others: Belgium, Denmark, Finland, Hungary, Ireland, Lithuania, Latvia, Malta, Netherlands, Poland and Slovenia. The company has, however, been embroiled in controversy, and has been subject to allegations of corruption and illegal and unfair business practices.¹⁵¹ The case of Nuctech serves as a pointer towards the ambitions of China to establish its position in the security market, with the assistance of institutional support and funding for technology development. Equally, it shows that the Chinese approach to the security market encompasses an important component of commercial diplomacy.

Turning to the remaining three countries, none of them appear as major competitors for the EU security industry, at least with respect to the specific segments that are the focus for this study:

- Drawing on engineering and technological capabilities that have sometimes been inherited from the Soviet era, there are probably a handful of Russian companies that have the potential to be internationally competitive in some niche market segments but, on the whole, it is fair to say that this potential is some distance away from being fully exploited;

¹⁵¹ In 2009, the EU imposed anti-dumping duties on the company's products, resulting in tit-for-tat anti-dumping duties being imposed by China in 2011. The Chinese duties were ruled to be in breach of WTO anti-dumping rules in February 2013. It seems unlikely, however, that the WTO decision will do much to actually open up the rapidly growing Chinese market for foreign screening equipment suppliers.

- South Korea is home to a number of highly export orientated companies that possess capabilities in the supply of electronic security related hardware and components (e.g. video cameras and digital video recorders (DVR)). However, the hardware specialisation of Korean companies and an apparent weakness in areas such as systems integration suggests that they are not an immediate threat to the competitive position of the EU (and US) security industry;
- Brazil's indigenous security industry is fragmented and currently does not occupy a significant position in the global marketplace. With respect to screening technologies and electronic security systems (alarm systems), it is unlikely that Brazil's weak competitive position will change any time soon, but the possibility for a stronger regional position cannot be ruled out. Equally, drawing on capabilities in aerospace and defence, the desire to provide 'home grown' solutions in fields such as wide-area border and maritime surveillance.

2.5.2 *Market attractiveness of selected countries*

Turning towards the demand side of the security market, drawing on the individual country analysis, Table 2.39 provides an evaluation of the relative attractiveness of the selected (third) country markets for the European security industry.

In this context, although the US security industry is presented as Europe's main competitor, it is also the case that several of the EU's leading companies have a strong market (and production) presence in the USA. This presence reflects both the continuing importance of the US market, both in terms of its overall size and its strategic importance from a global perspective (e.g. product approval and US market position act as a reference in the global security market). At the same time, when applicable to 'dual use' technologies, US International Traffic in Arms Regulation (ITAR) can be a constraint on companies wishing to supply products to the US market, since they may effectively limit the possibility to export technologies to other markets.

In terms of medium term growth prospects, it is evident that large and fast growing markets (e.g. Brazil, China and Russia) are all attractive in terms of their market potential. As noted above, however, the aviation screening equipment market appears to be largely closed to foreign competition, with Chinese procurement being directed to local companies. Moreover, although China already provides component supplies and production facilities for less sophisticated electronic security equipment, concerns relating to intellectual property protection may somewhat reduce the attractiveness of the Chinese market for high-end and innovative security technologies. For both Brazil and Russia, the local security industries are not considered as major competitors for the EU. Nonetheless, preference for local suppliers combined with a willingness to opt for lower-cost and less sophisticated foreign solutions may mean that EU suppliers face considerable competition in these markets.

For a combination of historical and geopolitical reasons, which have resulted in strong defence ties to the US, Europe's position in security markets in Japan, Korea and Israel has traditionally fallen behind that of the USA. It does not appear, however, that this has particularly disadvantaged EU suppliers of aviation screening equipment. For electronic security products the situation is more complex, since all three countries have comparatively significant domestic capabilities (and exports). To obtain a picture of market opportunities for the EU security industry would require, therefore, a more detailed assessment for specific product types than is provided by this study. Nonetheless, notwithstanding their inherent market potential, these countries also appear to offer opportunities around technology sharing and development.

Table 2.39 Assessment of the relative attractiveness of security markets for the EU security industry

Country	Market attractiveness assessment					Comments	
	Electronic security		Video surveillance	Screening / scanning equipment	Overall	Opportunities	Challenges
	Intrusion detection	Access control					
USA	Medium	Medium	Medium	Medium	Medium	<ul style="list-style-type: none"> Large and technology-orientated market. 	<ul style="list-style-type: none"> Competitive domestic security industry; Procurement / preference for domestic suppliers; Export controls (ITAR).
Japan	Low	Low	Medium	Medium	Low-Medium	<ul style="list-style-type: none"> Priority areas: crisis/disaster (radiation detection and protection; data protection and back-up, ...); cyber security; IP-based security systems (surveillance). 	<ul style="list-style-type: none"> Competitive domestic security industry (some segments).
Israel	Low	Low	Medium	Medium	Low-Medium	<ul style="list-style-type: none"> Priority areas: transport and other critical infrastructure protection; border control; Circumvention of US export controls (ITAR). 	<ul style="list-style-type: none"> Highly competitive domestic security industry; Existing presence of global (US) competitors; US preference (may be offset by ITAR); Slow underlying market growth.
China	Medium	Medium	Medium	Low	Medium	<ul style="list-style-type: none"> Large & fast growing market; Priority areas: Urban environment, transport/critical infrastructure, key business sectors (banking & finance). 	<ul style="list-style-type: none"> Non-transparent procurement process and domestic bias; Chinese certification requirements; Export controls (US ITAR); Protection of intellectual / industrial property.
Korea	Medium	Medium	Low	Medium	Medium	<ul style="list-style-type: none"> Priority areas: physical security and cyber security products; Cooperation opportunities with local hardware suppliers (e.g. for advanced software). 	<ul style="list-style-type: none"> Competitive domestic security industry (e.g. video surveillance, information security); Competition from US (high-end) and Chinese etc. (low-end) imports; Compatibility with locally supplied equipment; Market saturation.

Market attractiveness assessment						Comments	
Country	Electronic security			Screening / scanning equipment	Overall	Opportunities	Challenges
	Intrusion detection	Access control	Video surveillance				
Russia	Medium	Medium	Medium	High	Medium-High	<ul style="list-style-type: none"> Large & fast growing market / increasing concern over security related issues (terrorism, criminality, infrastructure protection); Limited domestic industry capabilities in most security segments. 	<ul style="list-style-type: none"> Non-transparent procurement procedures; Unclear regulatory environment and uncertain investment conditions.
Brazil	Medium	Medium	High	High	High	<ul style="list-style-type: none"> Large & fast growing market (major sporting events, transport infrastructure, key business sectors (e.g. banking & finance)). 	<ul style="list-style-type: none"> Slow procurement processes; Geographical constraints; Post 2016 (Olympic games) market slowdown.

3 Alarm systems and airport screening equipment: certification and conformity assessment

3.1 Comparative overview of certification schemes around the world

In each of the country studies, the certification and conformity assessment schemes regarding alarm systems and airport screening equipment have been addressed. In this section, a comparative overview of these schemes is presented. For details we refer to the country studies in the annex.

3.1.1 Alarm systems

For the comparative overview, the existence of the following elements of the certification and conformity assessment of alarm systems are taken into account:

- Existence of standards for alarm systems;
- Existence of a Standardisation body for standards of alarm systems;
- Testing laboratories that test performance of alarm systems against standards or performance requirements;
- Existence of a Certification body that issues certificates for alarm systems;
- Existence of an Accreditation body that accredits the certifying body and testing laboratories.

Furthermore, the costs for certification and for testing are included in the comparison (where available). Additionally, we have indicated whether there is a recognition of certifications from other nations.

An overview table is provided overleaf. As one can note in the table, there are many differences in the area of certification and conformity assessment of alarm systems in the different countries. We conclude the following:

- In many countries there are certain standards for certain categories of alarm systems. However, the coverage of these standards does address different categories of alarm systems;
- In the majority of countries there are also certification bodies active in the area of alarm systems;
- In some countries there are certificates issues, but standards do not exist;
- There does not seem to be any mutual recognition of certificates or test results from other nations.

Table 3.1 Overview of certification and conformity assessment policies for alarm systems in the different countries

	Standards	Standardisation body	Testing laboratories	Certification bodies	Accreditation body	Costs	Remarks
Brazil	No	No	No	Yes	Yes	Unknown	Certification is issued to companies in the electronic security sector, including manufacturers, distributors, and service companies.
China	Yes For intruder alarms	Yes	Yes	Yes	Yes	Test: € 400-8000 Certificate: € 140 Inspection: €1,200	Applies to: <ul style="list-style-type: none"> • Detectors for intruder alarm systems; • Burglar alarm control units; • Security alarm systems for automobiles; • Safe cabinet (Box).
Israel	Yes	Yes	Unknown	Yes	Unknown	Unknown	There exist Israel standards for simple alarm systems (for example burglar alarm systems), but no standards for more complicated systems. The responsibility for the certification of systems as perimeter protection, access control, surveillance systems etc. is at the ISRAEL SECURITY AGENCY (ISA) and for the protection of public infrastructure at the ISRAELI POLICE. The certification is made in face-to-face interviews with representatives of companies who want to deliver their products.
Japan	Yes	Yes	Unknown	Yes	Yes	Unknown	A self-certification system exists that authorizes registered to efficiently support any certification request for the Japanese market.
South Korea	Unknown	Unknown	Yes	Yes	Unknown	Unknown	The certification system is in the very first stages of being introduced in Korea. It is limited to Intelligent CCTV and Biometrics. Intelligent CCTV and Biometrics are where South Korea is relatively advanced and the Korea Internet Security Agency (KISA) is running a certification system for both fields of sort. KISA certifies products/services at a Biometric Test Center. The purpose of this is to promote domestic biometric industry by certifying that products/service meet international standard. However, this is not a mandatory certification that companies have to acquire, rather it is used for marketing purpose for the companies. KISA is also in the process of introducing certification system for intelligent CCTV.

	Standards	Standardisation body	Testing laboratories	Certification bodies	Accreditation body	Costs	Remarks
Russia	Yes	Yes	Yes	Yes	Unknown	Unknown	In March 2013 the Russian Federal Government excluded alarm systems from the list of goods which are subject to mandatory certification requirements. In addition to those standards there is an extensive list of more detailed technical requirements and guidelines for alarm systems. While they are voluntary they serve as an important benchmark.
USA	No	No	No	No	No	between \$33-\$80 per year.	Alarm system products are not certified. The companies, which supervise the monitoring central stations (a company that receives the alarm signal when the security device detects an alarm event), but also the installation and the maintenance of their security systems, can be certified. Systems and service features being equal for any two competing alarm packages, the charge that the certifying body makes to an alarm company per certificate is between \$33-\$80 per year.
EU	Yes On EU level	Yes On EU level	Yes On national level	Yes On national level	Yes On national level	€ 20-75K Per national test and certificate	No common certification and conformity assessment exists. No mutual recognition of certificates.

3.1.2 *Airport screening equipment*

For airport screening equipment we have made another comparative overview that is taking into account criteria that are more applicable to this market:

- Existence of Standards for airport screening equipment;
- Existence of National testing of airport screening equipment;
- Existence of a certification or approval of airport screening equipment;
- Recognition of foreign test results of airport screening equipment.

For a number of countries, the information is not readily available. The USA has a complete testing and certification procedure and we refer to the country report for its description. This US testing and certification procedure is free of charge, while the European ECAC CEP system is not. In China, there is also a certification system in place for domestic and foreign manufacturers. Also in Japan, there are standards and certification of airport security equipment required, as in Brazil. Russia issues certificates on a voluntary level, in which there is a modest form of recognition of certificates and approvals from other nations and regions. In addition, there is national testing. South Korea relies on the certificates of the US or ECAC approvals. A comparative overview is provided in the table on the next page. Unfortunately, especially data on the costs of certification is lacking as it is not available.

Table 3.2 Overview of certification and conformity assessment policies for airport screening equipment in the different countries

	Standards	National testing	Certification or approval	Recognition of foreign test results	Costs	Remarks
Brazil	Unknown	Unknown	Yes	Unknown	Unknown	Most of the certification of airport screening equipment is done by INMETRO or an agency accredited by INMETRO.
China	Yes	Unknown	Yes	Unknown	Unknown	<ul style="list-style-type: none"> The “Regulations on the Administration of Security Check Devices” were published by the Public Security Bureau of the CIVIL AVIATION ADMINISTRATION OF CHINA (CAAC) on 6 March, 2012 (14) and sent to all local civil aviation authorities, airports and public air transport enterprises; The Regulations apply to appraisal, use licensing, installation, transformation, maintenance, inspection, regular testing and routine maintenance for civil aviation security check devices in China; Security check devices failing to get the “Use Permit for Civil Aviation Security Check Devices” are not permitted to be used. The Regulations describe the conditions for domestic and foreign manufacturers to get the “Use Permit for Civil Aviation Security Check Devices” (valid for 3 years) in a very general way; Chinese owners of civil aviation security devices have to sign agreements on installation, repair and maintenance with the manufacturers or their entrusted agents.
Israel	Yes	Unknown	Certification	Unknown	Unknown	The responsibility for the certification of systems as perimeter protection, access control, surveillance systems etc. is at the ISRAEL SECURITY AGENCY (ISA) and for the protection of public infrastructure at the ISRAELI POLICE.
Japan	Yes	Unknown	Yes	Unknown	Unknown	The Japan Security Systems Association (JSSA) provides on line an exhaustive list of standard requirements for any security equipment and constructions in Japan. JSSA is also tasked with the Recognition of Better Security System (RBSS) certification, which concerns all security equipment and systems in Japan.
South Korea	Yes	No	No	Yes	Unknown	The Ministry of Transport requires that airport operators use two items qualified by national certification; X-rays and door type screening system. Since Korea doesn't have certification for these types of equipment, the Ministry allows operators to rely on American or European ones, such as certifications by TSA, DFT, or ECAC.

	Standards	National testing	Certification or approval	Recognition of foreign test results	Costs	Remarks
Russia	Yes	Yes	Yes Voluntary	Yes In consideration	Unknown	Currently there is no mandatory certification requirements for airport screening equipment. Since 2011 the Aviation Security Certification Centre conducts voluntary certification for four types of security equipment. The certification rules stipulate that the certification body takes into account existing foreign certificates for the equipment. The cost of certification is likely to be relatively low. One factor is that leading foreign producers whose equipment has been certified in the U.S. or in the EU might feel that the voluntary Russian certification would give them little additional credibility and they are unlikely to submit their equipment for certification especially when such cost is high.
USA	Yes	Yes	Yes	No	Free of charge	100% of all security equipment presently fielded at US airports have been qualified or certified by the Transportation Security Laboratory (TSL). For the company who wants to certify its product, the cost is close to zero as the access to the Transportation Security Laboratory (TSL) is free.
EU	No No harmonized standards	Yes	Yes	No	115-305 k€	There are currently no EU-wide certification systems for security technologies. National systems differ. There exists a whole body of EU legislation which sets out performance requirements for airport screening equipment. However, this legislation does not contain the conformity assessment mechanism required to ensure that certification of screening equipment in one Member State is mutually recognised in all other Member States.

3.2 EU Certification and conformity assessment – CBA alarm systems

3.2.1 Introduction

In this section, the cost-benefit analysis (CBA) on harmonization of the certification scheme of security alarm systems is addressed. The section provides a qualitative and quantitative assessment of the baseline. The costs and benefits of the different policy options are addressed largely qualitatively and will be elaborated in the next stage of the project.

Security alarm systems include:

- intrusion and hold up alarms;
- CCTV;
- access control;
- social alarms;
- alarm transmission systems;
- combined/integrated systems.

Fire alarm systems are outside the scope of this study.

3.2.2 Baseline

There exist some European standards for security alarm systems. These are¹⁵²:

- EN 50130: Alarm systems - Electromagnetic compatibility and Environmental test methods;
- EN 50131: Alarm systems - Intrusion and hold-up systems;
- EN 50132: Alarm systems – CCTV systems;
- EN 50133: Alarm systems – Access control;
- EN 50134: Alarm systems – social alarms;
- EN 50136: Alarm systems - Alarm transmission systems.

By nature of the EN standard, after its publication, such standard must be given the status of national standard in all CEN member countries (including all EU member states), which also have the obligation to withdraw any national standards that would conflict with it.

Some certification bodies however, add additional regulation regarding quality of products on top of the EU standards. This forces manufacturers to manufacture country-specific configurations of their products which adds costs.

There is at present no common EU certification scheme for security alarm systems, nor is there any mutual recognition of national certificates of security alarm systems. This means that whenever a manufacturer wants to sell its products on the European market, he must obtain national certificates in each of the member states to demonstrate that its product meet either a European Standard or a national standards.

Actors involved in certification of security alarm systems

The main actors in the area of certification of alarm systems are:

- Manufacturers of security alarm systems. Examples are Bosch, Siemens or Tyco;
- Certification bodies. National accredited organisations that issue certificates on conformity of products with national or European standards. These certificates are issued based on a testing report from a testing laboratory. There may be several certification bodies for security alarm systems in member states;

¹⁵² www.cenelec.eu.

- Testing laboratories. National accredited laboratories that test products on their performance according to national or European standards. They issue a test report. There may be several testing laboratories for security alarm systems in member states;
- National accreditation body: officially recognised body by national Governments to assess and verify—against international standards—organisations that carry out evaluation services such as certification, verification, inspection, testing and calibration.

In some countries, the testing laboratory and certification body is the same organisation.

The current process towards certification

The steps of the typical procedure between having a developed product and to have it certified in Europe are described in the table below. This excludes the initiatives from the market that are discussed below (CertAlarm and EFSG).

Table 3.3 Procedure for testing the alarm systems

No	Description	Actors involved
1	A manufacturer develops a new type of alarm system that is intended for the European market. This needs to comply with existing EN standards or national standards.	Manufacturer
2	In order to demonstrate conformity with the EN standards or national standards, the manufacturer submits its product to a testing laboratory in an EU member state for such testing. Documentation must be provided in the local language.	Manufacturer Testing laboratory
3	The testing laboratory issues a test report in which conformity with the EN standards or national standards is assessed. The testing laboratory may ask questions for clarification that must be addressed by the manufacturer.	Manufacturer Testing laboratory
4	The manufacturer sends the test report to a national certification body and asks for a certificate. This certificate is valid for this specific member state. Steps 2-4 may take half a year to a year.	Manufacturer Certification body
5	The manufacturer brings his product to the specific national market.	Manufacturer
6	In case the manufacturer wants to enter a national market in another member state, steps 2-5 need to be repeated.	Manufacturer

According to Euralarm, it takes the Industry on average 2 to 3 years to complete the full European approval process.

Initiatives in the market: Certalarm and EFSG

In addition to the generic process described above, there are two initiatives that are relevant to discuss. These are the CertAlarm certification scheme and the European Fire and Security Group.

The private **CertAlarm** is an industry initiative to provide a European-wide scheme for certification of traditional security products. CertAlarm is to date focussed on fire protection and detection systems intrusion and hold-up alarm system components¹⁵³ and alarm transmission systems and components¹⁵⁴, the latter falling within the security alarm system scope of this CBA task. To date, CertAlarm published 100 certificates, of which around 50 apply to alarm systems. CertAlarm has 15 registered manufacturers. The major drawback of the system is that it is privately run, and that Member State authorities have no obligation to accept certificates established under the scheme.

¹⁵³ Using EN50131 series standards.

¹⁵⁴ Using EN50136 series standards.

Industry indicates that they use this system as it is a first step towards elimination of national standards and an EU wide certification system. It is their hope that it will become a common mark, but this is about market acceptance. It is their view that the market still needs to be educated on the benefits of the system. Many of their customers, being local installation companies have never heard about the scheme. Furthermore, they are certified themselves on the basis that they use nationally certified products, which hampers acceptance of a product with a Certalarm certificate.

Another initiative worthwhile to note is the **European Fire and Security Group (EFSG)**. The members of EFSG are established certification bodies who work together with associated testing laboratories. Four certification bodies¹⁵⁵ and three testing laboratories¹⁵⁶ concluded an agreement on the components of *intruder alarm systems*^{157 158}. The object of this agreement is on the mutual recognition of test results to make it easier for manufacturers to obtain authorisation to use the mark of each Certification Body. To achieve this, test results as specified in the agreement, will be considered to be acceptable for all certification bodies within this basic agreement. The scope of the agreement encompasses six sub-standards of EN 50131. It should be noted that by far not all tests for each of six substandards are mutually recognised. For these tests, the certification body is free to accept or not to accept results from the test laboratory in question.

EFSG arrangements between members help manufacturers to obtain certification from more than one certification body use the related quality marks without duplication of testing. The level of acceptance of tests is dependent on the specific content of the relevant EFSG agreement. Where full agreement by all participating EFSG members is reached there is acceptance of all test results.

Manufacturers are free to select their certifier of choice. The process of testing and certification is in effect controlled by that single certifier. To achieve multiple certification it is necessary to have a contractual arrangement with each EFSG member whose approval is sought. This can be facilitated for the manufacturer by the certification body of choice. However, when multiple certifications are required the manufacturer must have a contractual arrangement with each EFSG member whose approval is sought. This ensures that an obligation is undertaken with each certifier to abide by the certification rules, particularly with respect to making sure the approved products continue to be built to the same standard of quality in the future. The basic EFSG process is depicted in the following graph.

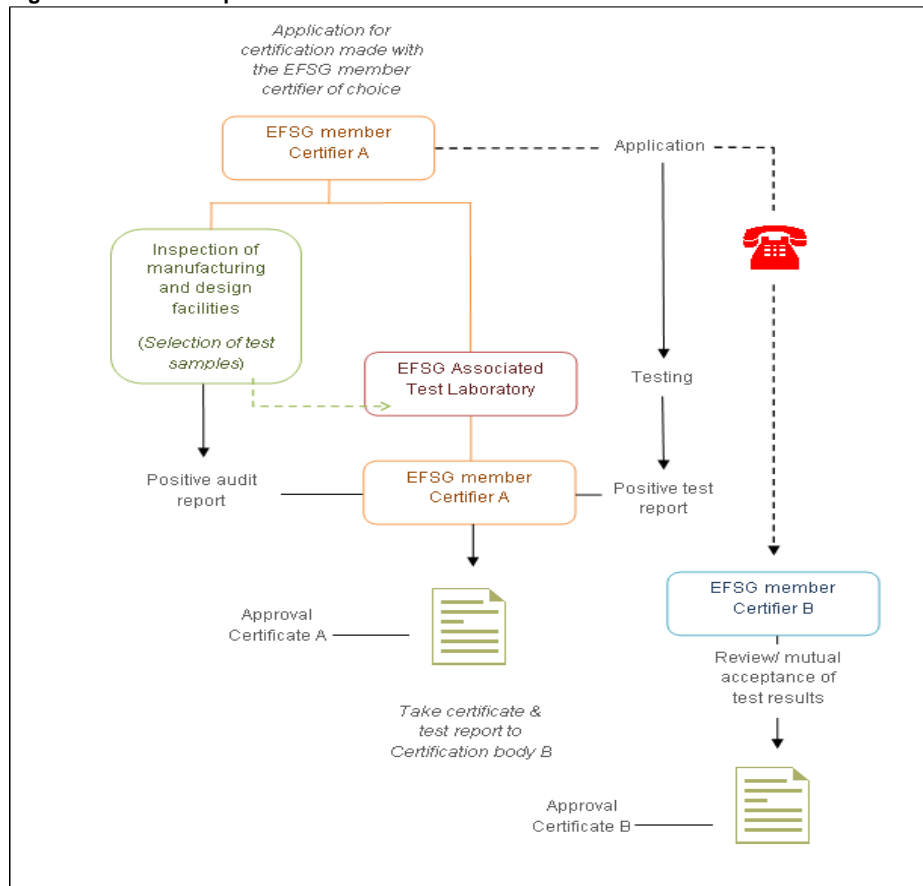
¹⁵⁵ AFNOR (F), CNPP (F), VDS (DE), LPCB (UK).

¹⁵⁶ CNPP (F), VDS (DE), BRE (UK).

¹⁵⁷ http://www.efsg.org/images/pdf/BA_IAS_November-2010.pdf.

¹⁵⁸ There have been concluded agreements on high security locks, safes and strong rooms and fire detection and fire alarm components as well. These fall outside the scope of this alarm systems definition of this study.

Figure 3.1 The EFSG process



Source: EFSG.

Evidence of compliance of a product (or system) to the specified standard(s) shall be based on the testing of samples selected by the EFSG member certifier and tested by an associated EFSG test laboratory (i.e. a test laboratory nominated by at least one EFSG member certifier and that has signed the respective EFSG agreement). Upon completion of the testing, reports will be provided to the relevant certification bodies (also party to the signed EFSG agreement). The certifier(s) will review the results and if the test results and the findings of the factory inspection are acceptable approval will be granted. Where appropriate the certificate(s) of registration shall be made available to other EFSG members who have been asked to accept the results of the assessments as part of their own certification procedure. Upon successful completion of the certification process the manufacturer receives approval certificates from each certifier involved.

Feedback from the industry on the above description of the EFSG process is in some cases it seems that the actual duration of obtaining the five certificates in the different EFSG countries via the EFSG route takes longer than obtaining a certificate in the traditional way, via different testing procedures. The discussion between EFSG members to arrive at an acceptance of each others work is said to be the cause. In some cases, the EFSG members do not accept each others work, and one would need to go via the traditional certification approach again.

The impacts of the current certification process

The current certification process for alarm system affects the various stakeholders involved in different ways. Some stakeholders incur negative impacts, while others clearly benefit from the current situation. Below we describe the impacts for the main stakeholders.

Manufacturing industry

The manufacturing industry of alarm systems is generally negatively impacted by the existing certification process in Europe. It incurs **additional costs** to obtain different certificates in the EU member states, which asks for duplication of product testing. The EFSG initiative offers an opportunity to save costs for testing, but as long as the EFSG procedure takes more time in some cases than the traditional testing procedure, it will not be attractive for manufacturers.

A major manufacturer of alarm systems indicates that in terms of direct costs associated with the current certification process, the following applies. This manufacturer employs two staff members that are full time employed with applying for national certification. The manufacturer has some 200 certificates, which need to be 'refreshed' every four years (which is shorter than the life cycle of the majority of the products). Including new products, they obtain on average some 5-10 certificates per year. The direct out-of-pocket costs for obtaining a certificate amounts to:

€ 20-25K for a single detector

€ 50-75K for a panel

This may thus easily add up to € 350- 500 K per year for a single manufacturer. This does not include the internal costs for the company.

The current certification process impacts **the time to market** of products in Europe. Euralarm indicates it takes on average 2-3 years to have a product certified across Europe, while a single certification takes some 10 months. This especially affects manufacturers of products at the high end of the innovation rate, such as CCTV cameras, where the innovation in the products makes the sales. Industry indicates that being too late with your product on the market means no sales.

A large manufacturer has indicatively quantified the costs of a delayed time to market. New products are brought on the market obviously to increase revenue but sometimes also to reduce production costs for a model. A broad estimate is that they currently incur some € 2.2 million per new product introduction for which they incur a 1 – 1.5 year of delay, due the fact that national certificates must be obtained. A rough indication is that 30% of this amount on average consists of lost savings in the production process and 70% on lost revenues. However, it is also acknowledged that in some cases a delayed revenue generation does not mean a lost revenue generation. The sales may just be incurred later. In the CBA, we will take into account the impact that a reduced time to market has on missed cost savings in the production process only as a conservative estimate.

The current certification process also forces manufacturers to develop local variants of products to comply with additional requirement on top of the EN standards. This increases the **costs of production**.

Finally, the current certification process **hampers innovation** of alarm systems by SMEs. While major manufacturers have the internal infrastructure to apply for national certification in Europe, the smaller manufacturers do not have this. Some of these smaller manufacturers take the decision not to export to the entire EU, but limit their market to their home market. This implies that when deciding to invest in product innovation, they sometimes take into account only a small home market, which may affect the innovation investment decision negatively.

Certification bodies and testing laboratories

Under the current situation, manufacturers of alarm systems need to apply for certification locally. This means that for each national certificate the manufacturer will pay the certification body a fee for certifying its product. As such, the certification bodies **generate revenues** from the certification of alarm systems.

The same applies for testing laboratories. National testing of alarm products means that the different testing laboratories **generate revenues** from testing the alarm systems in their different facilities. Additionally, testing laboratories **incur alignment costs** as a result from the EFSG process. In this process, they need to discuss with other testing houses on the mutual acceptance of testing methodologies and test results.

Users

Users buy (either directly or indirectly) and use the alarm systems. In many cases one is mandated to buy alarm systems with a national certificate. This mandate can be done by insurers or for example by tenderers for construction work that demand in their tender dossier that an alarm system with a national certificate is installed. As the current system adds costs for manufacturers, the consequence is that **users pay more** for the alarm systems, as one may assume that the costs increase is included in the final sales price of the system.

3.2.3 Quantifying the baseline

Direct impact

EURALARM, the industry association of manufacturers of alarm systems indicated that an estimated budget for approval submissions (from a major manufacturer / distributor) is around €2 million per year. This is further seen to have about a 33.3% split on approval renewals and 66.7% on new product submissions. They estimate that major manufacturers might represent around 8% of the European electronic Fire & security market product submissions. This implies that on an annual basis the costs for approval submissions amounts to around €25 million (8% represents €2.0 million, hence 100% represents 25 million). It should be noted that this value includes fire alarms. Fire alarms take-up some one-third of the market, hence an overall value of for the costs of approval submissions of around €17 million results, leaving fire alarms out of the analysis.

A large manufacturer confirms that on an annual basis the direct out of pocket costs for national approvals of new products is more significant. Generally speaking there are 9-10 countries in the EU that do not just accept a single conformity assessment to the EN standard, but require additional testing or have deviating requirements. This may add up from additional costs of €35-60k per product per country. Taking the lower bound of that bandwidth, and acknowledging that there are four countries in the set of 10 that do recognize the test results, an estimate is that on an annual basis this manufacturer spends around €270k for a single product on obtaining national approvals in the EU. Their estimate is that this is spent at least for 20 products per year, hence the costs add up to €5.4 million per year, that could be saved with a common European conformity assessment and certification scheme for alarm systems. This would assume that there are no national requirements anymore in place on top of or instead of the EN standards. This figure excludes hours spent by the employees of these manufacturer to coordinate the national testing and approval. Taking into account the market share of this manufacturer, a value of around €60 million per year arises for the entire market.

In the SECERCA study¹⁵⁹, the total costs for certification and conformity assessment of intruder alarm systems is estimated to range between €6.2 million and €13.2 million per year. The lower

¹⁵⁹ Ecorys, 2011, Security Regulation, Conformity Assessment & Certification

end of the range was estimated 'bottom-up' industry based on the certification costs for a single country extrapolated with a GDP share. The high end of the range was an estimate, based on earlier studies on the impact of the New Legislative Framework, where it was not entirely clear what was included in the costs figures for certification. Clearly, the total impact of the alarm systems industry would be higher, as the market is broader than intruder alarm systems only. The market for intruder alarm systems was valued at € 1.1 billion in SECERCA, while the market for physical security protection, including applications such as closed circuit TV (CCTV), access control, intrusion and fire detection, is ranging from €10bn to €15bn. As such, the intruder alarms only take some 10% of the total European market for security products. Assuming costs for certification and conformity assessment is more or less similar for intruder alarms as for other alarm systems, then the total annual costs associated with certification and conformity assessment of alarm systems amounts to €62-132 million (excluding fire alarm systems), or €41-88 million excluding fire alarms.

For the CBA, it is proposed to work with the range of costs from the industry estimates. This would mean an annual costs of € 17– 60 million for the certification and conformity assessment of alarm systems in Europe (including fire alarms).

Indirect impact

As indicated above, more substantial costs are incurred by manufacturers resulting from a delayed time to market. This implies that they are hampered to implement cost reduction processes in their production stemming from a new product line. From our interview programme, it was made clear that this could be conservatively estimated as around €660K per new product. We conservatively estimate this as around €60-80 million for the entire market. Note that this excludes delayed revenues from the long time to market, as these revenues may be generated (in part or in full) a year later.

Survey results

The European Commission launched a digital survey on further regulation of alarm systems among stakeholders. The majority of respondents to this survey expressed that the current situation without a harmonised certification system for alarm systems and system components has a negative effect on:

- Ensuring the best security for the European citizens;
- The efficiency of the certification process;
- Research and development costs;
- Commercialisation costs;
- The time to market of products and systems;
- Training of services personnel;
- Global competitiveness of EU companies.

The majority of respondents from industry that expressed opinion indicate that the lack of harmonised certification systems for alarm systems and system components in the EU has an impact of up to 25% on their research and development costs and commercialisation costs. The industry respondents also indicate that the availability of test laboratories and time to test appointment is inadequate, and that it is important to be able to choose test laboratory. The majority of respondents also indicate that test laboratories should be accredited on an EU level and that test laboratories should be regularly audited. Also, the majority of industry respondents consider the availability of limited pre-tests important in order to support manufacturers on the development and tuning of equipment. Finally, the large majority of industry respondents indicates that they have to subject a particular alarm system or a single system component twelve times to a certification /conformity assessment in order to market it in other EU Member States, and some respondents indicate even that they have to do this 27 times. They also have to modify/adapt a particular alarm

system or a single system component twelve times (majority) or even more than 27 times (one respondent) to comply with performance requirements in other EU Member States.

3.2.4 Policy options

The Commission has developed a set of alternative policy options in addition to the baseline option as detailed above. These are:

- 2. "Recommendation" – The Commission would issue a recommendation to Member States to mutually accept each other's national certification systems or to rely on the industry-led certification mechanism, provided that EU laboratories undertaking performance testing respect certain requirements. The aim of this recommendation would be to enable a producer of an alarm system to have his product certified only once in a single Member State in order to sell it in all Member States;
- 3. "Legislation" - The Commission would propose legislation on System/product certification and compliance testing principles. It would also specify areas/products/... for which standards need to be developed. The legislation would be elaborated jointly with regulators, industry representatives and certifiers alike. The aim of this legislation would be the same as for the recommendation, but implemented through a legally binding act of EU legislation. Two different variations of this legislation would be considered:
 - 3.1. The "directive-based approach", is characterised by a set of detailed specifications which are laid out in the directive itself. This approach is based on the so called "old approach", which usually targets specific technologies and not general areas. Automotive, chemicals and pharmaceuticals are examples of fields in which it is applied. Within this approach, certification would be based on certification by a governmental authority;
 - 3.2. The "standards-based approach" is not based on specifications as detailed as under the directive-based approach. This approach is based on the so called "new approach", which focuses on essential requirements written in general terms. Product legislation is restricted to the requirements necessary to protect the public goals of health, safety and security. The technical specifications under the standards-based approach are elaborated by the responsible European Standardisation Organisations (CEN/CENELEC and ETSI). Within this approach, certification would be based either on a third party certification or on a self-certification.

Costs of the policy options

Option 2

The costs for implementing option 2 is considered fairly limited compared to the baseline. The only costs that would be incurred from the Recommendation are the costs for assessing whether the testing laboratories in the EU undertake performance testing according to requirements. This would be a one-off cost to develop the assessment methodology, and annual recurrent costs to verify whether the laboratories worth according to the requirements. The policy option is unclear in terms of which entity would be responsible for the assessment of the testing houses.

Option 3.1

The costs for implementing option 3.1 would stem from the establishment of certification capacity in the governmental authority that would become responsible for certification under this option. However, the major advantage of this option is that approval and certification now needs only to be done once for the entire EU-28, while in the current situation it is clear that in at least 10 countries different approval and certification procedures are undertaken. On a balance it may thus be expected that this option 3.1 results in a cost reduction **for authorities**.

In addition, the option would also lead to an avoidance of duplication of testing of alarm system products. Again, under this option it would be necessary to test once if the product is conform the specifications in the directive. This implies **reduced revenues for testing houses**.

Option 3.2

The costs for implementing option 3.2 would stem from additional standards development by the **European Standardisation Organisations** (compared to their effort in the baseline). For firms, also the alternative – an equivalent standard – could be costly, since the burden of proof for equivalence to the EU standard falls on the firm. Furthermore, the costs would be in establishing assessment capacity at European level that needs to verify whether the third party certification or the self certification processes are working according to the requirements. These costs would also **accrue to firms** in the end. As there are already experienced third party certifiers that certify alarm systems, the additional costs incurred by these entities are assumed to be zero.

Costs for **authorities** currently involved in the approval and certification process is likely to decrease, as this involvement is no longer required.

In addition, the option would also lead to an avoidance of duplication of testing of alarm system products. Again, there would under this option be the necessity to test once if the product is conform the specifications in the directive. This implies **reduced revenues for testing houses**.

Benefits of the policy options

The benefits of option 2 are considered to be limited. It is questionable, confirmed by interviews with industry, whether the voluntary character of the option leads to mutual acceptance of certificates or to the acceptance of the Certalarm initiative. After all, this would be possible already, and it does not happen. Users or insurers are currently still demanding national certified products. If the Recommendation would not lead to mutual recognition of recognition of the industry initiative, benefits of this option would be nil. This is confirmed by the survey under stakeholders carried out by the European Commission.

The benefits of option 3 are described below.

Direct benefits

The benefits of option 3 are more apparent. The legislation would take away the current main problem of multiple testing and certification. As such, it would lead to a reduction of costs for industry. Industry estimates that a saving of 83% of the baseline costs for certification and conformity assessment could be saved under this option. The Secerca study estimated that 75% of the costs could be saved. Applying the average of this bandwidth to the baseline costs range of €17- 60, then the potential costs savings of this option would be around € 14-48 million per annum. These costs savings accrue to **manufacturers**.

This would further allow for **production efficiencies**, as manufacturers would no longer need to amend products to national regulations. The survey of the European Commission under stakeholders indicated that the majority of manufacturers has to amend their products 12 times for this reason.

Indirect benefits

However, the option would also imply that:

- Manufacturers are able to sell their products faster on the entire European market, as the 'one-stop-shop' for EU testing and certification takes away a lengthy process to go through in each of the member states;

- Manufacturers would be able to use the certificates as an EU mark, which is a selling point in the market outside Europe. During the interviews, manufacturers indicated this to be important for markets such as Middle East / North Africa (MENA) and Latin-America. However, it should be noted that also non-European manufacturers are able to obtain their EU certificate and use it as a market instrument. It is not possible to quantify this impact;
- Smaller manufacturers would get access to a larger market, as they don't have to go through multiple testing and certification, which does prevent them to export from their own country in the baseline. This means that they could take different investment decisions for innovation projects, which affects the innovation rate positively in the industry;
- There would arise competition under certification bodies and testing laboratories. This would decrease costs for certification and testing.

Euralarm estimates the impact of a faster time to market as follows. The current European forecast shows a decline of Global market share of 5% by 2020 and it is estimated that if the Fire & Security industry could introduce new products faster by the effective working of a single pan-European certification scheme - that this decline could be halved to 2.5%. In other words, there would be a lower decrease of about 2.5% of the market which has been identified as € 16.4 billion. Therefore the increase would be € 0.41 billion (69% Security / 31% Fire Safety), which is € 0.28 billion for the alarm systems segment only for the next seven years, i.e. some € 40 million per year.

A major manufacturer indicated that a reduced time to market could enable the implementation of costs savings in the production process, see above in 3.2.3. It was estimated that this could imply a potential cost saving of around €60-80 million per year.

In the CBA we therefore include a total range of €40-€80 million of potential benefits from a reduced time to market. These may likely be passed on to end users to a large extent.

From our interviews, manufacturers indicate that they would expect the benefits to be in the same order of magnitude for option 3.1 and 3.2. However, option 3.2 would be building on the standardisation effort from the past 20 years, so it would be most logic to connect to.

Survey results

Although our interview programme under manufacturers did not provide indications that the magnitude of the benefits as addressed above differs significantly between suboption 3.1 and 3.2, the survey carried out by the European Commission under stakeholders (broader than industry) provides a picture that impacts might differ between these suboptions. The majority of respondents indicate that option 3.2 provides a slightly larger potential, compared by option 3.1, to:

- the level of security for citizens;
- the clarity for citizens in terms of insurance coverage;
- the time to market;
- training of services personnel;
- competitiveness of EU companies;
- insurance companies;
- certification bodies;
- testing laboratories.

Conclusion

In the sections above, the various costs and benefits of the policy options in comparison with the baseline have been addressed. These are summarised in the tables below.

Table 3.4 Comparison of costs and benefits for options (compared to baseline)

	Option 1 (baseline)	Option 2	Option 3.1	Option 3.2
Impacts for Industry				
Reduction of costs for certification and conformity assessment	0	0	14-48 M€ p.a.	14-48 M€ p.a.
Efficiencies in production	0	0	+	+
Reduced time to market	0	0	40- 80M€ p.a.	40- 80M€ p.a.
Improved competitive position on non-EU market	0	0	+	+
Impacts for authorities				
Reduced costs for issuing certificates	0	0	+	+
Impacts for testing laboratories (TL)				
Verification costs of TLs work	0	-	0	0
Reduced revenues	0	0	-	-
Impacts for Eur. Standardisation Organisations				
Costs for standards development	0	0	0	-
Impacts for end users				
Reduced product price	0	0	+	+

+ = positive impact, - = negative impact compared to baseline.

On a balance, option 3 is favourable over option 2. Due to the voluntary character of option 2, it is doubtful if this leads to any benefits while one would need to make costs for the option. The option 3 brings significant direct and indirect benefits which may be above €100 million per year, plus a number of unquantifiable benefits as an improved competitive position on the market outside the EU. It is also likely that the option will have a positive impact on the price of alarm systems from the users perspective. The distinction between option 3.1. and 3.2 would stem from the costs of the option. However, these also seem to be largely similar. The advantage of option 3.2 would be that the costs burden of the option would be on the manufacturer (either via self-certification or via third party certification), while in 3.1 there would still be a government authority involved. The downside of option 3.2. is that the ESO need to make more costs for further standard development. However, it would connect most to the 20 year positive experience from standard development on European level, and it allows for further rolling out the EU standard to international (outside EU) level (IEC), which could positively affect European products. The survey under stakeholders indicates that stakeholders expect a slightly higher impact from option 3.2 compared to 3.1. as well.

3.3 EU Certification and conformity assessment – CBA airport screening equipment

In this section, the cost-benefit analysis (CBA) on harmonization of the certification scheme of security alarm systems is addressed. The section provides a qualitative and quantitative assessment of the baseline.

3.3.1 Baseline scenario

Existing process for airport screening equipment

There is currently no EU-wide certification system for airport screening security technologies.

The EU legislation sets out requirements for airport screening equipment. For LEDS, the Regulation 185/2010 (annex paragraph 12.7.3) provides for the mutual recognition of the test results by all Member States. There is a lack of harmonised standards and of a legally binding conformity assessment of airport screening equipment at EU level.

The European Civil Aviation Conference (ECAC)¹⁶⁰ set up the Common Evaluation Process of security equipment (or CEP). This is the central system in the EU for the testing of airport screening equipment towards ECAC standards ECAC CEP applies only to Explosive Detection Systems, Liquid Explosive Detection Systems, and security scanners. ECAC-CEP system is voluntary. ECAC provides reports to manufacturers indicating if they passed or not the relevant test. If a piece of equipment passes the test, ECAC reports so to the ECAC 44 member states and on their website. Approvals or certificates can only be given by member states. The test laboratories of the CEP system are not subject to a harmonised accreditation system under EU legislation. There are six ECAC- CEP test laboratories specialised in testing of specific types of security equipment. The respective test centres selected for specific technologies are located in the following countries:

- Explosive Detection Systems (EDS): DE, NL, FR, UK;
- Security Scanners (SSc): DE, NL, ES, UK;
- Liquid Explosive Detection Systems (LEDS): DE, NL, CH;
- Explosive Trace Detection (ETD): drafted;
- Advance Cabin Baggage X-Ray Systems (ACBS): study group.

Below we will further elaborate on the ECAC CEP.

ECAC-CEP

The ECAC Common Evaluation Process of Security Equipment (CEP) applies to Explosive Detection Systems (EDS), Liquid Explosive Detection System (LEDS), and security scanners.

Laboratory tests of EDS, LEDS and security scanners are conducted at various Participating Test Centres located in ECAC Member States with the objective of determining whether the tested equipment meets the required EU performance standards adopted by the Commission under laboratory conditions.

The CEP Management Group, which consists of national authorities contributing to the Process, analyses the test reports provided by the Participating Test Centres; where the equipment is evaluated as meeting an EU performance standard, the test reports are communicated to the ECAC Member States signatories to the CEP Administrative Arrangements. All forty-four ECAC Member States are signatories to these Arrangements.

The following sections provide information on the Explosive Detection Systems, the Liquid Explosive Detection Systems and the security scanners that were evaluated as meeting an ECAC performance standard. Please note that the evaluation made and the performance standard attributed is valid only for the configuration(s) of the equipment indicated in the table.

¹⁶⁰ ECAC has 44 members: all the EU Member States as well as Croatia, Iceland, Norway, Switzerland, Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Macedonia, Moldova, Monaco, Montenegro, San Marino, Serbia, Turkey, Ukraine.

Note: This evaluation does not constitute an approval or certification of the equipment by ECAC. Approval or certification of equipment remains the responsibility of the Appropriate Authority for aviation security in each ECAC Member State.

The ECAC Organization covers 44 countries: All of the 27 EU Member States complemented by Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, Georgia, Iceland, Macedonia, Moldavia, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, Turkey and Ukraine.

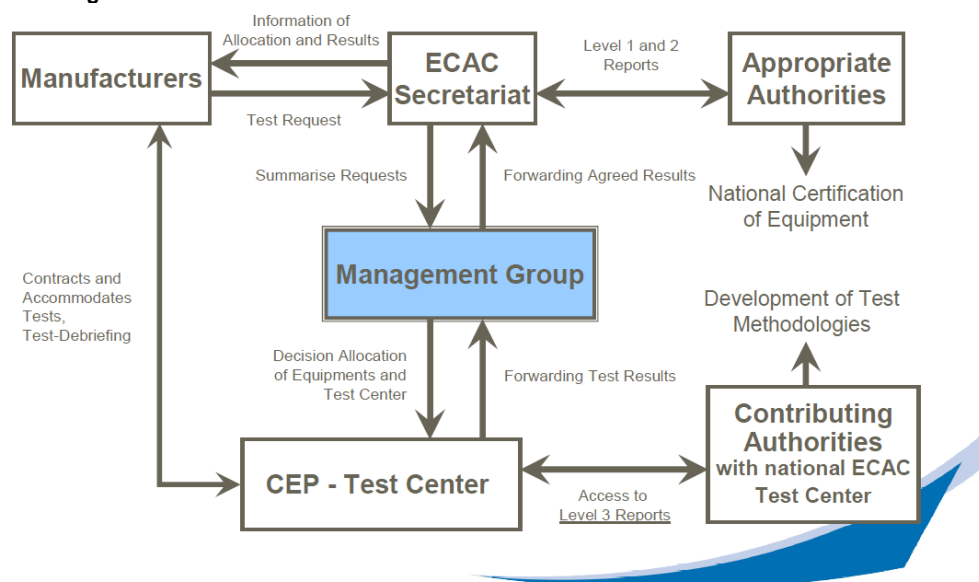
With this 44 countries there is a very good coverage of ECAC in Europe.

ECAC develops Common Test Methodologies (CTM's) as part of the CEP process. ECAC Study Groups (SG) are composed of, and chaired by, National Experts on technical level from ECAC Member States. Their tasks are as follows:

- Development of detailed Testing Requirements (Test Agenda / Test Volume);
- Definition of Threats (Type of Explosives, amounts, mixtures ratios, object shape/size);
- Definition of False Alarm Objects and Concealments;
- Evaluation Methods (counting of alarms, false alarms etc.);
- Types, numbers and contents of test objects (e.g. bags);
- Definition of a detailed run list;
- Formulas for calculation;
- Preparation of a Pilot Test to prove draft CTMs;
- Regulation of Simulator Re-Test;
- Reporting.

The steps of the overall ECAC-CEP are described in detail below while its organisation is presented in Figure 3.2.

Figure 3.2 Organisation of ECAC-CEP



Source: Federal Police Department / Federal Police Technology Centre

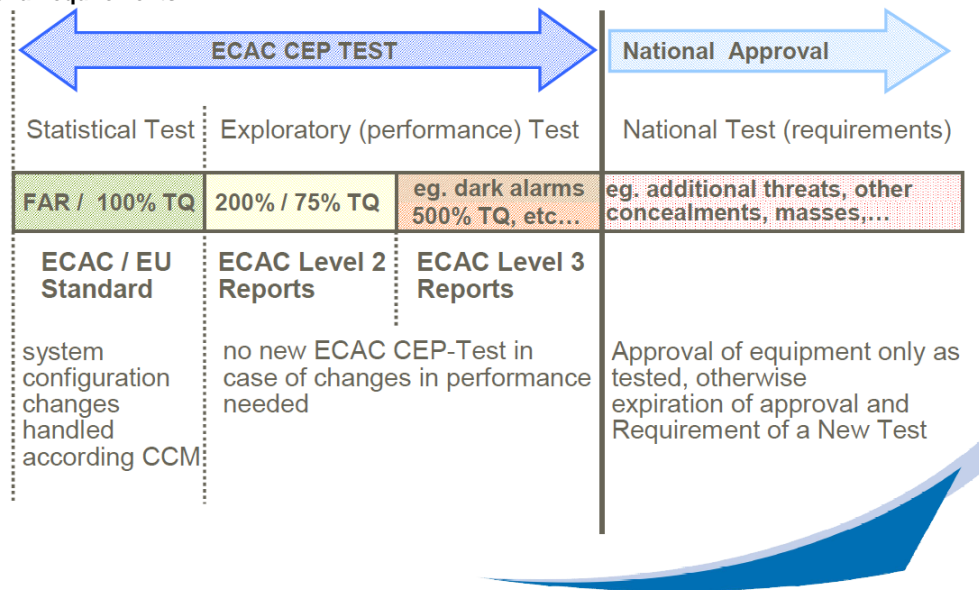
The steps of the typical procedure between having a developed product and putting it on the market are described in the next table.

Table 3.5 Procedure for testing the airport security equipment

No	Description	Actors involved
1	A manufacturer develops new type of equipment that is intended for the European market.	Manufacturer
2	Before submitting the equipment for ECAC-CEP tests to the CEP test laboratories, manufacturers often invest in "private testing". This is done in order to check the performance of the equipment and possibly improve it before the ECAC-CEP testing.	Manufacturer Private testing entity
3	The private testing entity informs the manufacturer on the performance of the equipment and whether its needs further improvement or alterations to ensure its performance levels are repeatable and reliable.	Manufacturer Private testing entity
4	When the manufacturer alters the equipment or when the product's performance is repeatable, the manufacturer contacts the ECAC Secretariat and asks for the allocation to a CEP-Test laboratory and a time slot.	Manufacturer ECAC Secretariat
5	The ECAC Secretariat contacts the ECAC Management Group.	ECAC Secretariat ECAC Management Group
6	The ECAC Management Group contacts an ECAC-CEP laboratory and provides the ECAC Secretariat with an answer. ECAC CEP meets four times /year to allocate time slots and test centres for tests	ECAC Management Group ECAC-CEP test laboratory
7	The ECAC Secretariat informs the manufacturer on the time slot and the test centre allocation – in practice there are a number of time slots a year. This is done in order to reduce the costs from the test laboratories to the manufacturer related to the materials used for testing and to test similar equipment in batches.	ECAC Secretariat Manufacturer
8	When the right time comes, the manufacturer transports and submits its new equipment to the specific ECAC-CEP test centre for a performance test.	Manufacturer ECAC-CEP test laboratory
9	The dedicated ECAC-CEP Test Centre conducts the tests. During the test period, the ECAC-CEP Test Centre can contact the manufacturer and ask him for additional information, for assistance, for visits to the ECAC-CEP Test Laboratory, etc. The ECAC-CEP Test laboratory uses the established procedures, performance levels and standards in place. These are partly known to the manufacturers, partly classified. Manufacturers may require access to the detection requirement standards from their member state authorities. The actual ECAC Test Protocols are not disclosed. ECAC does provide however an information note on how the test is done in more general terms.	ECAC-CEP test laboratory Manufacturer
10	After the testing is completed, the ECAC-CEP test laboratory develops reports. First of all, the ECAC-CEP test laboratory provides the manufacturer with a report which includes only the outcome of the test (statistical test). This is done based on the EU standard/requirements. Are the results positive and the new equipment passes the tests, on its website ECAC publishes the manufacturers name and the type of equipment that passed the test. It does not, however, inform the public about any negative results or the number of times the equipment did not pass the tests before	ECAC-CEP test laboratory Manufacturer National Authority 4 founder countries financing the ECAC-CEP scheme

No	Description	Actors involved
	getting an approval. ECAC-CEP produces also a report that is provided to national authorities responsible for conducting of national certification of equipment. Finally, a report is distributed to the 4 founder countries financing the ECAC-CEP scheme.	
11	After passing the ECAC-CEP tests, the manufacturer receives an announcement that equipment meets ECAC performance standards. For an airport intending to install manufacturer's equipment it has to send a request to its Appropriate National Authority for aviation security. In this request are to be named model and type of the equipment as well as the desired location(s) for installation. In case the airport wishes to deploy this equipment at additional locations new request(s) have to be submitted. (It should be noted that the certification process is handled differently by different member states and the procedure as described above might vary.	Manufacturer User National Authority
12	Not all European countries accept the ECAC system based on European requirements. Some countries may add national requirements on top of the European performance requirements. If a country has additional requirements on top, the manufacturer needs to submit its equipment to conduct an additional national test. If the equipment and its software already passed the ECAC-CEP tests, only additional test needs to be done. If, however, the equipment has new software, the manufacturer has to submit its equipment for a completely new test and go through the whole process again.	Manufacturer ECAC-CEP test laboratory National Authority

Figure 3.3 Tests and reporting levels against the European minimum requirements and additional national requirements



Source: Federal Police Department / Federal Police Technology Centre

The ERNCIP-AVSEC working group on “Inventory of procedures for approval employed in the EU for aviation security detection equipment” launched a questionnaire addressed to all Member States and EFTA (AVSEC Regulatory Committee). Responses were received from 24 EU + 3 EFTA authorities. The conclusions from the preliminary outcomes are as follows:

- Issuing product certificates: 18 countries have a procedure in place but only four countries issue product certificates. Approvals or certificates are issued mainly for EDS, LEDS and SSc (ECAC CEP today only applies to EDS, LEDS and SSc) but also for WTMD, HHMD and EDD and in a few cases for chemical reaction strips, ETD and Xray equipment. The most commonly used criterion for obtaining approval or certificate is the successful passing of the ECAC CEP. However, four countries require additional criteria based on the ECAC CEP level 2 and 3 reports and one country is considering doing so. These requirements are purely technical and are not 'more stringent measures in legal context. Thus, in practice not all equipment that has passed ECAC CEP can be approved;
- Process for approval/certification: Eight countries issuing certificates or approvals reported that the approval/certification scheme is described in the NCASP and five in national legislation. One country reported it is not described in official documents and one had the process included in both national legislation and the security programme. One country reports that the authority itself carries out the procurement of equipment, so there is no need for a process of approval or certification;
- Information to manufacturers and Member States: The majority of the countries having approval or certification procedures in place inform the manufacturers and vendors directly or via legal documents. However, no country reports informing other Member States. In ten countries out of the 18 the authority informs entities in charge of procurement by letter, legislative documents or by placing information on dedicated websites;
- Responsibility for procurement of equipment: Procurement of equipment for passenger screening check points and hold baggage are typically handled by airports while for inflight supplies and cargo it is sometimes handled by a regulated agent. Only two countries report that procurement is handled exclusively by authorities;
- Requested approval(s)/certificate(s)/information for procurement: Most respondents apply several performance criteria for eligible tenders. The most common requirements are 'Passed ECAC CEP' (20) and 'Complies with EU Regulation' (20), in combination chosen by 16 respondents. Out of those 16, four have additionally ticked 'TSA approved' and eight 'Used by other Member State(s)'. It is also noted that 'Passed ECAC CEP' only applies to EDS, LEDS and SSc equipment;
- On-site acceptance tests: On-site acceptance tests are required by the appropriate authorities in 11 countries;
- On-site maintenance: The majority of respondents named airport operators and the operators of equipment (including regulated agents) as responsible for maintenance and service;
- On-site routine testing: The airport operator is normally responsible for the routine testing. However, about half of the respondents assign the responsibility also to regulated agent. 19 respondents specified that daily tests are performed; only one country does not perform daily tests, while 12 respondents specified that routine tests are additionally carried out before equipment is taken into operational use, for example when switched on;
- Sensitivity settings procedures: Mainly two entities are responsible for adjusting sensitivity settings of equipment: the airport operators and the appropriate authorities. In 19 countries sensitivity settings may be adjusted to threat level.

Three product lines and data needs

For various types of technologies used for airport security screening, the related procedures, standards, regulation are at different stages of development and implementation. The aviation security screening equipment and technologies can be divided into three groups according to the

level of maturity and implementation of the procedures, standards, regulation. For the working purposes, we will call them three product lines. These can be defined as follows:

For some technologies, the relevant assessment methods and procedures are developed and well established, while the standards and performance levels are well known. An example can be the Hold Baggage Screening Equipment (EDS or commonly known as x-ray machines) that have been in operation for many years now. EDS = Explosives Detection System - equipment used for screening of hold baggage (=check-in baggage). Today it is exclusively X-ray based.

For other technologies, the standards are being developed during the development of the technologies or after that. In such cases, the equipment often needs to be revised and adjusted to the newly developed standards. An example of such a process can be found in the development of the Liquid Explosive Detection Systems. LEDS = Liquids Explosives Detection System - equipment today used for screening of liquids, aerosols and gels (LAGs) in cabin baggage. Various detection technologies are used.

Finally, for technologies under development manufacturers cooperate with technology assessment bodies and assist them in developing the standards for such specific equipment, as was the case for Security Scanner technology, commonly known as "body scanners". SSc being Security scanners (= body scanners, etc.) detect items attached to human body and concealed under clothes. Within the EU today they are exclusively based on mm-waves. In the US also called Advanced Imaging Technology (ATI). For this technology legislation and performance standards are in place.

3.3.2 Quantifying the baseline

Based on interviews with manufacturers¹⁶¹, we have estimated the costs of the ECAC-CEP procedure for manufacturers. We have developed three testing approaches that can be followed:

A	Pre - Testing	Private Testing
B	CEP Testing (live test)	ECAC approval Testing
C	CEP Re-Testing (replay)	ECAC approval Testing

For a manufacturer to be very efficient and successful in the development of an Aviation Security Screenings Device the minimal test cycle in order to reach approval or certification from Member States is a combination of a Private Test (A) followed by a successful pass of ECAC Test. However, for a manufacturer who needs multiple Private Tests in order to get / develop initial quality and then needs multiple ECAC Tests (B & C) for its Aviation Security Screenings Device, goes through a very time and money consuming cycle. The result is a set of twelve testing scenarios that may occur and are realistic. These include costs for the manufacturer and the duration before they have approval.

¹⁶¹ For this report, the input of 8 manufacturers was used. Of these group of manufacturers 50% was EU based and 50% originates from outside the EU.

Table 3.6 Possible Combinations in Testing including costs and time

Scenario	Testcycle						Costs		Time	
I	1	A	1	B	0	C	115	K€	8	mn
II	1	A	1	B	1	C	140	K€	12	mn
III	1	A	1	B	2	C	165	K€	16	mn
IV	1	A	1	B	3	C	190	K€	20	mn
V	2	A	1	B	0	C	170	K€	12	mn
VI	2	A	1	B	1	C	195	K€	16	mn
VII	2	A	1	B	2	C	220	K€	20	mn
VIII	2	A	1	B	3	C	245	K€	24	mn
IX	2	A	2	B	0	C	230	K€	16	mn
X	2	A	2	B	1	C	255	K€	20	mn
XI	2	A	2	B	2	C	280	K€	24	mn
XII	2	A	2	B	3	C	305	K€	28	mn

Costs include costs invoiced by the Testing Centres and the Expenses of the Manufacturer to set up their equipment and prepare it for testing. Costs are excluding transportation fees as this is varying from device to device, origin of manufacturer and test location.

The 12 scenarios above have been used to quantify the baseline costs for airport screening equipment approval. This is done for the three product lines as earlier introduced in this section: (i) EDS, (ii) LEDS and (iii) Security scanners. Our interview programme with manufacturers indicated that for EDS equipment, manufacturers typically face testing scenarios I-III, which this means a costs range of 115-165 k€ and a duration of around 8-16 Months. For LEDs, there is a much broader range of testing scenarios, namely between I and X, which is equivalent with a costs range of some 115—255 k€, and a total duration of 8-20 months. For security scanners, manufacturers indicate that a testing scenario like X-XII applies, or some 255-305 k€ in terms of costs and a duration of 20-28 months.

Furthermore, the past three years, a relatively limited number of airport screening devices have been offered for testing and approval¹⁶²:

- EDS: 12 equipment types, hence on average 4 per year;
- LEDS: 30 types, hence on average 10 per year;

¹⁶² Source ECAC.

- Security scanners: 1 scanner type. As this is a technology that is still in an early stage of the development, it is assumed for this analysis that on average 2 product types are offered per year.

The interview programme indicated as well that on average for 50% of the screening equipment machines offered for testing and approval, an additional testing procedure is required due to more stringent requirements from additional national regulation. Based on our interview programme, it is estimated that this additional testing procedure amounts to 100% of the original testing costs for EDS, 25% for LEDS and 50% for security scanners. Additional costs for getting a national approval are nil if the authority acknowledges the ECAC-CEP test results.

Based on the above assumptions, the baseline annual costs for the testing and approval procedures regarding airport screening equipment in Europe can be determined. This amounts to approximately € 2.6 – 4.6 million.

The European Commission carried out a stakeholder consultation by means of a digital survey. The majority of respondents to this survey expressed that the current situation without a harmonised certification system for aviation security equipment has a negative effect on:

- The efficiency of the certification process;
- Research and development costs;
- Commercialisation costs;
- The time to market of equipment;
- Legal certainty;
- Competition with US competitors;
- Harmonisation of third countries, for example the US.

The majority of respondents from industry that expressed opinion indicate that the lack of harmonised certification systems for aviation security equipment in the EU has a high impact on their development costs and a medium to high impact on commercialisation costs. The industry respondents also indicate that the availability of test laboratories and time to test appointment is inadequate, and that it is important to be able to choose test laboratory. The majority of respondents also indicate that test laboratories should be accredited on an EU level and that test laboratories should be regularly audited. Finally, the majority of industry respondents consider the availability of limited pre-tests important in order to support manufacturers on the development and tuning of equipment.

3.3.3 Policy options

The Commission formulated the following policy options in excess of the baseline option (option 1):

- Option 2. "Recommendation" - The Commission would issue a recommendation to Member States to mutually accept each other's national approval systems or to rely on the common evaluation process of ECAC, provided that EU laboratories undertaking performance testing respect certain requirements. The aim of this recommendation would be to enable producers of airport screening equipment to have their product approved in only a single Member State in order to sell it in all Member States;
- Option 3 "Legislation" - The Commission would propose legislation on product certification and compliance testing principles and procedures in order to ensure full compliance with EU security performance standards adopted under Regulation (EC) 300/2008. The legislation would be elaborated jointly with regulators, industry representatives and certifiers alike. The aim of this legislation would be the same as for the recommendation, but implemented through a legally binding act of EU legislation. This approach would ensure that producers can sell their products

without restrictions to operators in all Member States once they are certified in a single Member State. Three different legislative approaches would be considered:

- 3.1. The "directive-based approach" is characterised by a set of detailed specifications which are laid out in the directive itself. This approach is based on the so called "old approach", which usually targets specific technologies and not general areas. Automotive, chemicals and pharmaceuticals are fields in which it is applied. Within this approach, product certification would be based on certification by a governmental authority;
- 3.2. The "standards-based approach" is not based on specifications with the same level of detail as in 3.1. This approach is based on the so called "new approach", which focuses on essential requirements written in general terms. Product legislation is therefore restricted to the requirements necessary to protect the public goals of health, safety and security. The technical specifications under the new approach are elaborated by the responsible European Standardisation Organisations (CEN/CENELEC and ETSI). Within this approach, product certification would be based either on a third party certification or on a self-certification;
- 3.3. The "centralised approach", whereby product certification would be done centrally by an EU agency, such as the European Aviation Safety Agency, which already certifies all EU commercial aircraft.

In this framework, the main difference between the above-mentioned options 2 and 3 would be that the latter is legally binding, thereby providing legal certainty."

Costs of the policy options

Option 2

The costs of implementing policy option 2 seems to be relatively limited. The option does not seem to have requirements that would lead to costs for stakeholders. The only cost impacting feature is that EU laboratories undertaking performance testing need to respect certain requirements. One may expect that these laboratories are audited to verify this. It is unclear which organisation would do this, but it would bring about additional costs. These costs would be directly born by the laboratories, but may be transferred to the manufacturers.

Option 3.1

Regarding option 3.1 one may expect that the existing national authorities in the member states that currently approve or certify airport screening equipment, would be tasked to carry out the product certification under this option. However, this would need to be done in only one member state, as the certificate issued would now be valid in all 28 member states. As stated above, the JRC survey indicates that currently some 18 member states are issuing certificates or approvals. Apart from one member state, the other 17 would no longer need to certify. It is our understanding that these costs for approval or certification incurred by national authorities are pretty limited however. On a balance the costs for certification are therefore considered to be in the same order of magnitude as in the baseline. These costs are incurred by the authorities and passed on to the manufacturers.

Option 3.2

Regarding option 3.2, the same line of reasoning is valid for the costs of certification as in option 3.1. Under the scheme of self-certification, these costs would not be incurred, but that would presumably imply that an auditing scheme must be established to verify if the certificates are granted according to the requirements. The main costs for implementation of the option 3.2 would be additional effort put on the European Standards Organisations to develop the product standards. One may assume that this would be on average 2-3 staff extra involved in this activity, i.e. costs

would amount € 200-300k on average per year. This is borne by the ESOs, which would require additional funding from member states.

Option 3.3

The main costs of option 3.3 would be the extension of EASA (staff) required to accommodate the additional certification task. The costs would be charged to industry applying for certification. These costs are difficult to estimate. However, in EASA's charges and fee publication, it charges around € 2.250 for certification of aircraft products with a value above € 20,000. This seems the most applicable value at the moment. Assuming some 16 types per year (see 3.3.2) the costs would amount to some € 36,000 per annum.

It should be taken into consideration that no choice has been made already with regard to the number of testing laboratories that could become operational after the adoption of the possible Commission's legislative proposal in this area. If one would therefore assume that in each suboption the same test infrastructure would still be used as in the baseline there is no cost impact for testing laboratories.

It may also be assumed that the funding structure of ECAC-CEP would change, as ECAC-CEP is now funded by four members states, and under the options the costs would be shared under 27 member states.

Benefits of the policy options

The benefits of option 2 are very uncertain. As the option is limited to a recommendation (and thus is not mandatory), it is not clear whether this would lead to the desired effects. Indications from industry are not optimistic in the respect. This is confirmed by the Commission's survey among stakeholders.

The main benefits of option 3 (irrespective of the variant) are:

Direct benefits

A key direct benefit is the **reduction of duplication of testing** for manufacturers. As indicated in section 3.2.3, our interview programme indicated that on average for 50% of the screening equipment machines offered for testing and approval, an additional testing procedure is required due to more stringent requirements from additional national regulation. Based on our interview programme, it is estimated that this additional testing procedure amounts to 100% of the original testing costs for EDS, 25% for LEDS and 50% for security scanners. It is estimated that the actual benefit is then 50% of duplicated product tests against lower costs for testing of LEDS and scanners and against full testing costs for EDS, which amounts to. 0.5-0.8 M€ per annum. This value includes costs for preparation of the testing procedure for manufacturers.

Differing national requirements imply that manufacturers need to amend their products to comply with national regulations, which negatively affects production costs. A reduction of national requirements thus offers a **decrease of production** costs for manufacturers.

Furthermore, a common EU wide certification scheme brings **more clarity on the testing procedure and timing of the procedure** than in the baseline. This is positive for manufacturers.

Finally, an EU wide certification and testing procedure coordinated by an EU recognised organisation could reduce the risk for delays in the testing procedure and is likely to **decrease the time to market** of airport screening equipment for European producers. Such time to market improvement has two implications:

- Reduced differences in time to market between European manufacturers. This is not likely to affect the market volume, but will lead to **market share shifts** between European manufacturers;
- **Improved competitive position** of European manufacturers vis-à-vis non-European manufacturers in the European market. This is addressed below under the indirect benefits.

Indirect benefits:

An EU certificate could function as a quality mark, that could **improve sales of EU manufacturers outside Europe** positively. During the interviews manufacturers stated that having an EU Certificate or Formal Approval would benefit their Go To Market in third Countries and following this the EU influence in equipment used in third countries grows. Their experience is that manufacturers that have a product that is “TSA Certified” are using this “TSA stamp” in their sales on third markets, especially emerging markets, as a selling argument. This picture is confirmed in some of the country studies such as South Korea. When the EU would also be following the line of issuing formal EU Certificates for security equipment, EU manufacturers could also use this to generate sales in third countries. Therefore third countries would be deciding to accept EU certificates and enlarge the influence of the EU legislation beyond the EU boundaries. In section 2.4.2 this impact has been valued at €35 million, in terms of lower revenue growth on third markets for major EU manufacturers compared to their US competitors for the total period after the introduction of the TSA certification system. This is about €10 million on average per year.

A single EU wide certification system is likely to **improve the competitive position** of EU manufacturers on the EU market, vis-à-vis their non-EU competitors. Non-EU producers can now easily put their products in several EU countries on the market once they are TSA approved. A common EU certification system implies that these manufacturers have to go through the same route of testing and certification as the EU manufacturers. We have quantified this in section 2.4.2 again by comparing the revenue growth rates of EU and US manufacturers, but now for the EU market. This has been quantified at a value of €42 million for the total period since the TSA certification, which is about €12 million per annum.

One could argue that the direct benefits for manufacturers would have a negative impact on the sales price of the equipment. However, based on the current market structure with only a few suppliers per equipment type it is expected that cost pass-through is limited to zero, i.e. the impact on sales price would be absent.

Results from survey

Our interview programme under manufacturers did not provide indications that the magnitude of the benefits as addressed above differs significantly between suboption 3.1, 3.2 and 3.3. The survey carried out by the European Commission under stakeholders (broader than industry) provides a picture that impacts might differ between these suboptions. The majority of respondents indicate that option 3.3 provides the greatest potential, followed by respectively option 3.1 and 3.2, to:

- ensure the optimal level of security for European airports and citizens;
- increase the capacity of technology to adapt to emerging threat scenarios;
- increase the facilitation;
- reduce research and development cost;
- reduce commercialisation costs;
- foster the harmonisation with third countries, for example the US;

- provide better guidance to procurers;
- improve mutual trust in Member States' aviation security in view of "one stop security";
- reduce time to market of equipment;
- influence the competition with non-EU suppliers;
- simplify the procurement process of airport screening equipment for airport operators or their procurement agencies.

Conclusion

In the sections above, the various costs and benefits of the policy options in comparison with the baseline have been addressed. These are summarised in the tables below.

Table 3.7 Comparison of costs and benefits for options (compared to baseline)

	Option 1 (baseline)	Option 2	Option 3.1	Option 3.2	Option 3.3
Impacts for EU Industry					
Reduction duplication of testing	0	0	0.5-0.8 M€ p.a.	0.5-0.8 M€ p.a.	0.5- 0.8 M€ p.a.
Increased certification fees to EASA	0	0	0	0	0.04 M€ p.a.
Increased clarity on testing procedure	0	0	+	+	+
Efficiencies in production	0	0	+	+	+
Reduced risk for delays and improved time to market	0	0	+	+	+
Improved competitive position on non-EU market	0	0	10 M€ p.a.	10 M€ p.a.	10 M€ p.a.
Improved competitive position on EU market	0	0	12 M€ p.a.	12 M€ p.a.	12 M€ p.a.
Impacts for authorities					
Reduced costs for issuing certificates	0	0	0	0	0
Impacts for testing laboratories (TL)					
Verification costs of TLs work	0	-	0	0	0
Reduced revenues	0	0	-	-	-
Impacts for Eur. Standardisation Organisations					
Costs for standards development	0	0	0	0.2-0.3 M€ p.a.	0
Impacts for end users					
Reduced product price	0	0	0	0	0

+ = positive impact, - = negative impact.

The main conclusions from the analysis are:

- The benefits of option 2 are marginal (if any) due to the voluntary character of the option. At the same time, costs need to be incurred. As a result, benefits do not seem to outweigh the costs for this option;

- The benefits of suboption 3.1, 3.2, and 3.3 are on the same level. Our interview programme with eight manufacturers did not reveal any preference in this respect, as long as the option 3 was implemented (irrespective of the variant). However, the stakeholder consultation carried out by the Commission indicated that impacts are to be expected larger under option 3.3;
- The direct benefits in terms of reduced duplication of testing are limited considering the absolute numbers ;
- The main benefit of the option 3 is indirect: a European certificate brings European manufacturers 'on par' with their US competitors on markets in emerging markets and in Europe. The improved competitive position will increase revenue for the manufacturers and value added for the European economy. This is irrespective of the sub option chosen;
- Option 3.1 scores slightly better in terms of the benefit-to cost balance than the other sub options, stemming from the difference in costs. However, the degree of uncertainty around the costs could influence this ranking.

4 Security R&D programmes

4.1 Introduction

Innovation is essential to meet public demand for greater security and to address the evolving challenges of terrorism and organised crime. Effective R&D policies and programmes are one of the key ingredients for successful innovation. They also help to develop the future competitiveness of the security industry. Identifying the best measures and practices that have been used in other countries could provide valuable lessons for the EU policy makers. However, our investigation has revealed that data and information on security R&D are scarce. Extensive information on security research is available only for the United States. In other countries the transparency of security R&D is significantly worse. In some countries it is essentially non-existent and the whole area is clouded in secrecy. This lack of information rules out any comprehensive and systematic comparative assessment of security R&D programmes in third countries. However, this chapter attempts, under these information constraints, to provide a comparative overview of security R&D in some selected countries. More details about national R&D programmes in the security field can be found in country reports.

First, the chapter briefly describes the general context for R&D policies with more specific reference to domestic security environment and national innovation systems. Then it describes security R&D in selected countries and presents relevant quantitative data when available. Finally it identifies some useful lessons from the US experience in this field – the global leader in security R&D.

4.2 General context: overall R&D landscape and security environment

In every country civil security R&D policies, institutions and performance are determined, to a large extent, by a general national context. Two main elements of this context are of particular importance:

1. The domestic security environment and public perception of security threats; and
2. The national innovation system.

We will briefly consider both of them below.

4.2.1 Security environment

The need to address security risks provides “demand pull” for security-related innovations. The higher the level of such risks and their perception the higher the expected demand for innovation in the security field all other things being equal.

It is obvious that the security environment of the selected countries is widely different. The level of various domestic security risks (based on historical statistics) differs by orders of magnitude between the countries (see Table 4.1 and Table 4.2). The combination of risks also varies substantially. For example, Israel faces a high level of terrorist threat but the rate of intentional homicide is relatively low compared to other countries in the group. Brazil can be viewed as an opposite example: it has a high crime rate but the risk of high-profile terrorist accidents seems to be low, or at least that current/daily crime and violence have a higher priority. Russia scores high on both types of risk while South Korea and Japan have had low rates of crime and terrorist accidents

in the last decade (but there are potential external security risks in both countries originating from numerous border disputes and North Korea's provocative behaviour).

Table 4.1 Fatalities from terrorist incidents by year

Year\Country	Brazil	Israel	Russia	US
2000		1	33	0
2001		110	25	2987
2002		329	226	3
2003		174	159	0
2004		65	459	0
2005	1	27	38	0
2006		37	34	1
2007		4	66	0
2008		11	49	0
2009		0	14	15
Total	1	758	1103	3006

No fatalities from terrorist incidents have been reported for China, Korea and Japan in 2000-2010.

Source: RAND Database of Worldwide Terrorism Incidents (RDWTI), <http://www.rand.org/nsrd/projects/terrorism-incidents.html>.

Table 4.2 Rate of intentional homicide per 100,000 population, 2010

Country	Rate
Brazil	21.0
China	1.0
Israel	2.1
Japan	0.5
Republic of Korea (RoK)	2.6
Russia	10.2
US	4.8

Data for Japan from 2009.

Source: UN Office on Drugs and Crime, <http://www.unodc.org/unodc/en/data-and-analysis/homicide.html>.

Another important factor is the perception of the security risk by the government and the population at large. High-profile terrorist events, such as the 9/11 attack in the US, tend to lead to much more substantial changes in policies compared to persistent and steady threat of violent crime even when its casualties are startlingly high. For example, the 9/11 attack led to the creation of Department of Homeland Security and very large increases in public funding for anti-terrorism research and development in the US. In more authoritarian states the fear of public unrest might be another factor that drives increased investment in security R&D.

4.2.2 National innovation system

The national innovation system (or the science, technology and innovation system – the STI system) is another critical element of the overall context that has a direct impact on the structure and performance of security R&D programmes. The national innovation system can be defined as “a set of institutions whose interactions determine the innovative performance ... of national firms.”¹⁶³ Institutions involved in security research and development are part of the overall STI system. Therefore, an understanding of national innovation systems is important for the analysis of security-related R&D.

¹⁶³ Nelson, R. (ed.) (1993), *National Innovation Systems. A Comparative Analysis*, Oxford University Press, New York/Oxford.

The scope of this report prevents us from providing a detailed review of the different countries' innovation systems here, but good descriptions and analyses of national STI systems are readily available elsewhere. The ERAWATCH website,¹⁶⁴ for example, provides an excellent resource on various aspects of the national STI systems for all seven countries in our group (the site is supported by the **European Commission's Joint Research Centre**). The OECD also gives short summaries on country's STI systems in its regularly published Science, Technology and Industry Outlooks. Some country reports present relevant aspects of country's STI system as well.

Our aim is to conduct a quick comparison of the selected countries in terms of their STI inputs, processes and outputs based on a set of quantitative indicators. This exercise should be helpful in several respects. First, it illustrates the similarities and differences between the countries' innovation systems. Second, since data for security R&D are often missing it provides rough proxies for them. Overall national R&D figures does not tell much about more specific security-related R&D data but general patterns existing between countries in terms of research intensity, sources of funds, and other indicators are likely to be broadly valid for security R&D as well.

The most frequently used measure of R&D input is gross domestic expenditure on R&D (GERD). Figure 4.1 shows this indicator for all seven countries included in the report (as the area of bubbles). It illustrates that the selected countries spend vastly different amounts on R&D. This difference comes down to two factors: the size of the economy and the research intensity of economy, which is measured as a ratio of GERD to GDP and illustrated at the horizontal axis. R&D intensity is useful indicator of the nation's industrial structure – higher values tend to indicate large presence of high-tech industries and sectors in the economy. The chart also illustrates that countries with a higher level of GDP per capita tend allocate proportionally more resources to R&D (i.e. the research intensity is higher in the US and Japan than in China, Russia or Brazil). This relationship is not exactly linear: both Korea and Israel are global leaders in terms of R&D intensity but they are not as wealthy as the US.¹⁶⁵

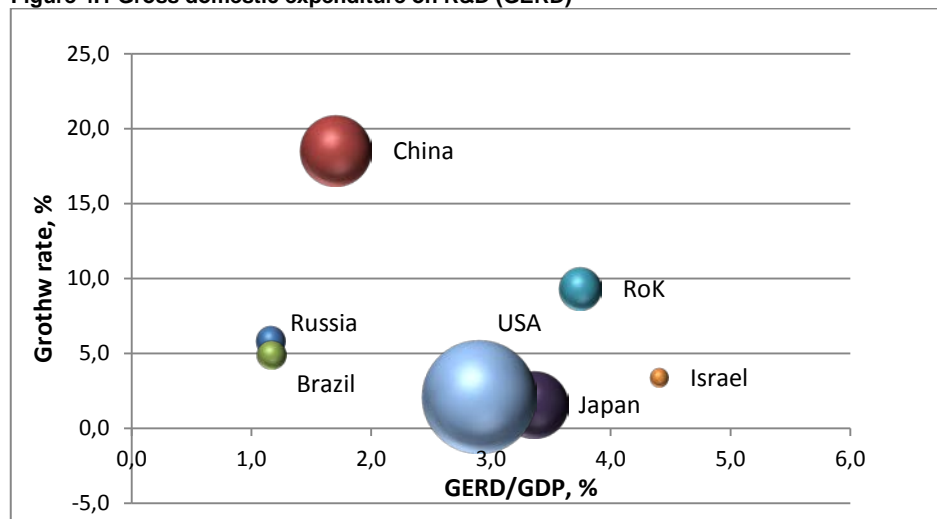
Another important dimension is the growth in GERD in recent years shown as the average growth rate over the period of 2000-2010 on the vertical axis of Figure 4.1. China and Korea are undisputed leaders in this respect. Their R&D expenditures have expanded more rapidly than their economies. As a result, over the last decade the R&D intensity in both countries increased substantially. In other countries this indicator has been flat or almost flat. Russia and Brazil have also been increasing the R&D expenditure more rapidly than in the US, Japan and Israel in the last decade but these increases have been in line with their GDP growth. As a result, their GERD to GDP ratio remained generally flat over the same period.

Overall GERD figures do not reveal the important differences between the sources of funds for R&D. Figure 4. provides an overview of the allocation of GERD by funding sources for all seven countries. There are several important details that this chart reveals. First, in Russia and, to a lesser extent, in Brazil, a very high share of total R&D funding comes from the government. Correspondingly, the contribution from their business enterprise sectors is smaller, reflecting the commodity-oriented character of their economies. In Asian countries – China, Korea and Japan – the situation is the opposite: by far the largest source of funding for R&D is the business sector. Israel has a very high share of foreign funding for R&D while the share of government funding is low but would be boosted if military R&D expenditure were included.

¹⁶⁴ <http://erawatch.jrc.ec.europa.eu/erawatch/opencms/>.

¹⁶⁵ High value of Israel's GERD to GDP ratio is even more impressive given that most of its military-related R&D is excluded from GERD numbers.

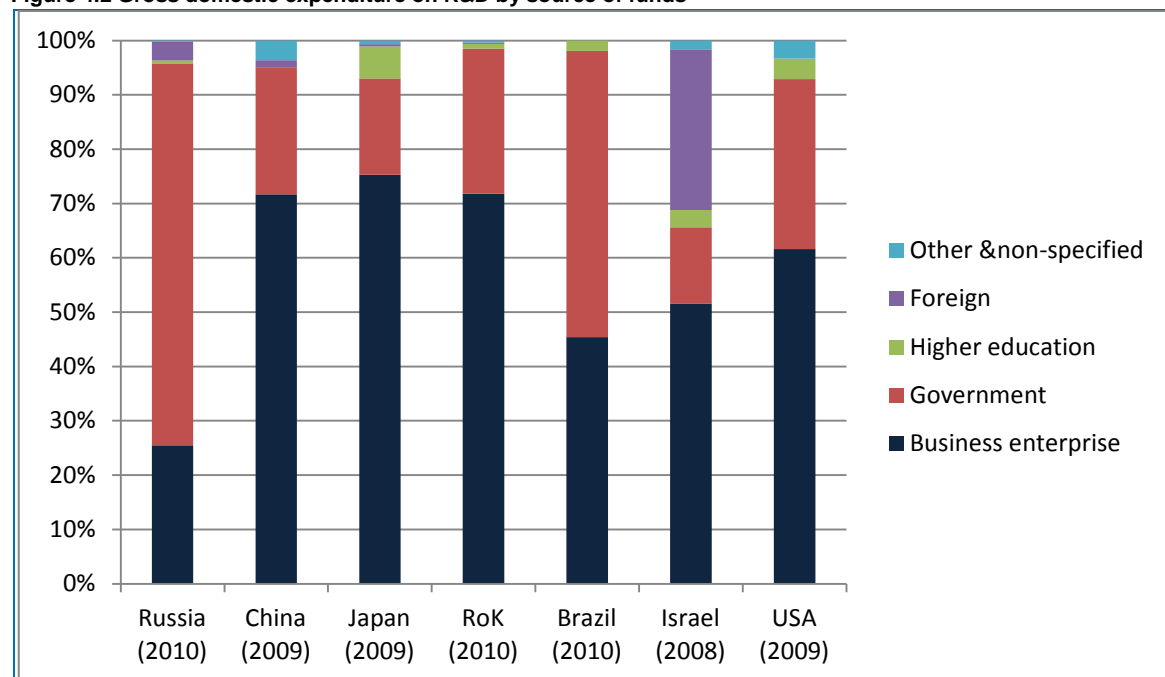
Figure 4.1 Gross domestic expenditure on R&D (GERD)



Notes: Area of bubbles correspond to GERD at 2005 US\$ adjusted for purchasing power parity (PPP). Data for 2010 or the latest available. Growth rate refers to the average annual increase in GERD measured in constant prices 2005 PPP US\$ over the period of 2000-2010.

Source: UNESCO Institute for Statistics, authors' calculations.

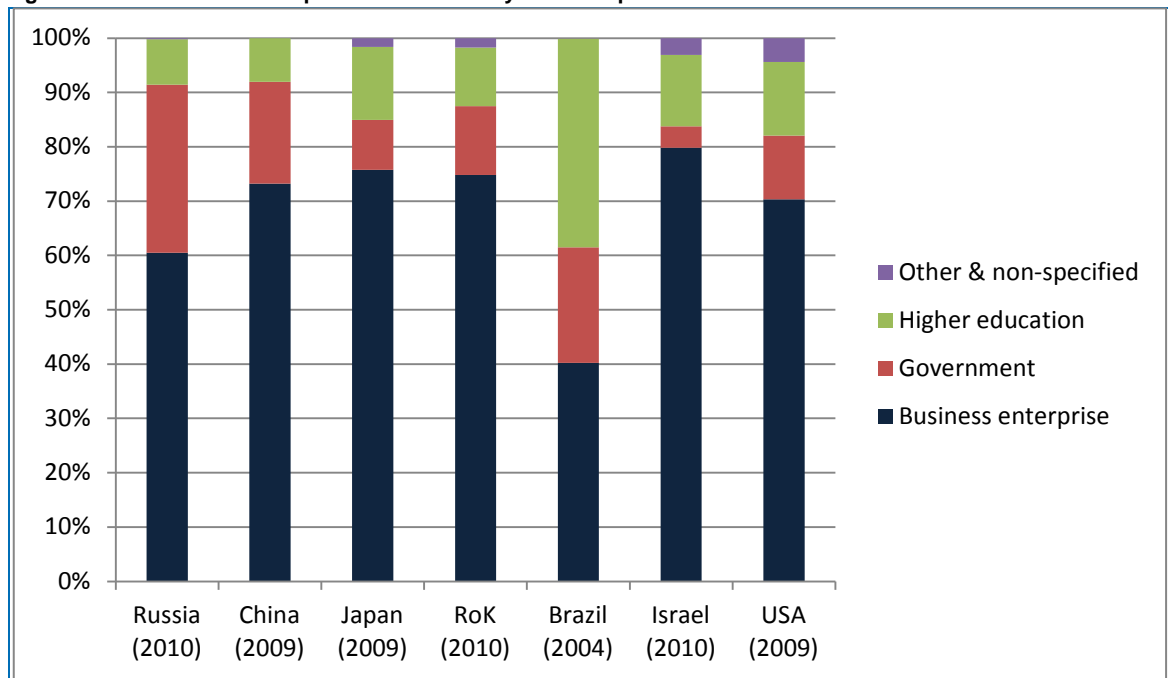
Figure 4.2 Gross domestic expenditure on R&D by source of funds



Source: UNESCO Institute for Statistics.

Figure 4.3 shows where research and development are conducted. While there is obviously a link between funding sources and sectors of performance, this chart shows that the role of the business sector and higher education in conducting R&D is larger than their share of R&D funding. The specific distribution is, of course, dependent on country's unique circumstances and traditions.

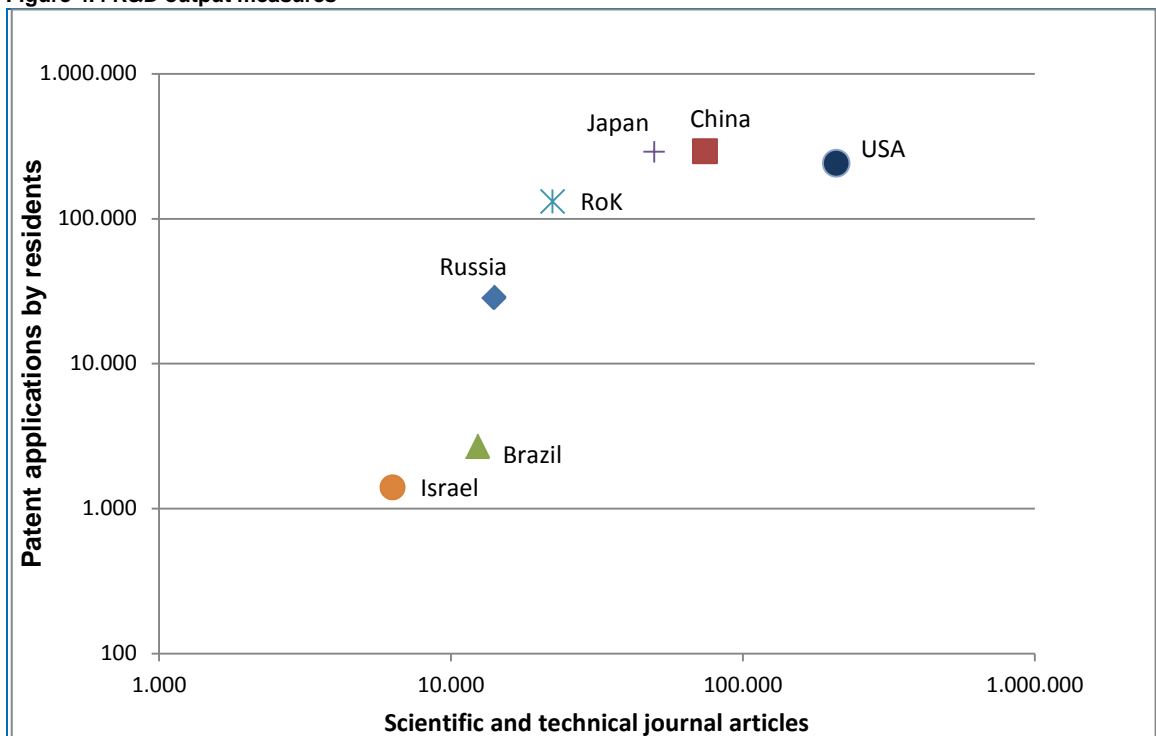
Figure 4.3 Gross domestic expenditure on R&D by sector of performance



Source: UNESCO Institute for Statistics.

Finally, Figure 4.4 shows two measures of R&D output – the number of scientific and technical journal articles and the number of patent applications by residents. Given large differences in these measures the chart uses logarithmic scale on both axes. Four countries – South Korea, China, Japan and the US – are significantly above the rest. The position of Israel on this chart is hampered by its much smaller population and the fact that most of its patent applications are made abroad (and are not included in chart's data).

Figure 4.4 R&D output measures



Source: World Bank – World Development Indicators.

This quick comparison shows that the selected group of countries includes nations with very different performance in the overall R&D field. These differences have substantial impact on countries' performance and success in security-related R&D. While the security context and other factors in every country might dampen (or exaggerate) the impact but they are unlikely to eliminate it completely.

4.3 Security R&D

4.3.1 Expenditures

We are not aware of the existence of systematic national-level data on civil security R&D expenditure in any country. The main reason for this lack of data is the fact that security is not included directly in the common classification systems used by statistical agencies to collect R&D data. For example, it is not present in the NABS (Nomenclature for the Analysis and comparison of Scientific programmes and Budget), which is used by Eurostat and other organisations to collect R&D statistics at international and national levels. NABS classifies R&D outlays according to their socio-economic objectives and include defence R&D but not security.¹⁶⁶

Another way that statistical agencies use to collect and organize R&D data, in particular in the business sector, is according to common economic activity and industry classifications such as ISIC (International Standard Industrial Classification of All Economic Activities). However, the security industry is not included into these classifications directly. Rather its different subsectors are hidden under several broader economic activity headings (such as Manufacture of computer, electronic and optical products).

In addition, information on civil security R&D expenditures is often considered as restricted or even secret, in particular outside the OECD countries. Even within the OECD, Israel, for example, does not disclose its public expenditure either on military or security R&D. Finally, even when some data exist their comparability might be questioned due to varying definitions of civil security and its blurring borders with defence and safety. This can be seen, for example, in divergent estimates of the security market size by various organisations cited in Chapter 2 of this report. The same issue also affects data on security R&D.

All these factors suggest that improvements in statistical data collection are important for better understanding of security R&D field and the security industry more generally.

The only systematic source of data on public expenditure on safety and security R&D comes (potentially) from the government finance statistics. The Classification of the Functions of Government (COFOG) developed by the OECD includes the functional group *Public Order and Safety* (code GF03). One sub-category (or second-level category) within this group is *R&D Public Order and Safety* (GF0305). In principle, this sub-category should include all civil security (and safety) R&D expenditures by public agencies and provide comparable data. The main problem is that many countries do not collect or do not report information according to the second-level of COFOG.¹⁶⁷ These data are not available for all non-European member countries of the OECD including Japan, Israel, Korea, and the United States.¹⁶⁸ While the Eurostat reports such

¹⁶⁶ Security is included only in the sense of social security.

¹⁶⁷ Additional problem was that "the second-level COFOG data were not comparable among countries because the SNA/UN guide and the International Monetary Fund Manual on Government Finance Statistics do not provide much practical information on the application of COFOG concepts. However, in 2005, Eurostat established a task force to develop a manual on the application of COFOG to national account expenditure data and to discuss the collection of second-level COFOG data for European countries." Source: OECD, *Government at a Glance*, 2011.

¹⁶⁸ OECD, *Government at a Glance*, 2011.

information at least for some EU member states there are substantial doubts about the comparability of the reported data on public order and safety R&D.¹⁶⁹

We found time series data on central government expenditure on security-related R&D only for two countries: the United States and the Russian Federation. The American Association for the Advancement of Science (AAAS) in its annual reports on research and development in the US provides figures for federal funding of homeland security R&D based on Office of Management and Budget data. Russia's budget classification is very similar to COFOG and Accounts Chamber's reports on the execution of the federal budget disclose aggregate numbers for applied research and development in the safety and security field. Table 4.3 provides these data from 2005 till 2012.

Even in the case of the US and Russia there are substantial problems with data.¹⁷⁰ It seems that both countries have changed their methodologies over the last few years and data might not be directly comparable over the different years.¹⁷¹ A recent report by the US Government Accountability Office (GAO) directly stated that the Department of Homeland Security (DHS) "does not know the total amount its components invest in research and development."¹⁷² In Russia approximately three quarters of total safety and security R&D expenditure is classified and information on its allocation between different agencies is not publicly available. Finally, comparison of data from the US and Russia is even more problematic since their collection and classification do not follow the same set of rules and the scope might be different

Although we urge caution when interpreting the data in this table some interesting facts can still be discerned. One is that the US security-related R&D expenditure dwarfs those of Russia any other country for that matter). The second and probably more surprising observation is that Russia's security and safety R&D outlays increased tremendously over the same period and now rival those of the EU. Big jump in Russia's safety and security R&D expenditure in 2010 was probably related to a reclassification of some defence programmes as security ones (as suggested in Russia country report). However, even without this one-time change, overall growth in Russia's federal safety and security R&D has been quite impressive. In the United States there is no clear time trend for homeland security R&D expenditure – it was generally increasing up to FY2010 but declined significantly in FY2011 and FY2012.

Table 4.3 Central government funding of safety and security R&D

Country/ Year	2005	2006	2007	2008	2009	2010	2011	2012
US								
million USD	4,893	5,138	4,867	5,089	5,485	5,946	5,181	4,989
million EUR	3,848	4,175	3,658	3,385	4,050	4,385	3,716	3,845
Russia								
million RUB	2,765	3,545	5,336	6,901	8,013	21,792	23,153	32,651
million EUR	78	104	153	189	181	542	566	818

Note: For the US: figures correspond to federal homeland security R&D funding (budget authority). Years refer to fiscal years running from October 1st to September 30th, i.e. FY2005 runs from 1/10/2004 to 30/09/2005. Data for FY2012 are preliminary. Sources: for the US – American Association for Advancement of Science; for Russia – Accounts Chamber of the Russian Federation.

¹⁶⁹ It seems doubtful, for example, that safety and security R&D expenditure in Germany and the UK differs by more than 10-fold when their total safety and security expenditure are comparable.

¹⁷⁰ CRS Report RL32482, Federal Homeland Security Research and Development Funding: Issues of Data Quality discussed this problem for the US.

¹⁷¹ For the US this issue is mentioned in AAAS Report: Research and Development FY2012, Table I-6, <http://www.aaas.org/spp/rd/rdreport2012/>. In Russia an indirect indication of such a change is more than 2.5-fold increase in R&D funding in 2010.

¹⁷² U.S. GAO, Department of Homeland Security: Oversight and Coordination of Research and Development Should be Strengthened, GAO-12-837, September 2012, Washington D.C.

The importance of security R&D among other R&D priorities can be judged by tracking the relative share of the corresponding funding. This share can be calculated based either on the government R&D funding or on total domestic expenditure on R&D (GERD). The former way is probably more informative since it directly reflects government priorities. The latter provides a more generic measure of the importance of public security R&D in overall national R&D portfolio. Table 4.4 shows both measures.

Table 4.4 Federal security and safety R&D as a percentage of total federal R&D funding and GERD

Country/ Year	2005	2006	2007	2008	2009	2010	2011
Share of security R&D in the federal government R&D expenditure							
US	3.7%	3.8%	3.4%	3.5%	3.8%	4.0%	3.6%
Russia	1.7%	1.9%	2.1%	2.4%	2.1%	5.6%	5.0%
Share of federal government security R&D in GERD							
US	1.5%	1.5%	1.3%	1.3%	1.4%	1.5%	1.3%
Russia	1.2%	1.2%	1.4%	1.6%	1.6%	4.2%	3.8%

Sources: see Table 4.3, authors' calculations.

Table 4.4 shows that in the United States there has not been a consistent trend (upward or downward) in the period of 2005-2011. At the same time the relative priority of security-related R&D has been steadily increasing in Russia.

Another way to look at security R&D funding is to analyse their share in overall public expenditure on security and safety. In other words, this is a measure of how R&D-intensive public expenditure on safety and security is, or to what extent government relies on development of new technologies and methods (R&D) to address domestic security challenges compared to other categories of expenditures such as wages, maintenance, equipment procurement, etc. Comparing the United States and the Russian Federation in this respect is somewhat tricky: in Russia the central government accounts for approximately 80 of public expenditure on security and safety, while in the US the proportion is reverse. It means that the role and responsibilities of federal ministries in these countries differ a lot and direct comparison would not be very informative. However, since public expenditures on security and safety R&D come almost exclusively from the federal government in both countries it makes sense to relate central (i.e. federal) government security and safety R&D expenditure to total public spending in this area. The results are presented in Table 4.5.

Table 4.5 Central government expenditure on security and safety R&D as a percentage of total budget outlays on public order and safety

Country/ Year	2005	2006	2007	2008	2009	2010	2011	2012
US	1.9%	1.9%	1.7%	1.7%	1.7			1.9%
US DHS	0.5%	0.5%	0.6%	0.6%	0.6%	1.6%	1.5%	0.5%
Russia	1.9%	1.9%	1.7%	1.7%	1.7			1.9%
For comparison:	0.5%	0.5%	0.6%	0.6%	0.6%	1.6%	1.5%	0.5%
Germany	1.9%	1.9%	1.7%	1.7%	1.7			1.9%
Netherlands	0.5%	0.5%	0.6%	0.6%	0.6%	1.6%	1.5%	0.5%
UK	1.9%	1.9%	1.7%	1.7%	1.7			1.9%

Source: see Table 4.3; OECD. Stat, authors' calculations.

In the US the ratio of security and safety R&D expenditure¹⁷³ to total public spending on safety and security has been declining but until 2010 it was still substantially higher than a similar ratio in Russia. However, after a jump in 2010 Russia's ratio came quite close to the US values. Within the US federal budget R&D expenditure obviously accounts for higher proportion of the funds allocated to public order and safety. For example, within the US DHS budget the share of R&D is about 2.5%. Since a substantial part of homeland security R&D in the US is funded by other federal departments (more on this below) the ratio of homeland security R&D expenditure over the total federal expenditure on homeland security is even higher – 7.3-7.7% in FY2011-2012. This is not far from what can be found in defence – around 11-12% in recent years (i.e. defence R&D accounts for 11-12% of total defence expenditure in the US and Russia). This suggests that American policy makers put a lot emphasis on new technological solutions to security threats.

Security R&D expenditure in other countries¹⁷⁴

Korea: Korean public expenditure on security R&D seem to be modest when compared to that of the US and Russia. The Korean Ministry for Industry, Trade and Energy put forward its *Securing Knowledge Korea 2013* plan in 2008 to promote the security industry as one of the new growth engines for the Korean economy. The plan stipulated an investment of 150 billion KRW (105 million EUR) to support basic and applied technology plans. However, lower than expected growth rates and budget cuts due to the global recession led to actual annual spending of approximately 6 million EUR since 2009 (as opposed to planned 21 million EUR).

While this plan is not the only source of public funding for security R&D in Korea, information about other sources is limited. The Ministry of Security and Public Administration funds some security-related R&D, e.g. in forensics. The Agency for Defence Development has undertaken the bulk of technological research in the defence field. It had budget of circa 760 million EUR in 2011. Some of its research has security applications (such as night vision devices).

Yet it seems that the main funder of security R&D in Korea is the business sector. It was reported by the Korea Internet Security Agency that the total technological R&D investment by physical security companies amounted to 257 million EUR in 2011. On average companies invested 2.9% of their revenues in R&D in 2011 and slightly less (2.8%) in 2012. The average company R&D budget was 910,000 EUR in 2011. The important role of the business sector in funding security R&D is consistent with its high (72%) share in GERD.

Japan

Overall public expenditure on security R&D in Japan is not known. Funding of security and safety R&D programmes is split between several ministries and agencies and aggregate information on such expenditures is not publicly available. Table 4.6 provides science and technology funding for the main ministries involved in the provision of civil security and safety in Japan in the proposed budget for the fiscal year 2013.

Table 4.6 Science and technology expenditure in the proposed FY2013 budget

Ministry	JPY billion	EUR million
Ministry of Defence	166.9	1,284
Ministry of Land, Infrastructure and Transportation	50.6	389
Ministry of Justice	5.6	43
Police Agency	2.0	15

¹⁷³ This were calculated as a sum of total federal homeland security R&D expenditure and R&D expenditure funded by the Department of Justice.

¹⁷⁴ Information for security R&D in China and Israel is very limited.

Security represents only one of several R&D areas that are funded by the Ministries listed in Table 4-6. The main focus of Ministry of Defence's funding is obviously military R&D. Ministry of Land, Infrastructure and Transportation has a broad scope of responsibilities (as its name suggests) with security and safety only one of them.

However, like in Korea, the main funder of security R&D in Japan is the private sector. Overall government is responsible only for less than 18% of total expenditure on R&D in Japan. While this share is likely to be higher in security R&D large Japanese companies, such as NEC, Hitachi, Fujitsu and others have invested substantial sums in security and safety R&D.

Brazil

Public expenditure on security R&D in Brazil are not publicly available. Brazil's expenditure on R&D as a percentage of GDP is relatively modest (see Figure 4.1) and security (excluding defence) seems to be not among main priority areas for R&D. The threat of terrorism in the country is comparatively small. However, the preparations for two large sport events – the 2014 World Cup and the 2016 Summer Olympics – provide the boost to public spending on security-related issues. For example, the budget for the 2014 World Cup allocates nearly €160 m to the implementation of comprehensive intelligence systems, information management and telecommunications for big-scale events.¹⁷⁵

Brazilian companies are also not particularly R&D intensive in general. The 2012-2015 National Strategy on Science, Technology and Innovation for National Development acknowledges the private sector's tendency to "seek little innovation with a view to the market and to adopting a passive culture regarding the transfer of technology".¹⁷⁶ The Brazilian government has implemented a wealth of measures to stimulate innovation in the private sector and the number of companies using shows an upward trend. Some foreign investors are quite active in the security R&D: Brazilian subsidiary of Smith Detection has invested more than €383 million in R&D in the last ten years.

No information on security R&D expenditures has been found for Israel or China but it is assumed that they are substantial at least compared to other government-funded R&D.

4.3.2 Main actors

Security is in many respects a public good. This is especially true in the case of terrorism threat. Therefore, the public sector is by far the main provider of security to the public in all but a few failed states. It is often the main buyer of advanced security products. Therefore, its procurement policies can play an important role in stimulating innovation. Even when it does not buy security equipment directly it sets the security and safety requirements that drive demand for such equipment, for example from critical infrastructure operators.

Research also has public good characteristics. It is logical that public agencies everywhere set the main priorities and play a large role in funding security R&D. The specific governance structure is different in every country and country reports provide some details on this. Typically it is law enforcement and counter-terrorism agencies that set thematic priorities for research and allocate the related funding.

¹⁷⁵ Menezes, D., "Secretaria de Segurança para Grandes Eventos terá R\$ 807,8 milhões em 2012", Contas Abertas, 13/03/2012. Available at: <http://www.contasabertas.org/WebSite/Noticias/DetalheNoticias.aspx?Id=822>.

¹⁷⁶ National STI Strategy (*Estratégia Nacional de Ciência, Tecnologia e Inovação*, ENCTI) 2012-2015, MSTI and CNPq, 2012. Available at: <http://www.mct.gov.br/index.php/content/view/336399.htm>.

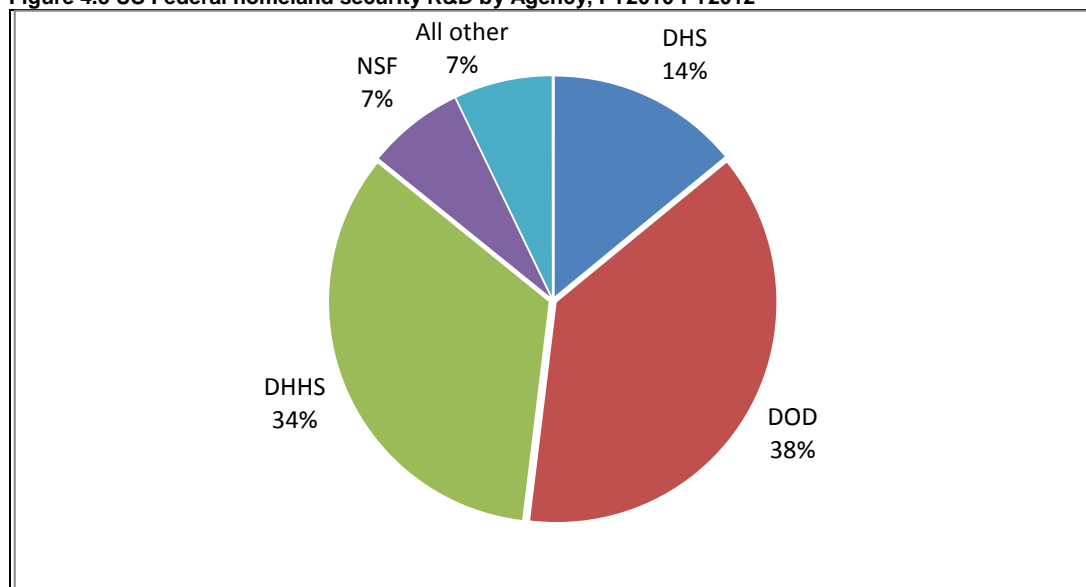
US

The Homeland Security Department is the main federal agency charged with protecting the US against terrorist attacks and responding to man-made accidents and natural disasters. Within the DHS the Science and Technology (S&T) Directorate is the agency's research and development arm. Its mission is «to ensure that DHS and the homeland security community have the science, technical information and capabilities they need to effectively and efficiently prevent, protect against, respond to, and recover from all-hazards and homeland security threats». It is also required to identify priorities and coordinate federal effort to develop countermeasures against terrorism.

However, it is not the largest funder of homeland security R&D. Department of Health and Human Services (DHHS), specifically the National Institutes of Health, and the Department of Defence (DOD) have accounted for larger shares of federal homeland security R&D funding. The National Science Foundation (NSF) has also been a substantial supporter of security-related research.

DHHS manages most of federal effort against bioterrorism. DOD's R&D activities in homeland security include work on countering chemical and biological threats. NSF's homeland security priorities focus on protection of critical infrastructures and include cyber security R&D.¹⁷⁷ Their shares of total homeland security R&D funding over the last three fiscal years are presented at Figure 4.5.

Figure 4.5 US Federal homeland security R&D by Agency, FY2010-FY2012



Source: American Association for Advancement of Science.

Homeland security R&D in the US is performed by a broad range of actors. They include among others:

- DHS internal laboratories;
- Three federally funded R&D centres (FFRDC) sponsored by the DHS;
- FFRDCs sponsored by other federal agencies, including for example Department of Energy's national laboratories;
- Universities;
- Private sector companies.

¹⁷⁷ CRS, Homeland Security Research and Development Funding, Organisation, and Oversight, August 2006.

According to the latest figures available¹⁷⁸, in 2008 the DHS spent 43.1% of its R&D funds in industrial companies, 25.1% were granted to DHS internal laboratories, 20.1% funded some federal R&D centres and 6.3% was spent in Universities and colleges.

Russia

Two main federal agencies – the Federal Security Service (FSB) and the Ministry of the Interior (MVD) – are the main funders as well as performers of security-related R&D. Another agency, the Ministry of Emergency Situations, has been very active in safety-related research and significantly increased its R&D funding in recent years.

The FSB is the main domestic security agency in Russia. Its main responsibilities include counter-intelligence, border security, counter-terrorism, and surveillance. One of its nine directorates is the Scientific and Engineering Service, which is responsible, among other things, for science and technology (S&T) policy of the FSB.¹⁷⁹ This directorate includes several research centres and institutes, including the Research Institute of Information Technologies. The FSB also has close ties with other state-owned organizations working in the area of information security. Most of security R&D funded by the FSB is carried out in specialized state-owned research centres and organizations, including those under direct control of the FSB. At the same time, private sector companies are also increasingly involved at least in some projects and programmes. Higher education institutions do not play any substantial role in security R&D.

The main organisation within the MVD that is responsible for the implementation of its S&T policy is the Research and Production Enterprise *STiS*.¹⁸⁰ It carries out a broad range of R&D to meet the needs of various MVD departments and its internal troops. It also conducts testing and evaluation of equipment produced by other companies for the MVD. Another research centre *Okhrana*, which is part of the MVD, provides research support to MVD's organisations with respect to alarms systems and a leading actor in standardisation of alarm systems in Russia.

Japan

In Japan the National Public Safety Commission sets national policy in the field of public order and safety. It also administers the National Police Agency (NPA), which in turn supervises prefectural police departments. The National Research Institute of Police Science, which is part of the NPA, conducts research in forensics and criminology. Other agencies involved in the provision of civil security include:

- The Ministry of Land, Infrastructure and Tourism, which supervises the Transport Safety Board and the Japan Coast Guard;
- The Ministry of Justice, which supervises the Public Security Intelligence Agency;
- The Ministry of Defence, with the Technical Research and Development Institute being the main actor in performing defence-related R&D.

Korea

The Korean Ministry of Security and Public Administration is in charge of the civil and domestic affairs in South Korea. It includes the National Police Agency and the National Emergency Management Agency. As it was mentioned the Ministry for Industry, Trade and Energy supports R&D in the security industry.

¹⁷⁸ National Science Board, *Science and Engineering Indicators 2010* (NSB 10- 01), Appendix Table 4-20.

¹⁷⁹ <http://www.agentura.ru/dossier/russia/fsb/structure/> (in Russian).

¹⁸⁰ Translation of its full Russian name means - Special Equipment and Communication, <http://stismvd.ru/>.

We have not been able to identify any national research institute that conducts basic research for the civilian security sector. Some dual use research (or closely related to defence technologies) is likely to be conducted at the Agency for Defence Development.

However, the main funders and performers of security R&D in Japan are private companies, in particular large electronics companies.

Israel

The definition of Homeland Security in Israel is harder than in other countries. Infrastructure as a separation barrier and the so-called “Iron Dome” missile shield are more than HLS and partly belong to the military sector. Furthermore intelligence, surveillance and reconnaissance are of high importance. And so several ministries in Israel have a responsibility for homeland security:

- Ministry of Public Security, active in terrorism response, order violations, earthquakes and other catastrophes;
- Ministry of Interior, responsible for entry/exit at borders and therefore part of border security;
- Ministry of Defence with a special unit responsible for the protection of critical infrastructure including urban transport and the protection of the public against nuclear, chemical and biological dangers.

Within the Ministry of Industry, Trade and Labour (MOITAL) and empowered by the “Law for the Encouragement of Industrial Research & Development - 1984” (The R&D Law), the Office of the Chief Scientist (OCS) oversees all government sponsored support of R&D in the Israeli industry. It operates through the R&D Fund, as well as a gamut of domestic and international programs, agreements and collaborations. The OCS annually supports hundreds of projects, from incipient concepts within a pre-seed framework, followed by support of incubator and start-up companies. The OCS had an annual budget of around EUR 361mn in 2012.

When a government-assisted R&D project results in a commercially successful product concerned company is obligated to pay royalties. Such royalties are used to fund future grants that encourage and support industrial R&D.

China

R&D in China is very centralised through the State Council. The Ministry of Science and Technology (MOST) of the People’s Republic of China, formerly the State Science and Technology Commission, is the body primarily responsible for science and technology strategy and policy. It also administers national research programs, S&T development zones and international co-operation. The Ministry of Education oversees education as well as research institutes at universities. Several other ministries such as the Ministry of Industry and Information Technology are also involved in S&T.

Based on the success of the Special Economic Zones of the PRC, China has created Economic and Technological Development Zones. They have the purpose of building up high-tech industries, attracting foreign investment, increasing exports and improve the regional economy. They are considered to have been very successful and have been extended from an initial fourteen to fifty-four (15).

The situation of R&D for security products and equipment however, in China is ambiguous, with R&D institutes belonging to the military forces, other state R&D institutes, institutes of universities and of the China Academy of Sciences and R&D departments of state and private owned companies, all of them active in R&D for security.

Brazil

The central agency for science and technology in Brazil is the Ministry of Science and Technology and Innovation (MCTI), which includes two main funding agencies: the CNPq and Finep. The CNPq, National Council for Scientific and Technological Development, is the main research funding agency aiming to promote scientific and technological research and also to train and qualify researchers in the country and abroad. Finep (the Studies and Projects Finance Organization) supports economic and social development by fostering innovation in public companies, universities, technological institutes and other institutions in Brazil.

The Ministry of Defence (MoD) is also important actor in security-related research. The MoD's Science, Technology and Innovation Assessment Commission for National Defense (*Comissão de Assessoramento de Ciência, Tecnologia e Inovação para a Defesa Nacional*, COMASSE) coordinates MoD-led security and defence research & development activities.

4.3.3 Thematic priorities

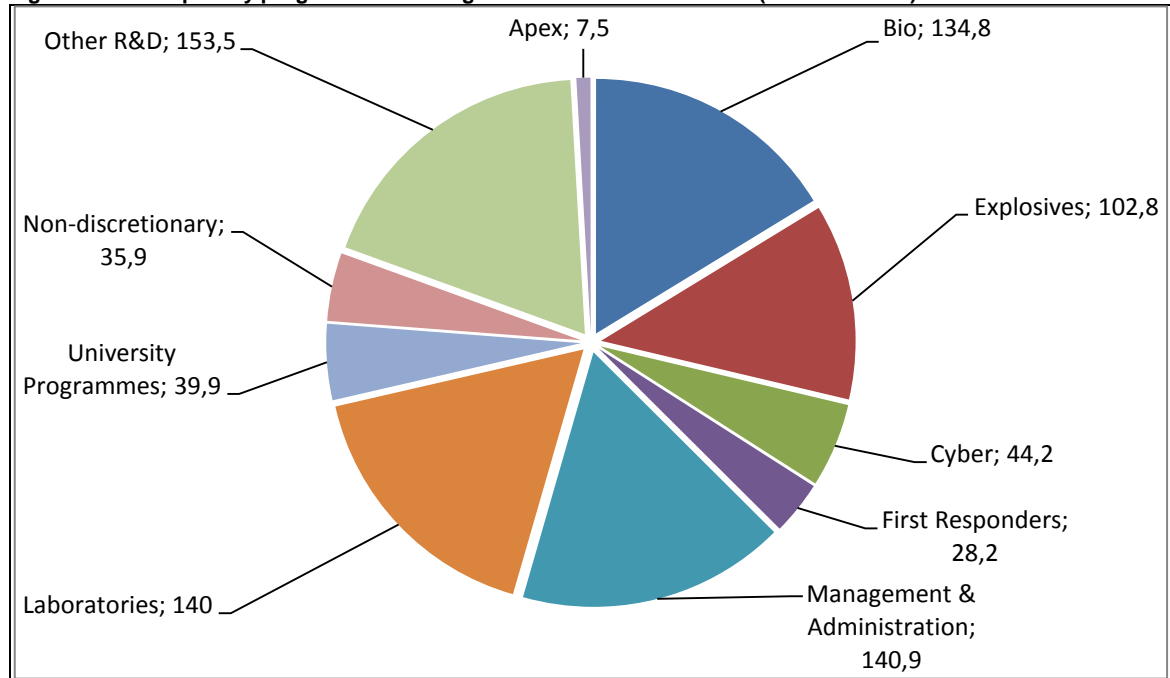
Thematic priorities for security R&D are heavily dependent on general context, including strengths and weaknesses of the national innovation system and security environment. These are different in different countries. However, some common themes are also emerging.

One of those is cyber security. As our dependence on computer systems as well as the number of computer incidents are increasing so too policy makers' attention to protection computer networks from cyber attacks. In all selected countries cyber security is either officially set as one of the main priorities for security R&D or this can be reasonably assumed based on indirect indicators.

Explosive detection also seems to be a major priority in several countries, including the US, Russia and Israel. Biometric systems based on various principles is yet another major area for security R&D in particular in the US and Japan.

In general, there is not much systematic information on the security R&D thematic priorities. Such information supported by budget allocations is available only for the US. It is presented on Figure 4.6.

Figure 4.6 S&T's priority programmes funding breakdown for the FY 2011 (in million USD)



Source: S&T Directorate: FY 2011 in Review.

Six technical divisions in the S&T Directorate also provide an indication of the main priorities for the DHS's R&D:

- Borders and Maritime Security Division;
- Chemical and Biological Defence Division;
- Cyber Security Division;
- Explosives Division;
- Human Factors and Behavioural Sciences Division;
- Infrastructure Protection and Disaster Management Division.

For comparison Russian STiS has five thematic centres:

- Weapons and personal (body) armour;
- Surveillance, forensic and detection equipment;
- Communications technologies and systems;
- IT and information protection;
- Special transport vehicles.

4.4 Lessons from the security R&D in major third countries and recommendations for the EU

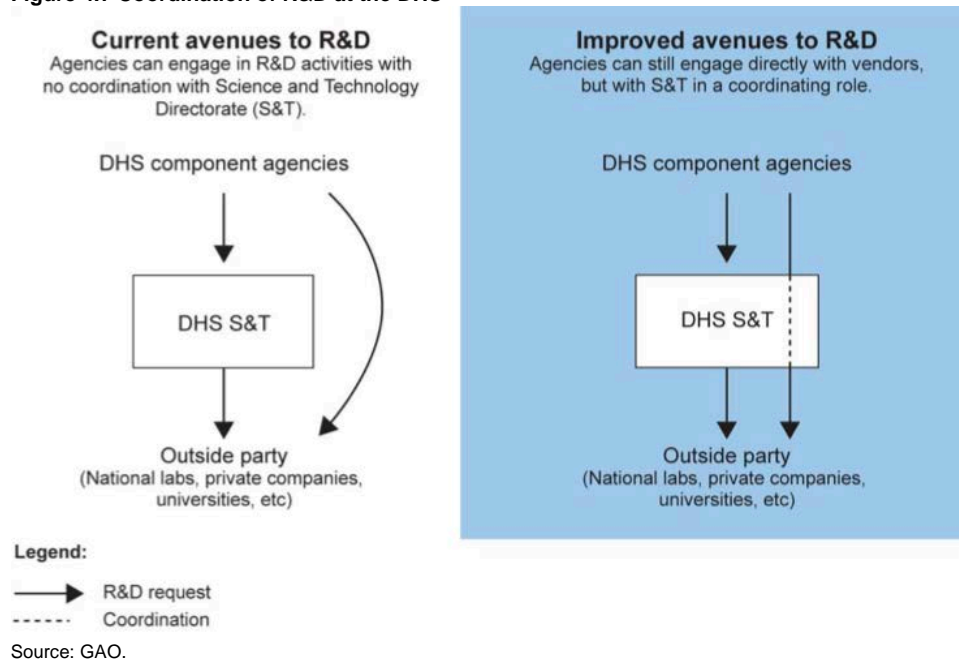
The seven countries covered in this report differ enormously in terms of their security environment, policy priorities, institutional context, technological advancement and other factors. It is difficult therefore to draw some common themes and lessons that could be easily applied to the EU context. In addition, detail information on security R&D programmes including their comprehensive evaluation is essentially limited to the United States. This is why this section focuses on the US experience in organising and conducting security R&D more specifically within DHS' Science and Technology (S&T) Directorate. Nevertheless, one broad conclusion that applies to all countries in the report can be still drawn.

Lesson 1. National context and policy priorities matter a lot in the field of security R&D. The perception of the security threats have direct implications for budget allocations to security R&D and its thematic priorities. National institutional context to a large extent determines the main actors in security R&D. In countries with a strong military R&D establishment such as the US, Israel and Russia security R&D tend to follow the military model of R&D and innovation, with public security agencies providing by far the largest share of funding and determining the main priority areas for R&D. In Japan and Korea private companies play a leading role in funding security R&D, which is driven mainly by international market prospects for a particular technology.

The DHS S&T Directorate was created from scratch in 2003 and given complex responsibilities. As many young organisations it has experienced many problems. It has received a fair share of criticism over its ten years of existence. One of them dealt with the risk of duplication of R&D work. This lack of coordination led to overlapping contracts. For example, the TSA awarded to different manufacturers almost identical contracts to develop algorithms to detect the same type of explosive.

To reduce such risk, S&T has recently acquired the ability to coordinate all R&D efforts among DHS components (Figure 4.7 below).

Figure 4.7 Coordination of R&D at the DHS



Lesson 2. Security R&D is in many aspects a new field where an institutional framework is still in the process of active evolution. This increases the risk of duplication of R&D efforts. This risk is amplified by often overlapping responsibilities in the security field (e.g. in cyber defence). In the European context this risk is further increased by the necessity of coordination between the EU and member states. In designing security R&D programmes the European Commission should pay a special attention in identifying mechanisms to reduce such risks.

In another step to mitigate the risks of unnecessary duplication and to be more responsive to customers' needs the S&T Directorate has instituted procedures called Integrated Product Teams (IPTs) to solicit input from the operational components of the DHS, to work with the components in identifying technology gaps and needs, and to develop mechanisms to meet those gaps and needs.

The goal is to identify technology solutions that can be developed and delivered to the acquisition programs of operational units within three years.

The IPT process explicitly recognizes the other DHS components as the consumers of the S&T Directorate's R&D efforts. Each IPT is focused on a different topic and brings together decision-makers from DHS operational components and the S&T Directorate as well as select end-users. Each IPT consists of customer representatives, whose role is to identify gaps in capability; providers from the S&T Directorate, whose role is to provide technical solutions; acquisition officials and/or financial officers, whose role is to validate and execute future acquisition plans; and end-user representatives, whose role is to provide the end users' perspectives. Congress and other observers have generally taken a positive view of the IPT process.

Lesson 3. Security R&D should be oriented to customers' needs. This requires close involvement of first responders and other operational agencies in setting R&D programmes' directions and providing feedback on their implementation.

Since 2010 DHS S&T has prioritised meeting the urgent operational needs of various DHS components and first responders and delivering useful products more rapidly than the typical decade-long R&D cycle.¹⁸¹ To achieve this S&T has shifted its focus on the late stages of R&D. To provide a direct route for first responders to communicate with S&T, the directorate has established the TechSolutions program (an email address for first responders to communicate with the S&T Directorate through the Tech Solutions program has been created). The goal of TechSolutions is to field technologies that meet 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements.

Partnership with the private sector is one of the S&T's top priorities and their main goal is to transfer useful technologies developed by the S&T Directorate to the market. More specifically SMEs have been identified as an important engine of innovation and job creation and as a result, the Small Business Innovation Research (SBIR) Programme was created in order « *to develop technology solutions to homeland security issues that are innovative and accelerate transitions into the marketplace* ». Since 2004, SBIR awards have produced 31 patents and 42 products on the market.¹⁸²

The S&T Directorate even set up a dedicated office, namely the Commercialization Office, to develop and implement « *programs that identify, evaluate, and commercialize technologies into products or services that meet the requirements of the Department of Homeland Security's stakeholders* ».

Lesson 4. Late stages of R&D are often critical for successful introduction of a product to the market. The European Commission should fully implement the pre-commercial procurement instrument set out in Horizon 2020 for security R&D as it proposed in its Security Industrial Policy (COM (2012) 417 final).

Another objective of DHS R&D strategy is to maximize return on investment in R&D by pursuing active collaboration with other R&D organisations. The S&T Directorate has set partnerships with Universities all over the US to meet its needs. S&T supports some twelve university-based Centres of Excellence (COE) which « *pursue a mixed portfolio of basic and applied research addressing*

¹⁸¹ Written testimony of S&T for a Senate Committee on Homeland Security & Governmental Affairs hearing titled "The Department of Homeland Security at 10 Years: Harnessing Science & Technology to Protect National Security & Enhance Government Efficiency, July 17, 2013, <http://www.dhs.gov/news/2013/07/17/written-testimony-st-senate-committee-homeland-security-governmental-affairs-hearing>".

¹⁸² Ibid.

both short- and long-term homeland security needs (...) and the education of promising students in Homeland Security-related Science, Technology, Engineering, and Mathematics (HS-STEM) fields». A COE federates several universities under in specific research area: i.e. the Centre for Explosives Detection, Mitigation, and Response, led by Northeastern University and the University of Rhode Island or the National Transportation Security Centre of Excellence, led by Texas Southern University in Houston, Tougaloo College, and the University of Connecticut. The R&D topics are aligned with the S&T Directorate's needs and are funded by the Directorate through the University Programs with the budget of approximately US\$37 million in 2012.

At the international level, the S&T Directorate has signed 12 bilateral agreements *to leverage its capabilities*. In 2011, it had 134 active bilateral projects, including US\$15 million in contributions from international partners.

Lesson 5. Close collaboration between different actors is helpful in leveraging R&D investment and fostering new ideas. The Commission should continue its efforts in promoting cooperation between public and private sector organisations within Horizon 2020.



P.O. Box 4175
3006 AD Rotterdam
The Netherlands

Watermanweg 44
3067 GG Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com

W www.ecorys.nl

Sound analysis, inspiring ideas