EUROPEAN COMMISSION

Brussels, 26.7.2012
SWD(2012) 233 final

COMMISSION STAFF WORKING PAPER

Security Industrial Policy

Accompanying the document

Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee

Security Industrial Policy

Action Plan for an innovative and competitive Security Industry

{COM(2012) 417 final}

1.1. Introduction

Security is unmistakably one of the central concerns of any society. A safe and secure environment is the very basis on which any stable society is founded upon. Citizens need to be free of security related preoccupations if they want to live their lives freely and contribute to the well being of our society.

Our societies become ever more dependent on technologies, foreign supplies of energy and raw materials. The constant technological evolution of our society had countless benefits for our daily lives, but the growing performances of our energy, transport and communication networks has also led to an ever increasing technological dependency[1].

A vivid example of the consequences of a terrorist attack were of course the losses in the aftermath of the 9/11 attacks, which did not only lead to the death of over 3000 people but also had a dramatic effect on the worldwide economy. It is estimated that 9/11 caused losses in US productivity amounting to US$ 35 billion, 47 billion in total output and a rise in unemployment by almost 1% in the following quarter.[2]

Open data puts the direct cost of crime, terrorism, illegal activities, violence and disasters in Europe at EUR 650 billion / year (excluding bribery, corruption and money laundering) or about 5% of the EU 27 GDP (~billion 12.000 EUR in 2010).[3] At the same time we see an increase of natural disasters requiring crisis management technologies.[4]

The threats to which our society is confronted are permanently evolving, terrorist and criminals will always look for loopholes in our technologies and try to bypass our security systems. We need to be aware of the fact that no technology will ever guarantee a 100% security, but at the same time, no security concept is thinkable without the adequate technologies. A competitive EU security industry is the *conditio sine qua non* of any viable European security policy and for economic growth in general.

Many EU security companies are still among the world leaders in most of the segments of the security sector, thanks to their level of technological development and their high quality manufacturing. Recent forecasts, based on market developments, studies and industry predictions do however indicate that the market shares of European companies on the global market are bound to decrease constantly over the next years.[5]

On the one hand, many US companies are still the technological front runners, they additionally also benefit from a harmonised legal framework and a robust internal market.

---

1 See for example Global Risks 2011, Sixth Edition, An Initiative of the Risk Response Network, World Economic Forum, January 2011.

2 See Sandler, T. and W. Enders (2004). "An Economic Perspective on Transnational Terrorism" European Journal of Political Economy **20**(2): 301-316.
See also Report for Congress "The Economic Effects of 9/11: A Retrospective Assessment" (see: HTTP://WWW.FAS.ORG/IRP/CRS/RL31617.PDF)

3 See: http://www.eos-eu.com/LinkClick.aspx?fileticket=y0rpzCaYh7o=&tabid=318

4 For statistics relating to disaster in Europe see Annex I of SEC(2009)202, Impact Assessment accompanying the Communication on 'A Community approach for the prevention of natural and man-made disasters'.

5 See: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

This gives them not only a reassuring basis but also the benefit of a clearly recognised and distinguishable US brand, which proved to be a highly valuable advantage compared to EU companies in terms of international competition.

On the other hand, the Asian countries such as China are closing the technological gap that separates them from EU companies at an alarming rate. Without a technological advantage, the EU companies will be confronted with a nearly insurmountable competition, as the discrepancy in terms of production costs is largely disadvantageous for EU companies.

Industry and market forecast studies predict that the current market share of EU companies in the security sector could drop from roughly 25% in 2010 of the world market to 20% in 2020, if no action is launched to enhance the competitiveness of the EU security industry.[6]

In response to these challenges, the Commission made the security industry one of the essential parts of the EU 2020 flagship initiative "An Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage ".[7] Therein the Commission announced to launch a dedicated initiative on a Security Industry Policy.

This Commission Services Staff Working Document is the result of a dedicated analysis by the services of DG ENTR on possible areas and measures where the EU could launch policy initiatives in support of the EU security industry. It should be noted that this Document will not be followed by any legislative proposal.

Any possible future legislative policy measure on the Security Industry will be preceded by a dedicated Impact Assessment as well as thorough stakeholder consultations.

1.2. Consultation and expertise

External expertise

In the context of this analysis, three different studies were commissioned to an external contractor[8]:

- Competitiveness of the EU Security Industry;
- Regulatory Framework and Certification/Conformity Assessment Procedures in the Security Sector (referred to as SECERCA study in the footnotes); and
- Pre-commercial Procurement in the field of Security.

A further study on the civil-military synergies in the field of security is currently in its final stages.[9] In addition, a previous study undertaken by DG ENTR on "Industrial implications in Europe of the blurring of the dividing lines between Security and Defence"[10] was also used.

---

[6] These estimations are based on the studies performed by ECORYS and on estimations made by Visiongain and HSRC

[7] See: **HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/INDUSTRIAL-COMPETITIVENESS/INDUSTRIAL-POLICY/INDEX_EN.HTM**

[8] The three studies can be found on the website of the FP7 security research theme: **HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM** .

A highly valuable contribution in the understanding of these issues is the work of the FP7 (7th Framework Programme, a list of acronyms used in this report is contained in the annexes) research project EUSECON (A New Agenda for European Security Economics)[11]. This project analyses the economic and social costs of terrorist attacks and anti-terror policies.

Stakeholder Consultation

A number of stakeholders were consulted throughout the analytical process, through both public and targeted processes.

An online public consultation was held from the 14th of March until the 15th of May 2011. The Commission received in total 59 responses to this public consultation. It should be underlined that despite the relatively low number of participants, all the relevant actors and stakeholders of the security sector participated. Contributions were received from stakeholders in 13 countries (one additional participant did not specify his country of origin), including 2 EFTA countries. The respondent's background was spread over the following areas: large enterprises 32%, business associations 22%, SME's 19%, national administrations 7% and NGO's 7%. The results of the public consultation can be found throughout this Staff Working Document and under the Annex 2 "Results of the Public Consultation".[12]

A series of targeted consultations were also held in the context of conferences and public/private debates.

- On 9 February 2011, a "High Level Public-Private Security Roundtable" was organised by the main European business association for security companies, the European Organisation for Security (EOS) together with the Commission.[13]

- A further consultation took place on the 23rd of May, the "High Level Conference Defence and Security Industries and Markets" which was organised by VP Tajani and Commissioner Barnier.[14]

- On 29 September 2011 a Workshop was organised with CEN, CENELEC and ETSI on standardisation in the security area. A summary can be found in Annex 1.

---

9 Once finalised, the study will be made available at: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

10 See: HTTP://EC.EUROPA.EU/ENTERPRISE/SECTORS/DEFENCE/FILES/NEW_DEFSEC_FINAL_REPORT_EN.PDF

11 See: HTTP://WWW.ECONOMICS-OF-SECURITY.EU/EUSECON

12 See:HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/FILES/DOC/PUBLIC_CONSULTATION/RESULTS_OF_THE_PUBLIC_CONSULTATION_ON_AN_INDUSTRIAL_POLICY_FOR_THE_SECURITY_INDUSTRY_EN.PDF

13 See: HTTP://EC.EUROPA.EU/AVSERVICES/SERVICES/SHOWSHOTLIST.DO?OUT=PDF&LG=EN&FILMREF=75367 and HTTP://WWW.EOS-EU.COM/LINKCLICK.ASPX?FILETICKET=YHFFMB11COE%3D&TABID=322

14 See: HTTP://EC.EUROPA.EU/ENTERPRISE/SECTORS/DEFENCE/CONFERENCE/INDEX_EN.HTM

- On 14 October 2011 a Conference on "Competitiveness through Standardisation" was held in Brussels. One of the round tables addressed "Standards as a tool for security industrial policy", the results of which can be found in Annex 1.

- On 18 October 2011 a Workshop on "Security Industrial Policy" was held in Brussels, the results of which can be found in Annex 1.

- On 21 March 2012, the second "High Level Public-Private Security Roundtable" was organised by the main European business association for security companies, the European Organisation for Security (EOS) together with the Commission.[15]

The results of the consultation were fully supportive regarding the initiative of the Commission. The main aspects of the problem definition were fully supported by a large majority of the stakeholders, both from the public and the private sector (i.e. by ~ 80% of the respondents of the public consultation). The need for the EU to launch dedicated policy initiatives to strengthen the EU security industry was also widely acknowledged (i.e. by 87% of the respondents of the public consultation).

The minimum standards of the Commission for consultations have all been met.

2. CONTEXT

Security as a national prerogative

The underlying problem faced by the EU security industry is that security policy is still very much a national prerogative, where Member States delegate a limited amount of authority to supra-national entities.

This is emphasized even further by the diverging threat perceptions and assessments in the EU Member States. Each Member State has its own specific cultural and geopolitical background which directly influences its security priorities. Some countries have to deal more often with natural disasters like earthquakes or large forest fires, while others have repeatedly been the victims of terrorist attacks.

However, the EU has already found ways to overcome this problem, for example in the area of airport security, where whilst it is left up to Member States to use certain screening equipment or not, if they use it they have to follow performance requirements set by the EU.

The issue of diverging threat assessments among the Member States has already been addressed by the Commission Communication: "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", which called for a common all-hazards approach to threat and risk assessment: *"The EU should establish by 2014 a coherent risk management policy, linking threat and risk assessment to decision making."*[16]

Policy developments

---

15 See: HTTP://WWW.EOS-EU.COM/DEFAULT.ASPX

16 See: HTTP://EC.EUROPA.EU/COMMISSION_2010-2014/MALMSTROM/ARCHIVE/INTERNAL_SECURITY_STRATEGY_IN_ACTION_EN.PDF

So far, the main initiative addressing the issue of security industrial policy in the EU has been the "European Security Research and Innovation Forum (ESRIF)".[17] Between 2008 and 2009 more than 600 experts on security worked on an extensive analysis of the EU security sector, in particular regarding the medium and long-term challenges that Europe faces.

The final report of ESRIF was adopted on 23rd November 2009[18], providing a list of key messages, recommendations and an extensive list of security research topics for the EU over the next 20 years, called the "European Security Research and Innovation Agenda". The work of ESRIF provided the EU policy makers with a knowledge base for the measures to enhance the security of its citizens.[19]

The Commission subsequently published on 21 December 2009 a Communication setting out the Commissions' initial position on ESRIF's key findings and recommendations[20] The Communication emphasised for the first time the need for an industrial policy for the security sector.

3. PROBLEM DEFINITION

3.1. Market overview

3.1.1. Overview on the scope of the analysis

Defining the exact scope of the security industry is a difficult task:

Firstly, the security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcom, etc.). The production of security-related items is hidden under a wide range of industry and services headings. Statistics for these headings don't distinguish between security and non-security related activities.

Secondly, 'security' is not a stable concept. It varies with changes in the perception of new threats. The scope of the security industry changed after 9/11, to encompass new anti-terror activities; more recently cyber-crime came to the forefront.

Thirdly, from a supply-side perspective, procurers of security equipment and systems can be reluctant to provide information on security expenditures.

The definition of security industry used in the context of this Staff Working Document is the result of a cross-analysis of the most commonly used typologies of the security industry (i.e. the scope used by previous studies on the security industry (inside and outside of the EU), the scope of the FP7 Security Theme as well as the scope of the US Department of Homeland Security (DHS)). This resulted in the categorisation of the 2009 Commission study on the "Competitiveness of the EU security industry".[21]

---

17 See: COM(2009)691 final.

18 See: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/FILES/ESRIF_FINAL_REPORT_EN.PDF

19 The executive summary of ESRIF can be found in the General Annexes to this report: Table14: Executive summary of the "European Security Research and Innovation Forum"

20 COM(2009) 691 final.

21 See: HTTP://EC.EUROPA.EU/ENTERPRISE/NEWSROOM/CF/_GETDOCUMENT.CFM?DOC_ID=5579

The EU security industry can broadly be subdivided into the following sectors:

- aviation security;
- maritime security;
- border security;
- critical infrastructure protection;
- counter-terror intelligence (including communication);
- physical security protection; and
- protective clothing.

A list of illustrative examples for the different sectors encompassed in the security industry can be found in Annex 3.

3.1.2. Relative market size and employment figures

In the table below are some more details on the relative **market size** of the different sectors.

Table 1: Relative market size of the global and European security industry markets (indicative € estimates by sector)[22]

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

Source: ECORYS (2009)

The physical security protection, a traditional security market based on general security applications such as closed circuit TV (CCTV), access control, intrusion and fire detection, counts for nearly 40% of the total European market, with a market value ranging from €10bn to €15bn.[23] Border security as well as counter-terror intelligence are both estimated to, at least, represent €4.5bn of the European security market, while critical infrastructure protection has a market value within a €2.5bn to €3.5bn interval. Last but not least, the

---

22 See: HTTP://EC.EUROPA.EU/ENTERPRISE/NEWSROOM/CF/_GETDOCUMENT.CFM?DOC_ID=5579

23 See General Annexes: Figure 2 Public-private involvement in 'traditional' and 'new' security markets

aviation and maritime security sectors are both estimated to have a market value ranging from €1.5bn to €2.5bn.[24] The tables in the general annex (tables 7 and 8) give a more detailed view on the strengths and weaknesses of the EU security industry in the most relevant areas (Overview of market characteristics for specific equipment segments and SWOT analysis of the European Security Industry).

The global security market is worth some €100bn (2008 figure) with around 2 million persons employed worldwide in the security industry. The European security market has an estimated market value in the range of €26bn to €36.5bn (2008 figure).[25][26]

From a global perspective, North America (mainly the US) is the largest security market, with a current market share of around 40% or more. Europe is ranked 2nd in the global security market, with a market share ranging approximately from 25% to 35%. Despite the financial crisis, global demand for security equipment is expected to grow at a minimum of around 5% per annum, with the fastest growth in coming years expected to be mainly in Asia and the Middle-East.[27]

As regards **employment** in the security industry, it is estimated that around 180,000 persons work in the EU in the security industry (2011 figure). This figure includes 130,000 working directly for the security industry and another 50,0000 induced or secondary markets (i.e. subcontractors).[28]

3.1.3. Distinctive features of the security market

The EU security market consists of products/technologies and services. As present studies and stakeholder opinions have shown the main pressure of global competition will lie on the products/technologies sector as those form the vast majority of contemporary and potential future security related exports. The main question for security service providers will rather be whether they would still have access to EU made products/technologies in the future to foster and maintain the quality of their business or whether they would have to acquire these from the EU's competitors.

The security market has three distinctive features which differentiates it from the majority of the other industrial sectors. That is not to say that these features are not also common to other markets, they are however especially pronounced in the security markets, which is largely due to the national sensitivities on security matters.

(1) **Fragmentation of the market along national or even regional boundaries:** Security, being one of the most sensitive policy fields, is one of the areas where

---

[24] See: "Study on the Competitiveness of the EU security industry", chapter 2.3 "Market size estimates for the security sector":
HTTP://EC.EUROPA.EU/ENTERPRISE/NEWSROOM/CF/_GETDOCUMENT.CFM?DOC_ID=5579

[25] See table below: " Relative market size of the global and European security industry markets"

[26] For a country study, see for example a study financed by the German Ministry of Economics and Technology "Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen - Thema: Der Markt für Sicherheitstechnologien in Deutschland und Europa - Wachstumsperspektiven und Marktchancen für deutsche Unternehmen Schlussbericht", Berlin 2009.

[27] See: General Annexes: Table 1:Summary table: Main competitors

[28] Figures are based on the study on the Competitiveness of the EU Security Industry, the Study on Pre-Commercial Procurement in the field of Security (see in particular page 58) and EOS.

Member States are hesitant to give up on their national prerogatives[29]. This means in concrete terms:

Higher barriers to entry than in other sectors, in particular:

- higher investment costs associated with technology development and, also, with the transition from technology development to placing a product on the market. This is even more aggravated by the fact that in the security area there is often an asymmetric level of knowledge between the demand side and the supply side, thus making it difficult to bring research results quickly to the market.

- higher costs associated with securing markets (e.g. lobbying, marketing, commercial diplomacy). An important aspect to this is related to needs to 'educate' clients on technological possibilities and choices.

(2) **Societal/ethical dimension:** While security is one of the most essential human needs, it also is a highly sensitive area. Security measures and technologies often provoke the fear of a possible endangerment of privacy. Any attempt to introduce a security solution that could violate ethical values would lead to fierce societal reaction.[3031]

(3) **Institutional market**: In large parts the security market is still an institutional market, i.e. the buyers are public authorities. Even in areas where it is a commercial market, the security requirements are still largely framed through legislation.

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

The SMEs present in the security sector often have limited access to the market for larger scale public (and quasi-public) and major private security equipment and systems contracts. It appears difficult for SMEs to grow significantly.[32]

An example for this can be found in a case study financed by the Austrian Ministry for Transport, Innovation and Technology (bmvit).[33] Whilst the average increase of turnover

---

29 This was already clearly underlined in the Commission's Communication on ESRIF's key findings and recommendations (COM(2009) 691 final, see in particular page 4.

30 See: HTTP://WWW.ESCI.AT/EUSIPO/ASP14.PDF

31 This was already clearly underlined in the Commission's Communication on ESRIF's key findings and recommendations (COM(2009) 691 final, see in particular page 3. See also: "A comprehensive approach on personal data protection in the European Union" COM(2010) 609 final
HTTP://EC.EUROPA.EU/JUSTICE/NEWS/CONSULTING_PUBLIC/0006/COM_2010_609_EN.PDF

32 See: HTTP://EC.EUROPA.EU/ENTERPRISE/NEWSROOM/CF/_GETDOCUMENT.CFM?DOC_ID=5579, as well as "Ex-post Evaluation of the Preparatory Action for Security Research (PASR) - Interim Evaluation of FP7 Security Research – Final Report, January 2011", at:
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/FILES/DOC/INTERIM_EVALUATION_OF_FP7_SECURITY_EX_POST_PASR_FINAL_REPORT_EN.PDF

between 2007 to 2009 for companies active in the sector of critical infrastructure protection (as one "core-group" of the security industry) was at 19.2 %, the turnover for the 15 largest companies increased by 32.2%.

3.1.4. Competitiveness of the EU security industry

The estimations on the general market evolutions detailed in this analysis are based on the results of the four studies launched by the Commission services as well as on industry forecasts.

The Commission services will, in order to remedy this lack of data, develop an empirical basis on which more reliable figures on the security markets could be established. Cooperation with EUROSTAT as well as the main trade associations is essential to such an undertaking. The 2009 study on the competitiveness of the EU security industry could serve as an initial starting point for such an analysis.

The current market situation

To this date, the competitiveness of the EU industry is acceptable in a number of segments. EU companies are still among market leaders and benefit from a relative technological advantage and high quality manufacturing compared to some of the emerging countries in Asia. The forecasts made by the EU security industry on the future competitiveness of the EU security companies are however less encouraging.

The EU is not in a position of being the sole producer of certain innovative technologies nor can it sell technologies at prices below those of the US and Chinese competitors. Chinese companies are closing the technological gap that separates them from EU and US companies at an increasingly fast rate.[34] These prospects are further darkened by the reality that few if any EU company will be able to compete on an equal level with Asian companies in terms of production cost.

Illustration on burglar and fire alarms:

A concrete example for this evolution is the segment of burglar and fire alarms. EU companies are among the front runners in the world wide competition and have generated considerable benefits in terms of external trade. The recent market evolutions as well as the stakeholder consultations do however reveal a rather bleak outlook. As shown in the two tables below, the trade balance and the competitive advantage of EU companies, after having peaked in 2009, is now facing a progressive decline.

It should be noted that the alarm systems represent a highly important segment in terms of economic size, with a market size of EUR 4.5 Billion or 50% of the physical security

[33] PlanConsult Holding (2010): "Studie betreffend das Potenzial der österreichischen Sicherheitswirtschaft und deren Entwicklung 2007 bis 2010 (ohne Bewachungsunternehmen)"

[34] A current example for this development is the Chinese producer of scanning equipment Nuctech, created in 1997, which is pushing strongly on the worldwide market as a direct competitor of EU companies. In general terms, China is encouraging the development of home-grown technologies, ranging from radio communication to body scanners.
See: HTTP://BLOGS.WSJ.COM/CHINAREALTIME/2011/04/22/INVASION-OF-THE-CHINESE-BODY-SCANNERS/

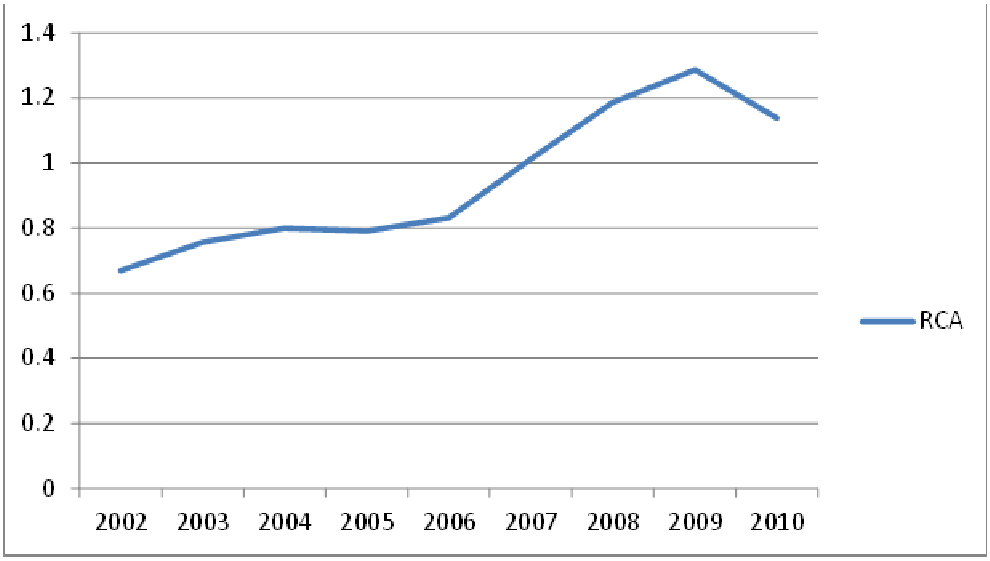
market. A detailed analysis of the competitiveness of this industry segment can be found in the attached Annex 7 "Competitiveness proofing – two illustrative examples".

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

Year	Total extra-EU exports	Total extra-EU imports	Trade Balance
2002	217.4	355.6	-138.2
2003	256.0	398.0	-142.1
2004	304.0	453.3	-149.3
2005	314.7	497.5	-182.8
2006	378.0	576.5	-198.5
2007	497.3	579.9	-82.6
2008	660.1	608.6	51.5
2009	665.3	554.8	110.5
2010	599.1	602.0	-2.9

(source: ECORYS 2011)

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



(source: ECORYS 2011)

The main competitors

The main competitors of the European security companies often have a vast internal market and/or a very favourable regulatory framework.[35] The strongest player and most important competitor for the EU is the United States. The US is not only the biggest market, but US companies are often technical frontrunners in high-end security equipment.[36]

[35] See: General Annexes: Table 2: Breakdown US security industry market

[36] See General Annexes: Tables 2-4 for detailed information on the US security market and the main US companies.

Illustration on airport screening equipment: US comparison

The US represents the main competitor to the EU in the aviation security screening sector - and for the security industry in general – and is the largest single market for aviation security equipment and systems. In terms of factors shaping the business environment for suppliers of aviation security screening equipment and systems, two features of the US situation are of particular relevance:

- A single Federal authority – the Transport Security Administration (TSA) – is responsible for setting the approach to aviation security and technology adoption, for determining performance requirements, for evaluating and approving security equipment and, finally, for the procurement and deployment of equipment.

- The SAFETY Act provides for the reduction of liability risks for manufacturers and distributors of anti-terrorism technologies. Further DHS designation and certification[37] under the Act provides *de facto* approval of security equipment and technologies that is recognised in global markets.

Compared to the present EU situation, the US market is characterised by:

- Lower costs of supplying the market, both in terms of the costs associated with compliance (conformity assessment) and approval (certification) of equipment and systems, and more generally for securing markets.

- Lower uncertainty over the potential market size for new security products and technologies; there is a single US position on the utilisation of technologies and performance standards/requirements.

- Lower risk attached to investments in research, technology development and innovation activities, both because of more certain market potential and liability situation.

- Shorter 'time to market' for new security technologies and innovations.

A detailed analysis of the competitiveness of this industry segment can be found in the attached Annex 7 "Competitiveness proofing – two illustrative examples".

Israeli and Japanese companies have a strong position in high-end security equipment, but mainly cover specific niches such as IT and communication security. The Chinese and Russian markets show strong growth rates in the traditional physical security protection segment (CCTV, access control). However, Chinese and Russian companies produce mainly low-end security equipment and do not yet compete with the high-end oriented EU companies.[38]

[37] The Act provides for two levels of approval: (i) designation and a qualified anti-terrorism technology and, for more mature technologies, (ii) certification as a DHS approved product.

[38] See General Annexes: Table 1:Summary table: Main competitors

China

General overview

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

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

Main fields of activity

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

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

Japan

General overview

Currently, security is an important public concern in Japan and the size of the security industry is growing fast. In its analysis of the Japanese security industry, the US commercial Service indicates that this public concern is related to very high crime rates (mainly related to burglary), but also credit card and e-mail scams and identity theft. The size of the total Japanese security industry (including both the sales and installation of security equipment and security services) is estimated at a projected size of 4.6 billion ($5.7 billion) in 2010.

Main fields of activities

Five main segments can be identified within the security equipment market. Image/monitoring and access control were the leading markets in 2005 while image/monitoring equipment as well as sensors are the main expected growth segments. The US Commercial Service observes that school and town security (emergency alert systems) and also regional safety (mass notification systems) are emerging sub-segments (with a projected size in 2008 of €78 million).

Israel

General overview

Given the unstable political situation in the Middle-East and direct terrorist threats, security is a top priority in Israel. Both the defence and homeland security (HLS) industry are seen as a fundamental part of the national security of Israel. At the same time, HLS knowledge and experience is more and more seen as an interesting export product.

Several (government related) websites promote the Israeli HLS sector as an important trade and investment opportunity for foreign countries. The Investment Promotion Center (IPC, part of the Ministry of Industry, Trade and Labor), for example, identifies HLS & Public Safety as one of the main business sectors for investment, stating that 'Israel has earned a worldwide reputation for providing leading security solutions'.

The annual HLS industry turnover (2008) is approximately €2.7 billion ($4 billion). Approximately 25% of that turnover is related to export of security products. It is assumed that the HLS (including surveillance, see below) is comparable to the turnover of the Israeli military and defence industry (€4 billion / $5 billion in 2006). Employment within the HLS industry is estimated at 25,000 people, being therefore slightly smaller than the military and defence industry (35,000 employees).

Main fields of activity

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

Russia

General overview

The estimated value of the total Russian security market (including security services and equipment) was approximately €4.5 billion ($5.6 billion) in 2006. Approximately 20% of this total relates to the security equipment market (€1.1 billion in 2006). The rest of the security market is mainly related to security services (guarding services and physical protection). The Russian market shows high annual growth rates.

Main fields of activity

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

A crucial competitive advantage that mainly concerns US companies is the benefit of a large home market. Having a harmonised market of over 310 million inhabitant's guarantees US companies access to a stable and reliable market, which in turn allows them to gain a critical mass and increases their competitiveness in terms of price and costs. The large and well known US market also gives these companies the advantage of "brand recognition".

For example, a large number of different standards and certification procedures exist in the EU alone for airport screening equipment. The US has only one. US companies can state for instance that their airport scanners are used in hundreds of airports in a country of over 300 million inhabitants. US manufacturers thus have a better and clearer reputation on a global scale than an EU manufacturer that can only refer to his comparatively small market.

This lack of a similar "EU brand" is especially critical if one considers that the central future markets for security technologies will not be in the Western Hemisphere but in emerging countries in Asia and the Middle East. To cite just some examples: China plans to build 80 new Airports by 2020, many major sports events (which are typically huge markets for security technologies) will take place in Asia such as the 2018 Winter Olympics in Pyeongchang (South Korea) and the 2022 FIFA World Cup in Qatar.

Stakeholder contribution on this issue, taken from the Public Consultation
"An EU-wide accepted certification scheme with one unique label (e.g. CertAlarm -> www.certalarm.org) in all Member States with the withdrawal of all national marks would allow the European security industry to present a united front on the global market."

3.2. The main problems of the security sector in the EU and their drivers[39]

The main problems of the EU security industry are the **highly fragmented nature of the EU security markets,** the **difficulty in closing the gap between research and market** and the **uncertainty of societal acceptance for security technologies**.

3.2.1. The fragmentation of the EU security markets

The main challenge the European security industry faces today is the highly fragmented nature of the EU security market. Divergent approaches have effectively led to the creation of 27 different security markets. This situation is not only an anachronistic rarity in the European Union, it has also several negative consequences both for the supply and the demand side:

Supply side:

- Commonly existing high barriers to market entry are considerably aggravated, particularly at the 'high-end' of the 'new' security market[40]. Instead of having just one central market to address to, the security companies have to multiply their efforts associated with securing markets by 27, which considerably raises the investment and commercialisation costs of security technologies[41]. These

[39] A problem tree can be found in Annex 6 "Structure of the Problem Definition".

[40] See Figure 2 of the General Annexes.

[41] See the illustrative example given on "Conformity assessment and certification of screening equipment under "chapter 7.1 Market Fragmentation" of this Staff Working Document.

disproportionate burdens often discourage the security industry (and SMEs in particular) to go beyond their national borders[42].

- True economies of scale can therefore not be realised which aggravates further the fragmentation of the market and weakens the competitiveness of the security industrial base. This fragmentation forced industry in some cases to foresee different product configurations for different target markets.

Demand side:

- National orientation of the security companies leads to a lack of competition among suppliers and users of security products are therefore not always able to buy the best security products at the lowest price.

- Eventually the demand side is forced to purchase a less controversial product which does however not entirely fulfil the technological requirements. In the end the demand-side has to opt for products that do not necessarily meet the initial technical requirements

Stakeholder contribution on this issue from a business association taken from the public consultation:

"Market fragmentation and the absence of a real European market results in high cost structures and therefore high costs for the Society. Within a harmonised market larger quantities could lead to better cost recovery in procurement and sales."

It should be noted that the level of fragmentation of the EU security markets is not equal to the usual fragmentation that can be found across other industrial sectors in Europe. Almost every industrial sector is characterised by some degree of fragmentation, the large majority does however have at least some common denominators, be it EU wide standards, harmonised certification systems or procedures of mutual recognition.

Producers of airport screening equipment are, for instance, faced with over 15 different certification procedures. This means that a producer of such technologies has to modify his product, in some cases substantially, if he wants to access new markets. This high degree of fragmentation has subsequently prohibited the creation of an internal market for security technologies. The only sector where a similar level of fragmentation can be found is the defence sector.

This particularity of the EU defence and security markets had been clearly laid out in the Impact Assessment that accompanied the proposal for Directive 2009/81/EC on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security.[43]

---

[42] A security company will often focus only on its own national market, not because of a lack of demand, but simply because it is not economically viable to repeat the same onerous procedure up to 27 times. This led in turn the EU security industry to be mostly nationally or even regionally oriented.

[43] See copy of this Impact Assessment (in particular page 11) at: **HTTP://EC.EUROPA.EU/INTERNAL_MARKET/PUBLICPROCUREMENT/DOCS/DEFENCE/IMPACT_ASSESSMENT_EN.PDF**

This negative effect of the fragmentation on the EU security markets was also unambiguously underlined in the above mentioned Commission Communication "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations": "The security industry in Europe needs to become more competitive and efficient. Up to now the industry suffered from the fragmentation of the markets that lead them to be nationally or even regionally oriented."[44]

The specificity of the high degree of fragmentation of the Security Industry has also been acknowledged and criticised throughout the stakeholder consultations organised by the Commission services.

Stakeholder contribution on this issue from a Member State taken from the public consultation:

"La sécurité : un secteur à part entière

Trop souvent associé à d'autres domaines connexes, le secteur de la sécurité se distingue pourtant de ceux-ci à de nombreux égards. Il est ainsi caractérisé par :

Une fragmentation importante de l'offre

[…]

Une fragmentation plus importante encore de la demande

Admis depuis déjà de nombreuses années, ce constat ne semble malheureusement pas s'améliorer. Ainsi, la demande est toujours caractérisée par d'une part des utilisateurs finaux publics (police, gendarmerie, sécurité civile, pompiers…) très éclatés qui se répartissent sur différents niveaux, du local jusqu'au national, et à travers de multiples services opérationnels. De l'autre, s'ajoute également les opérateurs qui représentent une part importante, voir peut-être majoritaire de la demande, et pour lesquels, trop souvent, la sécurité représente un investissement supplémentaire ainsi qu'une charge additionnelle sur ses opérations.

Cette fragmentation est encore accentuée au niveau européen par la forte disparité des législations nationales et des sensibilités vis-à-vis des libertés et droits individuels qui rendent encore plus difficile la constitution d'une demande plus homogène à travers l'Europe.

Ainsi, force est de constater que le marché intérieur reste encore qu'un concept vague et loin d'être réalisé dans le secteur de la sécurité."

Underlying drivers of the market fragmentation

Nearly each EU Member State has different regulations on performance standards[45] and certification systems/conformity assessment[46]:

(1) The absence of clearly defined **EU wide performance standards** introduces uncertainties for equipment providers in relation to the expectations of customers

[44] COM 2009(691) final.

[45] Performance standards: Standards establishing a set of minimum requirements to be fulfilled by systems, equipments or procedures, for any use related to security.

[46] Conformity assessment: shall mean the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.

regarding required performance and, in turn, for determining investments in technology/product development[47].

EU illustrative example:

Illustration: Secure Communications among police forces

A very concrete example for the lack of EU wide performance standards is the issue of secure cross border communication among police forces in the EU. Currently two different communication systems exist: "TETRA" and "TETRA-POL". The lack of interoperability between the two systems leads to severe communication problems between police forces of adjacent Member States such as Portugal and Spain. In the case of the BENELUX countries cross border communication is still gravely hindered, even though the three countries all use the TETRA-POL standard, because of a lack of interoperability between the technologies of two different producers. This situation has led to a series of cross border incidents, which in turn initiated a number of FP7 security research projects.[48]

The participants to the Public Consultation, independently form their background also largely supported this assessment.

Responses to the question: *Do you agree that the lack of EU wide standards for security affects the market fragmentation?*

Respondent profile	Do not agree at all	Do not agree	Agree	Agree very much	Do not know
A business association	1	2		9	1
A national administration			2	2	
An academic institution or think tank			2	1	
An individual				1	
Large enterprise (more than 250 employees)		2	2	14	1
Medium enterprise (between 50 and 249 employees, turnover less than €50 million)		1	1	3	
Micro or small enterprise (fewer than 49 employees, turnover less than €10 million)		1		5	
Non governmental organisation				1	3
Other				3	
Regional or local administration				1	
Grand Total	1	6	7	40	5

(2) The absence of **EU wide certification systems:** No common system of certification exists at a European level for security equipment and there is no mechanism of mutual recognition across countries[49]. A producer of security technologies has to go

[47] See: HTTP://WWW.CEN.EU/CEN/SECTORS/SECTORS/SECURITY%20AND%20DEFENCE/SECURITY/PAGES/DEFAULT.ASPX

[48] See for instance: the project EULER: HTTP://WWW.EULER-PROJECT.EU/ and the project DITSEF HTTP://WWW.DITSEF.EU/

[49] See the SECERCA study, "chapter 3 Overview: current situation, key themes and issues, main findings and conclusions": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

through the costly and lengthy certification processes for each and every country in which he wants to commercialise his technologies.[50]

EU illustrative examples:

Illustration: Conformity assessment and certification of screening equipment

An industry source has indicated, for example, that the cost of a single test of an Explosive Detection System (EDS) could be in the region of €65 thousand and for a liquid explosive system (LAGS) the figure may vary from €30 to €75 thousand; these figures relate to a single test procedure and do not take into account any repeat testing that may be required. The aforementioned products are relatively small systems and costs associated for larger systems are reputed to be significantly higher and may run into several hundred thousand Euros; for example, an amount of €100 thousand has been indicated for an 'imaging test' for a cargo scanner while a figure of €500 thousand has been indicated for the cost of the certification process for a biometric identity card model.[51]

Illustration: Conformity assessment and certification of alarm systems

Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. The costs of certification of an alarm system are on average (with a large spread depending on the nature of the product) at the level of EUR 200-300 thousand for full access to Europe including all tests. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to EUR 40-60k.

The negative effect of the lack of harmonised certification/conformity assessment procedures for security technologies on the market fragmentation was also widely acknowledged by all the participants of the public consultation, be they from national administrations, business associations, large enterprises or SME's. On the question "Do you agree that the lack of harmonised certification/conformity assessment procedures for security technologies affects the market fragmentation" 80% of the participants agreed and only 5% disagreed.[52] More detailed information on the responses to this question can be found in the table below.

[50] An overview to the general framework of the security regulation, conformity assessment and certification can be found in the General Annexes, Figures 6 to 9.

[51] See the SECERCA study, chapter "11.4)": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

[52] For more detailed information on the results of the public consultation see annex 2 results of the public consultation on an industrial policy for the security industry.

Responses to the question: *"Do you agree that the lack of harmonised certification/conformity assessment procedures for security technologies affects the market fragmentation?"*

Respondent profile	Do not agree at all	Do not agree	Agree	Agree very much	Do not know
A business association			4	6	3
A national administration			3	1	
An academic institution or think tank			1	2	
An individual				1	
Large enterprise (more than 250 employees)		2	2	14	1
Medium enterprise (between 50 and 249 employees, turnover less than €50 million)			2	3	
Micro or small enterprise (fewer than 49 employees, turnover less than €10 million)		1	1	4	
Non governmental organisation			1		3
Other			1	2	
Regional or local administration					1
Grand Total	0	3	15	33	8

(3) **Delays in certification procedures:** the slow speed of the certification process can mean that technologies are already outdated before they receive approval [53].

EU illustrative example:

Illustration: X-Ray Scanners

A French company, which is specialised in neutron generators and analysers, developed a detector that was complementary to conventional X-ray tomography for detecting explosives in baggage. However, in France the transposition into the public health code of Euratom Directive 96/29 greatly widened its scope, going beyond the maximum activation threshold of the Directive. In practice it prohibits any "activation" of consumer goods or food products, whatever the intensity. Because of this, the newly developed technology could not be used or tested in France, because all hold or cabin baggage may contain consumer goods or food products.

The absence of an EU wide certification system for security technologies has the following consequences on the EU security industry sector.

Consequences of the current situation on certification procedures in the EU:[54]		
Market conditions	Producers	Procurers/ users

[53] See the SECERCA study, "chapter 3 Overview: current situation, key themes and issues, main findings and conclusions": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

[54] See the SECERCA study, "chapter 3 Overview: current situation, key themes and issues, main findings and conclusions": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

□ A lack of transparency on product performance	□ Costs of complying with multiple national procedures;	□ Lack of transparency
□ Market fragmentation	□ Delay in 'time to market' of products;	□ Limited choice of suppliers
	□ Adaptation costs to meet national conformity assessment and certification procedures and standards;	
	□ Slow development and diffusion of new security technologies and solutions.	

3.2.2. The gap between research and market

For the EU security industry it is very often difficult to close the gap from research to market. In other words, when doing R&D on new technologies, it is often very difficult for industry to predict whether there will be in the end a market uptake, or to get some sort of guarantee that there will be a market. While this is a widely spread problem across many industrial sectors, it is an especially pronounced issue for the security industry. This is in particular due to the fact that the security market is very often an institutional market.[55] And this institutional market is mostly driven by catastrophic events/crises, as well as regulatory frameworks that set out security requirements.

The problem is aggravated by the fact that those that set the security requirements are most often not the same entities that provide R&D funding and which are again different from the procurement agencies[56].

Supply side:

For the supply side this often means that some of its R&D investment is simply wasted, as there is no subsequent market uptake. Given that it is mostly an institutional market, it is not really possible to divert this investment into other market segments.

It also means that companies often simply do not explore new, potentially promising R&D concepts, or are not bringing R&D concepts that are promising for the public sector quicker to the market.[57]

EU illustrative example:

The problem of appropriate R&D funding was described by stakeholders in the following way:

[55] See: the ESRIF report WG 9 page 195: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/FILES/ESRIF_FINAL_REPORT_EN.PDF

[56] For an overview of these differences, see chapter 2.1 of the "Study on Pre-commercial Procurement in the field of Security": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

[57] See Chapter 5 of the "Study on Pre-commercial Procurement in the field of Security": See the SECERCA study: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

"This is a classic question concerning technology push and market pull. There is always a gulf between the manufacturers, researchers and the market. Researchers often have difficulties to identify the market needs, as the market needs tend to be evolutionary rather than revolutionary which is always more interesting to a researcher. The entities that fund research are also often composed of technical people that share the same views, they hence tend to fund programs which are more aligned with technology push rather than market pull. This results in very little take up of the new technology and very long development times. Companies will only invest if they can address an available market rather than in blue sky research. It is therefore essential that the market is defined properly to overcome the lack of interest from the demand side to invest into R&D."

Demand side:

The consequence for the demand side is that it is often faced with a supply-driven R&D procurement, rather than a demand-driven R&D, given that industry wants to have a return on its R&D investment, which the demand cannot guarantee. However, this means that sometimes products are procured which are either not entirely fitted for the destined purpose, or they have a level of technology sophistication which is not required for the destined purpose and leads to a more expensive procurement.[58] Furthermore, in case that promising R&D concepts are not brought to the market or only brought to the market at a later stage, this means that technologies that could improve the security of the citizen are not available for public procurers. Eventually, similarly to the private sector, this means that a notable amount of public R&D investment is not used in the most efficient way.[59]

A series of initial initiatives, aimed at closing the gap between research and market, have already been launched by the Commission through the Security Theme of the 7th R&D Framework Programme, notably through the involvement of end-users in so called demonstration projects and through Pre Operational Validation activities[60].

Noteworthy is also Directive 2009/81 on the procurement in the fields of defence and security, which expressly provides that the contracting authority/entity may buy the product developed within an R&D contract without having to organise a separate procurement procedure if certain conditions are met.

- US illustrative examples

The US has clearly recognised the need to fill the gap between research and market in the security area. To that effect, the US has created two instruments:

---

58 See PCP study (chapter 4) and the SECERCA study ("chapter 3 Overview: current situation, key themes and issues, main findings and conclusions"):
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

59 See PCP study (chapter 4) and the SECERCA study ("chapter 3 Overview: current situation, key themes and issues, main findings and conclusions"):
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

60 **Demonstration Projects** are large scale research projects aimed at the integration, validation and demonstration of new security systems of systems. **Pre Operational Validation** involves directly – and supporting financially - end-user agencies (typically national or European authorities). This would shorten time to market and encourage market acceptance of new technologies when seen as part of a coordinated policy framework, including: standardisation, certification and regulation of innovative goods and services (and eventually facilitating coordination of procurement policies). The basic idea of a POV scheme is to support the *demand* side of research, rather than the *supply* side in their direct quest for new security solutions.

- The Small Business Innovation Research (SBIR) Program of the Department of Homeland Security (DHS), which is aimed at increasing private sector commercialization of innovations and at promoting the participation of SME's in homeland security research. The targeted areas are: Borders and Maritime Security, Chemical/Biological Defence, Cyber Security, Explosives, Human Factors/Behavioural Sciences and Infrastructure Protection and Disaster Management[61].

- The US Safety Act provides for legal liability limitations of anti-terrorism technologies. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability protections. The legal text states "The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of antiterrorism technologies from developing, deploying, and commercializing technologies that could save lives."[62] In other words, this instrument by promoting innovative technologies is aimed at closing the gap between research and market.[63]

This disadvantageous difference between the EU and the US was also underlined by the large majority of the industry participants to the public consultation, who stated that:

"The industrial base across the EU is however fragile in the sense that it is currently losing out to industries in countries such as the United States in a fiercely competitive global security market; in significant part owing to the support industries outside receive from their host Governments. The industrial policy framework for helping companies in the EU to compete in the security market is currently insufficient. Subsidies and related initiatives such as the US Safety Act mean that the security industry across the EU is losing its competitive edge in the global market."[64]

A specific issue with regard to closing the gap between research and market relates to civil-military synergies. The possible benefits for the security sector through the exploitation of synergies between civil and defence technologies remains to this date largely untapped. This is truer today than ever before, where certain technologies (e.g. electronics, telecommunications, surveillance, intelligence) developed by the defence sector could also be of relevance for internal security and vice versa.[65] In many cases civilian and military technologies share a common base which is then adapted to their specific needs. The same basic helicopter can for instance be modified for civilian or military utilisation.[66]

---

61 See: http://www.dhs.gov/files/grants/gc_1247254058883.shtm

62 See: **Federal Register** / Vol. 71, No. 110 / Thursday, June 8, 2006 / Rules and Regulations, page 33148.

63 For additional details on the US safety act see: SECERCA study chapter 9.5. Anti-terrorism technologies: the US SAFETY Act.

64 See: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/FILES/DOC/PUBLIC_CONSULTATION/RESULTS_OF_THE_PUBLIC_CONSULTATION_ON_AN_INDUSTRIAL_POLICY_FOR_THE_SECURITY_INDUSTRY_EN.PDF

65 See the study on CIV – MIL synergies: HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM and the study "The Industrial Implications in Europe of the blurring of dividing Lines between Security and Defence" HTTP://EC.EUROPA.EU/ENTERPRISE/SECTORS/DEFENCE/FILES/NEW_DEFSEC_FINAL_REPORT_EN.PDF.

66 An example for this is the transformation of the civilian helicopter EC135 by EADS - Eurocopter to a military helicopter the EC635. The EC135 is widely used amongst police and ambulance services and for

At the moment such synergies are partially taking place at the level of R&D cooperation. However, such synergies are currently neither sought more upstream at the level of capability development, nor more downstream at the level of standardisation. Such upstream synergies could help civil security users in better defining their research requirements with a view to ensure that the subsequent procurement is based on clearly defined needs. And such downstream synergies could as well help in reducing the gap between research and market, as the potential market would be bigger if "hybrid" standards were to exist, thus encouraging industry to explore promising R&D concepts.

Underlying drivers of the gap between research and market

The underlying driver of the gap between research and market is largely due to the lack of information about security technologies and capabilities from the side of the public authorities. This can be contrasted with the defence area, where public authorities are well accustomed in defining their future technology requirements and pulling the development through from research to the actual purchase[67]. This culture is, however, still missing in the area of civil security, not the least because in the civil security purchasing is normally more short term than based on a long term planning like in the defence domain[68].

Another driver is the fact that the security end-user is highly diversified between central and local governments, police forces and border guards, etc etc up to private end-users like commercial security service companies and infrastructure operators. In contrast in the defence domain there is generally only one customer, the Ministry of Defence[69].

3.2.3. The uncertainty of societal acceptance for security technologies

Another problem is the uncertainty associated to the societal acceptance of security technologies.

The societal acceptance of products and technologies is a general problem across many different industrial sectors. A good example for one of the liveliest debates of the last years was for instance the debate about the commercialisation of genetically modified food. There are however a number of specificities that distinguish security technologies from other areas.

The main reason for the specificity of the security market is that security technologies, devices and measures implemented often concern fundamental rights (e.g. privacy, freedom,

---

executive transport, the EC635 is marketed for troop transport, medical evacuation, cargo transport and armed combat support missions. The EC135 was adapted for military use through a reinforcement of the vital parts with bullet proof materials, two side-mounted Multi-Purpose Pylons with aerodynamic fairings for weapons systems, military grade communication and navigation systems. Other examples for civ mil synergies include: the internet (derived from the military DARPANET), radar technology (invented by the RAF in World War 2), digital photography (developed for satellite surveillance), nuclear research etc.

[67] See "Study on the Competitiveness of the EU Security Industry", pages 39 and 64.

[68] See: "The Industrial Implications in Europe of the blurring of dividing Lines between Security and Defence"
HTTP://EC.EUROPA.EU/ENTERPRISE/SECTORS/DEFENCE/FILES/NEW_DEFSEC_FINAL_REPORT_EN.PDF

[69] See Chapter 3 of the study "The Industrial Implications in Europe of the blurring of dividing Lines between Security and Defence"
HTTP://EC.EUROPA.EU/ENTERPRISE/SECTORS/DEFENCE/FILES/NEW_DEFSEC_FINAL_REPORT_EN.PDF

etc.)[70]. Any possible endangerment of these fundamental rights immediately raises concern among the population and often suscitate a very visible and concrete reaction.

A second aspect is that in, most cases, when security technologies, devices and measures are implemented, citizens do not have the choice to avoid them. For example, the only way to avoid security measures in airports would be not to travel by plane.

Another aspect is that security technologies are in many cases highly visible. Security cameras, access gates or security scanners are becoming more and more part of our daily environment. Everyone who goes to an airport is directly confronted to a detailed examination of their person and belongings. Passing through an airport checkpoint is also a very concrete experience and not something relatively abstract such as for instance the genetic code of our food. Security technologies are therefore often perceived as an intrusion of our personal sphere[71].

Responses to the question: *"Do you agree with the problem definition, that security products need to be privacy compliant from the development to the production?*

Respondent profile	Do not agree at all	Do not agree	Agree	Agree very much	Do not know
A business association	1	1	4	4	3
A national administration			1	2	1
An academic institution or think tank		1		2	
An individual				1	
Large enterprise (more than 250 employees)	1	2	6	8	2
Medium enterprise (between 50 and 249 employees, turnover less than €50 million)	1	1	2	1	
Micro or small enterprise (fewer than 49 employees, turnover less than €10 million)	1		2	3	
Non governmental organisation	1			3	
Other	1			2	
Regional or local administration				1	
Grand Total	6	5	15	27	6

Supply side:

These societal aspects have a very tangible effect for a company that wants to invest in security technologies. The security industry has to be sure that its products will be compatible with the general opinion of the public. The commercialisation of their new technologies would otherwise be impossible. The financial and human efforts that go into the development and production of a security product can therefore be easily wasted.

This uncertainty consequently reduces the willingness of the EU industry to invest in the development of new technologies, if they do not have an assurance of its economical viability. The lack of a proper technological implementation of societal and ethical aspects in the drafting of technological requirements thus ultimately weakens the competitiveness of

[70] EU Charta of Fundamental rights: HTTP://WWW.EUROPARL.EUROPA.EU/CHARTER/PDF/TEXT_EN.PDF. See: Article 6 Right to liberty and security; Article 7 Respect for private and family life; Article 8 Protection of personal data.

[71] See: HTTP://WWW.CPSI-FP7.EU/

the EU security industry. At the same time third country competitors who do not have such constraints can however develop technologies which can be commercialised in their own markets as well as in other non-EU countries[72].

EU illustrative example:

Illustration: Biometric screening

An example for this problem is the use of biometrics technologies for the screening of people at external borders. Further development of these technologies is currently hindered by the fact that no clear and transparent common criteria on privacy requirements have been established. Manufacturers of security technology cannot therefore make the necessary investments to develop privacy enhancing technologies as an integrated part of their technology solutions.

Demand side:

The demand side is also confronted with an unsatisfying situation, in which they cannot acquire the technology they initially intended to purchase. Eventually the demand side is forced to purchase a less controversial product which does however not entirely fulfil the technological requirements.

EU illustrative example:

Illustration: Terahertz scanners

A good example for this issue is the well known case of Security Scanners (know to the wide public as "Body Scanners"), based on mm-wave technology and used for access control and border checks (such as airports). Electromagnetic radiation in the mm-wave region can penetrate fabrics and plastics, so it can be used in surveillance to remotely uncover concealed weapons on a person. As much as this technology is efficient as much protest it generated from public and civil rights groups.[73]

The European Parliament bought six of those scanners for €725,730 in 2005 as a precaution measure after the 2001 al Qaeda attacks on New York and Washington. In October 2008, lawmakers had opposed a proposal allowing the use of full body scanners in the EU, unaware of the six unused devices lying around in the basement.[74] In the end the EP never unpacked these scanners and auctioned them away in 2010.

The results of the public consultation also reflected the importance accorded by all stakeholders, be they public or private, to the proper implementation of privacy concerns into technical requirements. On the question "Do you agree with the problem definition, that

[72] See the SECERCA study, chapter "9 Overview of US framework for conformity assessment and certification of security products": HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

[73] Body scanners can also be based on other technologies than the terahertz based systems, this does however not change the meaning of this example.

[74] See: **HTTP://EUOBSERVER.COM/9/29219**

security products need to be privacy compliant from the development to the production" (i.e. the concept of "privacy by design")[75] over 70% of the participants stated their agreement.

Stakeholder contribution on this issue, taken from the Public Consultation
Body scanners: some EU Member States do not allow the use of certain types of body scanners (x-ray backscatter). Although these systems comply with all standards, including Euratom, they are excluded. This blocks the EU internal market for security scanners and the development of a one-stop-security system.

Underlying drivers of the ethical concerns

The different ethical sensitivities among Member States

The approaches on the ethical issues related to security vary considerably among the Member States. A measure that is perceived by one Member States as completely uncontroversial could be unthinkable in another. A good example for this are for instance the different regulations of identity cards across the EU. While in some countries like the UK citizens are not obliged to have an ID card, in others countries like Germany, France and Portugal ID cards are not only obligatory, they also include a fingerprint of the card holder. The diverging regulations are often the results of lively debates among the citizens.

These varying perceptions of security have also been confirmed by a recent EUROBAROMETER report on the perception of internal security by the European citizens. A table, taken from this report, summarising the different priorities for EU citizens on internal security aspects can be found under Annex 5.

Two main questions arise out of this circumstance: which ethical standards should apply? and how should those ethical concerns be implemented into technical requirements?

While a certain number of general rules exist, such as for instance articles six to eight of the "Charter of Fundamental Rights of the European Union" (6 "Right to liberty and security"[76], 7 "Respect for private and family life"[77] and 8 "Protection of personal data"[78]), the technical translation of ethical concerns into legally binding technical requirements still remains largely unclear[79].

This already complex and sensitive situation is further complicated through the lack of a common EU wide approach on the technological requirements for privacy compliance of

---

[75] The principle of prrivcay by design implies that when a product is to be designed, it will be built in such a way that it will include the technical and organisational requirements to ensure the protection of the fundamental right to privacy and data protection of individuals. Privacy by default implies that a product is built in such a manner that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it. For instance the kind and amount of data processed are limited to the minimum necessary for a specific purpose; the storage of information processed is retained to the minimum necessary, there are mechanisms that restrict access to information processed to only authorised persons and do not allow for indefinite disclosure.

[76] *"Everyone has the right to liberty and security of person."*

[77] *"Everyone has the right to respect for his or her private and family life, home and communications."*

[78] *"Everyone has the right to the protection of personal data concerning him or her"*

[79] Under the Charter, the European Union (EU) must act and legislate consistently with the Charter and the EU's courts will strike down EU legislation which contravenes it.

security technologies. The approaches to security of the Member States vary considerably, some countries face fierce reactions to any possible intrusions to the privacy of citizens, while others can operate more freely, notably in the area of surveillance.

This issue has also been addressed in the recent Commission Communication "A comprehensive approach on personal data protection in the European Union"[80] (i.e. the possible creation of EU **certification schemes (e.g. 'privacy seals')** for **'privacy-compliant'** processes, technologies, products and services)[81].

Another aspect, connected to the societal dimension, which influences the structure of the EU security market, are the financial constraints related to the uncertain privacy requirements. A company will be less willing to invest in a technology or product if they do not have the assurance that they will actually be able to commercialise it. Moreover, the imposition of too cumbersome ethical requirements can also discourage companies from investing in the development of new technologies, should these appear to be economically unviable. An example for this are the already mentioned "Body Scanners".

Civil-military synergies

The possible benefit of an enhanced Civ-Mil cooperation for the civilian security sector is a highly sensitive topic. Civil rights movements have often stated their fear of a "militarisation" of the civilian sector. Most administrations have therefore refrained from launching effective initiatives to promulgate the integration of military technologies into security related applications.

The potential benefits of synergies have, however, been acknowledged on numerous occasions by the European Council through a number of declarations and conclusions.[82]

4. THE CURRENT SITUATION

4.1. Market fragmentation

The current situation is well exemplified with regard to **certification/conformity assessment procedures.** Member States have their own national certification systems in place with no mutual recognition of certifications taking place. In addition, the current situation can be described as quite uneven in that some Member States have for the same products certification procedures in place, whilst other Member States have no procedures in place. This uneven situation combined with a lack of mutual recognition would in all likelihood continue.

Another good example are **standards.** The Commission currently mandates on an ad-hoc basis the European Standardisation Organisations. Whilst not many European standards in the area of security exist, the current situation can, nevertheless, be described as a patchwork

---

[80] See: HTTP://EC.EUROPA.EU/JUSTICE/NEWS/CONSULTING_PUBLIC/0006/COM_2010_609_EN.PDF

[81] Examples for this privacy compliant processes are: "the right to be forgotten", "the principle of data minimisation", "privacy by design", etc.

[82] See for example European Council Declaration of 11 December 2008 on "Strengthening capabilities" HTTP://WWW.CONSILIUM.EUROPA.EU/UEDOCS/CMS_DATA/DOCS/PRESSDATA/EN/ESDP/104676.PDF

of standards rather than standards being developed with an overall design in mind for what the standardisation landscape should look like.[83]

The Commission submitted, in 2011, a so-called programming mandate (M/487) to the European Standardisation Organisations which aims at providing such identification, as well as providing a gap analysis. However, in itself if this programming mandate is not followed-up through specific standardisation mandates based on a clear prioritisation developed together with stakeholders, the current patchwork situation would continue to exist.

The central EU wide effort to address the issue of security on the level of security research is the FP7 security research theme.[84] A specificity of this theme is its end user and market oriented nature, bringing together representatives from national authorities, industry, research and end users. A number of these projects are thus also focussed directly on issues relevant to the competitiveness of the EU security industry such as standardisation, the economical aspects of security and interoperability.[85]

4.2. Gap between research and market

At the moment no **pre-commercial procurement** (PCP) is taking place at EU level (i.e. via FP7) in the area of security. Pre-commercial procurement is understood here as an approach to procure R&D services, whereby the Intellectual Property Rights (IPR) do not belong (exclusively) to the contracting authority[86]. Through such an approach the end-user will define its requirements at an early stage, thus allowing industry to focus R&D efforts on the technical specifications required by that end-user. At Member State level some very few Member States have been experimenting with PCP schemes. This is for example the case in the Netherlands. Again, we can speak of an uneven situation in the Member States which would continue under this situation.

It should be noted, that the Commission has recently published a proposal for Horizon 2020 which contains a specific PCP funding scheme. However, having such a scheme and making use of such a scheme are two pair of shoes. Given that so far few Member States have used PCP in the area of security, without a forceful promotion of this scheme by the Commission, it is unlikely that this scheme would be used for security under Horizon 2020[87].

So far neither the EU, nor Member State introduced legislation on **third party liability limitation** in the area of security. The Commission also has so far not taken any concrete

---

[83] The total list of existing EU wide security standards encompasses currently only some 66 standards. An initial list of these standards can be found under Annex 13 "Initial list of EU wide standards for security". In other sectors such as machinery some 500 EU wide standards exist. (HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/EUROPEAN-STANDARDS/DOCUMENTS/HARMONISED-STANDARDS-LEGISLATION/LIST-REFERENCES/MACHINERY/INDEX_EN.HTM)

[84] Created in 2007, the FP7 security research theme is a mission oriented research theme that addresses all areas of security (security of the citizens, intelligent border surveillance, critical infrastructure protection, crisis management, security and society etc.). With a budget of EUR 1.4 billion the security theme effectively represents over 50% of all the funding spent in the EU on security research. To this date, committed over EUR 800 million, spread over 203 projects with more than 1500 participants from 43 countries.

[85] A detailed overview of these projects can be found here:
HTTP://CORDIS.EUROPA.EU/FP7/SECURITY/PROJECTS_EN.HTML

[86] See COM(2007) 799 final.

[87] See the PCP study.
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

action with regard to third party liability limitation. Potentially, this could mean that some technologies may not be brought onto the market, as companies might consider the liability risks linked to these new technologies to be too high.

Civil-military synergies are currently being sought with the European Defence Agency through the so called European Framework Cooperation. Under this cooperation that has been asked for by the Council, there is an on-going coordination between the FP7 Security Theme and EDA's defence research activities. The aim is to synchronize this research in such a way as to avoid duplications and to profit from possible synergies. Without any additional initiative this cooperation would continue. However, this would mean that synergetic effects would be limited to the research domain.[88]

4.3. Integration of the societal dimension into industrial policy

It should be underlined that there exists no EU security industrial policy at the moment. This does however not mean that the societal dimension is not addressed at EU level. Currently activities are limited to R&D, where via its FP7 Security Theme the EU finances research projects in the area of security that look into how to better integrate ethical aspects into technology, e.g. through research into privacy by design technologies. It is afterwards left to industry whether they pursue these technologies and actually integrate them into products hitting the market.

In some areas it is likely that industry will indeed integrate ethical concerns, notably privacy issues, into its products. However, without any measures taken at EU level, it is unlikely that a more comprehensive approach will be taken by industry on this. It will remain a case by case consideration made by industry.

5. EU RIGHT TO ACT

Problem 1: The fragmentation of the EU security markets

Article 26 (1) of the Treaty on the Functioning of the European Union (TFEU) foresees that the Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market".

As the participants to the public consultation unambiguously stated, EU action is necessary to overcome the fragmentation of the security markets.

Problem 2: The gap between research and market

Article 173 (1) of the TFEU states that the Union and the Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exist. Actions to that effect shall be aimed inter alia at "fostering better exploitation of the industrial potential of policies of innovation, research and technological development".

---

[88] See: HTTP://WWW.EDA.EUROPA.EU/NEWS/11-09-16/EDA_AND_THE_COMMISSION_SIGNED_A_EUROPEAN_FRAMEWORK_COOPERATION_COORDINATION_LETTER_YESTERDAY

The participants of the public consultation were adamant on the need to improve the competitiveness of the EU security industry.

Problem 3: The uncertainty of societal acceptance for security technologies

Article 67 of the TFEU states that "The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States".

More than 70% of the participants of the public consultation stated that the societal dimension and more specifically the privacy compliance of security technologies was essential.

Security as a national prerogative

Whilst the Treaty of the European Union states that the essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security remains the sole responsibility of each Member State (Article 4, paragraph 2), there is an evident link between national security and security of the Union, which is further spelled out in the Treaty of the European Union. Thus, the Union "shall offer its citizens an area of freedom, security and justice" (Article 3, paragraph 2).

The EU right to act was also unmistakeably supported by the participants of the public consultation. Over 86% of the participants agreed that action by the EU would be necessary to reduce the market fragmentation and to reinforce the industrial base in the security area. Not a single respondent answered with "no".

The issue of a security industrial policy was also presented to and discussed with on several occasions to the Programme Committee of the FP7 Security Theme. The FP7 Programme Committee is constituted by representatives from Ministries (Interior, Research, Economics and Defence) from the EU 27 Member States and 14 associated countries.[89] A large number of Member State expressed their support for EU action during these meetings, no Member State objected on the presented policy measures.

A further aspect that should be taken into account when assessing the EU Right to act is related to the financial and technical capabilities in the Member States on security technologies. Only 7 (France, Germany, The UK, the Netherlands, Sweden, Austria and Finland) of the EU 27 Member States currently have a national security research programme. The FP7 security research theme represents more than 50% of the whole EU wide funding for security research. Only a very limited number of Member States have national capabilities to address issues related to security technologies, the large majority depend on EU initiatives.

It is very unlikely that the Member States will overcome those challenges on their own. As the participants to the public consultation and to the Workshops (among which representatives from Austria, Belgium, France, Germany, the Netherlands, and Spain) unambiguously stated, EU action is necessary.

---

[89] Switzerland, Israel, Norway, Iceland, Liechtenstein, Turkey, Croatia, the Former Yugoslav Republic of Macedonia, Serbia, Albania Montenegro, Bosnia & Herzegovina, Faroe Islands, Republic of Moldova.

6. OBJECTIVES

The general policy objective is to enhance the competitiveness of the EU security industry.

Increased competitiveness of the EU companies on a worldwide level, but also stronger competition inside the EU would allow the mostly public end users to purchase more adequate technologies with a better cost-benefit ratio. The central beneficiary of this evolution would be the European citizen, who would see his security enhanced.

The importance of the European Union for security of its citizens has been clearly stated in article three of the "Treaty on European Union"[90]as well as article six of the Charter of Fundamental Rights of the European Union[91].

The specific objectives are to reduce the fragmentation of the EU security markets, to reduce the gap between research and market, and to contribute to a better integration of societal aspects into security industrial policy. For each of these, operational objectives are reflected in the following table.

General and specific objectives

General objectives	Specific objectives	Operational objectives
Enhance the competitiveness of the EU security industry	Reduce the fragmentation of the EU security markets	• Improve mutual recognition of security products • Speed up standardisation in the area of security
	Reduce the gap between research and market	• Encourage Pre-Commercial Procurement • Analyse the need for a third party liability regime • Strengthen civil-military synergies
	Contribute to a better integration of the societal dimension into industrial policy	• Introduce societal aspects at the pre-commercial development level of products • Introduce societal aspects at the production process level

[90] Article 3 TEU: *"1. The Union's aim is to promote peace, its values and the well-being of its peoples. 2. The Union shall offer its citizens an area of freedom, security […]"*,

[91] Article 6 Charter of the Fundamental Rights of the European Union: *"Right to liberty and security - Everyone has the right to liberty and security of person"*

7. ENVISAGED POLICY INITIATIVES

The stakeholder consultations (public consultations as well as workshops) as well as the studies launched by the Commission services identified a progressive step by step approach to be the most suited and feasible approach to address the problems of the EU security industry.

The main advantage of such a step by step approach would lie in its analytical and progressive nature, i.e. no legislative initiative would be launched by the Commission without a prior consultation of all the relevant stakeholders (be they public or private), a thorough analysis of the legal framework and finally a dedicated Impact Assessment. The approach thus ensures that no legislative initiative could be initiated that could have a detrimental effect on the EU citizens, Member States or industry (large, medium or small enterprises).

Area	Initiative	Stakeholder approval rate
Certification	Step by step certification/conformity assessment procedures focused on certain priority areas or priority technologies where there is a clear EU added value.	71.19%
Standardisation	Step-by-step end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to ESO's	76.27%
Pre Commercial Procurement	A focused pre-commercial procurement scheme being built up via the possible future FP8 and/or CIPII funding.	76.27%

This approach would focus on initiatives that could probably be agreed with the European Parliament and Member States in the short-term and would identify areas where action should be taken in the medium-term or where further study was needed for the long-term.

7.1. Market fragmentation

Certification/conformity assessment procedures

The EU would introduce **certification/conformity assessment** procedures for certain priority technologies or areas. Based on the study commissioned, as well as intensive stakeholder consultations, it is considered that in a first step the following two areas should be covered by an EU wide certification scheme:

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

Both areas were chosen by the Commission services as they would:

- directly **address one of the central problems** of the security markets: fragmentation due to the lack of harmonised standards and certification procedures for security technologies;

- create **substantial benefits** and cost savings in each of the targeted segments;
- encourage the **establishment of an EU brand** for the concerned technologies, thus raising the profile of European technologies in comparison to their international competitors;
- be relatively **unproblematic from a political and technical point** of view, as they would build on a pre-existing legislative and technical basis and given that a strong support for EU action on those segments has been expressed by all stakeholders; and
- should be **uncontroversial on a societal level**, as they would not affect any ethical or privacy related issues.

A detailed explanation on these aspects can be found in the following passages as well as in the annexes 7 to 10.

Alarm systems

As regards alarm systems[92], there exist already some European standards, and in addition there exists an industry-led certification mechanism called CertAlarm. CertAlarm is the only European Accreditation endorsed certification scheme for the fire and security industry. CertAlarm has been initiated by the main business association for alarm systems in the EU, EURALARM. EURALARM encompasses national associations of 14 European countries, with around 700 companies having a total turnover of approx. 3.5 billion Euro, i.e. approx. 70 % of the total European market for alarm systems.

However, this system is faced with the problem that it is privately run and authorities of Member States have no obligation to accept certificates established under the CertAlarm scheme.[93] The potential for cost savings through the introduction of a harmonised EU wide certification scheme is therefore left untapped.

Stakeholder contribution on this issue taken from the Pubic Consultation:

"We would recommend to develop and push acceptance by Member States of pan-European certification schemes which will definitely remove intra-EU barriers to trade. The CertAlarm scheme could certainly constitute a basis for other similar certification schemes."

A detailed overview on the quantitative analysis of benefits of a harmonised certification scheme can be found in the illustration below and in Annex 8.

The Commission would address this issue by announcing the drafting of a legislative proposal setting up an EU-wide conformity assessment scheme for alarm systems. Such a legislative proposal would evidently be preceded by a **dedicated Impact Assessment**.

Illustration: competitiveness effects for alarms

The development of EU-wide harmonised standards and a common conformity assessment

92 See Annex 7: Competitiveness proofing, for a detailed overview.

93 See: HTTP://WWW.CERTALARM.ORG/CA/INDEX.PHP

procedure is expected to significantly reduce the certification costs for suppliers of intruder alarm systems where they serve multiple national markets in the EU. Moreover, it should reduce costs incurred in developing variants of products that are adapted to comply with differing standards and conformity assessment procedures at national level, which industry stakeholders consider often have limited actual impact on product performance for final customers. Removing the need for multiple certifications would enable suppliers of alarm systems to more rapidly access different parts of the EU market which, in turn, could benefit the organisation and scale of production activities. Further, by reducing delays in 'time to market' caused through multiple certification requirements, an EU-wide scheme should reduce the risk of new product innovations being replicated by competitors. Thus, an EU-wide scheme should increase the potential return and reduce the level of risk associated to investments in research and technology development.

Although a handful of major players dominate both the EU (and US) market, there remain 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. Conformity assessment and certification costs represent a proportionately higher share of total costs for SMEs and consequently a greater market access barrier. Accordingly, they are expected to benefit in particular from the cost savings resulting from EU-wide harmonised standards and certification procedures. In addition, an EU certification scheme should serve as a recognised mark of product performance and quality that can reduce the importance of 'reputation effects' of larger players and local companies, thus facilitating SMEs to trade across borders within the EU and even in global markets.

Overall, an EU-wide scheme is expected to increase market efficiency in the EU by raising the level of competition – both between EU companies and from outside the EU – and stimulate improvements in industry performance levels (e.g. productivity). It is not expected, however, that the reduction in costs resulting from an EU-wide approach would have a significant impact on the price competitiveness of EU alarm products in international markets. Nonetheless, a less fragmented EU market should encourage investment in research, technology development and innovation, which would have an impact on 'dynamic' competitiveness. Further, to the extent that it obtains higher market recognition than existing national schemes, an EU-wide certification scheme (providing for a corresponding EU security 'performance mark' or 'quality label') should contribute to strengthening broader international market awareness and acceptance of EU products.

Airport screening equipment

As regards airport screening[94] equipment there exists a whole body of EU legislation which sets out performance requirements for such equipment (see Regulation EC 300/2008, Regulation EC 272/2009 and Regulation EU 185/2010). However, this legislation does not contain the underlying conformity assessment mechanism which would be required so that a screening equipment certified in one Member State (according to EU performance requirements) is mutually recognised in any other Member States.

[94] Annex 7: Competitiveness proofing, for a detailed overview.

The Commission would announce the drafting of a legislative proposal that would set up an EU wide conformity assessment scheme, initially referring to the performance requirements already set out in EU legislation with regard to airport screening equipment. This legislation could easily be extended in the future when performance requirements will have been developed for related areas (e.g. port security). Such a legislative proposal would evidently be preceded by a **dedicated Impact Assessment**.

It should be underlined that, given that the performance requirements already exist at the EU level, through EU legislation there would not be a need to "harmonize" national security policies.

This legislation could easily be extended in the future when performance requirements will have been developed for related areas (e.g. port security).

Illustration: competitiveness effects for airport screening

By promoting mutual recognition of certification, the proposed EU-wide scheme should remove – or, in so far as Member States set more stringent requirements, reduce – the necessity for equipment to undergo multiple/additional national conformity assessment procedures. Consequently an EU-wide scheme is expected to reduce costs (direct and indirect) for conformity assessment and certification for suppliers of aviation security screening equipment which, for example, the European Organisation for Security indicates can be as much as € 2 million of a large scanning machine undergoing certification throughout the EU. Furthermore, a common certification scheme should reduce the 'time to market' between product development and commercialisation, which would be beneficial both to industry and to customers looking to deploy new security technologies and solutions.

Industry representatives also point to the benefits of a more unified and predictable market environment. The scheme should ensure that, once equipment is certified, it will be accepted throughout the EU as meeting the necessary EU performance requirements. Thus the potential market within the EU can more readily be identified and conditions for competition will be more transparent. This would provide *inter alia* for a reduction in the uncertainty associated to investments in research and technology development (RTD), which is expected to be of particular benefit for the aviation security screening sector given the importance of technology development in underpinning competitiveness. Overall, by contributing to a less fragmented and more transparent market, the proposed scheme would raise overall market efficiency and industry performance levels.

The introduction of an EU-wide scheme is not expected to significantly alter the overall structure of the aviation security screening sector in which the major players already compete at a global scale. For smaller players, it is thought unlikely that the proposed EU-wide scheme would significantly alter their capability to challenge the major equipment suppliers and systems integrators. However, in so far as EU certification serves as a recognised mark of product performance within the EU market, then it may facilitate SMEs to act as supplier to the major players in the sector.

At an international (global) level, in addition to providing an indicator of product performance, a unified EU approach should facilitate international dialogue towards greater reciprocity (notably with the USA) in the recognition of certificates that would reduce costs associated to third-country certification and enhance international market access for EU

certified products.

As regards **standardisation**, the Commission would instigate an end-user driven standardisation based on a careful identification of existing, national, European and international standards. As mentioned above, to this effect the Commission already submitted a so called programming mandate to the European Standardisation Organisations (M/487) which aims at providing such identification, as well as providing a gap analysis. Major gaps were identified in the following areas:

– Chemical, Biological, Radiological, Nuclear and ExplosivesCBRNE – minimum detection standards as well as sampling standards, including in the area of aviation security;

– Border security – common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers; and

– Crisis management/ Civil protection – standards for communication interoperability, as well as interoperability of command and control, including organisational interoperability, as well as mass notification of the population.

7.2. The gap between research and market

The Commission services would build on the **PCP** scheme to be built up via Horizon 2020. This scheme also foresees the possibility of a top-down PCP scheme, i.e. where such a PCP scheme would be organised via appropriate EU agencies. The Commission would make full use of this new funding scheme with regard to security research. Additionally, the Commission would encourage the Member States to launch similar initiatives on a national level, in compliance with Directives 2004/18 for non-sensitive and 2009/81 for security sensitive procurement.

Concerning **third party liability limitation** there is a strong request from industry to introduce something similar to the US Safety Act in Europe. However, there are clear limitations with regard to EU competence in this area, as well as to whether this would have a concrete effect on the competitiveness of the EU industry. All issues related to third party limited liability protection (legal, economic, etc.) would be further studied.

Regarding **civil-military synergies**, so far cooperation focused on the research area. However, the more downstream elements of such synergies have largely remained untapped. The idea is that there are some areas where "hybrid standards" could be foreseen, covering the civil and the military domain. A good example are Unmanned Areal Vehicles (e.g. relating to sense and avoid systems or airworthiness requirements) and reconfigurable and cognitive radio (also known as Software Defined Radio). Technology in these areas is very similar if not the same in the civil and military domain. In these areas the Commission, in close cooperation with EDA, would issue standardisation mandates.

7.3. The integration of the societal dimension

Concerning the **societal dimension**, an effort would be made to introduce this dimension at the stage of the production process. This means that an economic operator wishing to have

his production process audited for being "privacy by design" fit, would have to fulfil a set of requirements defined through an appropriate EU standard that would be mandated by the Commission to the ESOs. Such a standard could be modelled on existing schemes, such as for example the existing standards of the ISO 29100 family developed in the Privacy Standardization ISO/IEC JTC 1/SC 27/WG 5 «Privacy & Identity Management Technologies». It would, however, remain voluntary for companies to apply such a standard. There would, nevertheless, be a strong peer pressure.

Also at the level of the pre-commercial development of products the societal dimension would be introduced. This would be done by using the PCP scheme outlined above to also "test" the societal acceptance of new technologies.

7.4. Overview of the envisaged policy initiatives

This table gives a brief summary of policy initiatives envisaged by the Commission services as possible areas for EU action.

Policy area	Action
Certification	The EU would launch certification/conformity assessment procedures focused on certain priority areas or priority technologies where there is a clear EU added value. Based on the results of the studies and the stakeholder consultations the two following areas were identified to be the most promising: airport screening equipment and alarm systems.
Standards	The Commission would instigate an end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to European Standardisation Organisations.
Pre-commercial Procurement	Making full use of the pre-commercial procurement scheme being built up via "Horizon 2020". PCP would be organised in a top down approach, via agencies such as FRONTEX. The Commission would furthermore encourage the Member States to launch similar initiatives on their national level, in compliance with Directives 2004/18 for non-sensitive and 2009/81 for sensitive security procurement.
Third Party Limited Liability Protection	The Commission would launch a thorough analysis on all issues related to third party limited liability protection. (e.g. dedicated studies, public and targeted consultations of all relevant stakeholders in the EU). All possible options of liability schemes will have to be taken into account in the context of this analysis (e.g. the creation of a victim compensation fund, etc).
Civil – military synergies	The Commission would strengthen the synergies between civilian and defence technologies through a downstream coordination at the level of development of

	standards.
Societal aspects	The economic operator wishing to have his production process audited for being "privacy by design" fit, would have to fulfil a set of requirements defined through an appropriate EU standard that would be mandated by the Commission to the ESOs. Such a standard could be modelled on existing schemes, such as for example the ISO 9000 quality management scheme, but applied to management of privacy issues during the production process, e.g. the ISO 29100 family developed in the Privacy Standardization ISO/IEC JTC 1/SC 27/WG 5 «Privacy & Identity Management Technologies».[95] It would, however, remain voluntary for companies to apply such a standard. PCP schemes would be used to "test" the societal impact of new technologies.

8. THE EXPECTED BENEFITS OF THE ENVISAGED POLICY INITIATIVES

The launch of a successive set of policy measures on certification, standardisation and pre-commercial procurement is expected to have a highly positive effect on the EU security industry.

The step by step approach would ensure that the policy initiatives are based on a **thorough and well founded analysis** of the EU security markets. Thus enabling the Commission to identify the most appropriate and efficient policy measures needed to address the main currently existing obstacle for the creation of a true internal market for security: the fragmentation of the national regulatory frameworks.

8.1. Market fragmentation

The central envisaged EU action would be the development of adequate **EU wide harmonised standards and certification procedures** for alarm systems and airport screening equipment. This would not only open up the national security markets and develop the competition among the EU security companies, it would also reduce the cost of commercialising security products and improve the choices for end-users.

The expected positive consequences of harmonised EU wide certification procedures are:

- reduction of costs associated to multiple testing;
- facilitated access to markets;
- reduction of the "time to market";
- improved transparency of performance requirements and standards;

[95] See: HTTP://WWW.ISO.ORG/ISO/ISO_TECHNICAL_COMMITTEE?COMMID=45306

- enhanced competition among EU suppliers;
- reduction of costs for conformity assessment and certification (CAC) services and the development of security technologies;
- lower prices for security technologies

Producers of security technologies should benefit from the introduction of EU wide harmonised CAC procedures in the targeted sectors. The most evident being the reduction of costs associated to the multiple testing of security technologies across the Member States. The cost for CAC procedures of basic security technologies can amount to several hundred thousand Euros per Member State. Committing these costs just once, instead of multiplying them by 27 for each of the Member States, can enable producers to save several million Euros in the development and commercialisation cost of new technologies.

For the two targeted areas, the cost-benefit analysis shows that up to 29 million EUR yearly could be saved in certification costs. A detailed overview on the quantitative analysis can be found under Annex 8.

Alarm systems:

The total costs for certification and conformity assessment of intruder alarm systems is currently estimated to range between EUR 6.2 million and EUR 13.2 million per year. These costs cannot be reduced completely through a harmonised certification scheme.. After all, there is still need for a single certification and conformity assessment, and associated need for testing etc. It is nevertheless assumed that a single EU system reduces the cost associated to differences in technical rules and multiple testing/certification by three-quarters (75%). This would suggest a saving of EUR 4.7 million to EUR 9.9 million per year.

Airport screening:

A harmonisation of the certification and conformity assessment procedures for airport scanners would prevent all duplications at national level, which allows for considerable cost savings. The cost for certification and conformity assessment would thus amount to EUR 3 million (30 products * EUR 100 thousand). This implies that the impact of the harmonisation in terms of reduction of costs for certification and conformity assessment would amount to approximately EUR 19 million per year[96].

A common CAC procedure should also increase the transparency of the certification process, giving producers a better understanding of the required performance standards. A single EU wide CAC system should also improve the openness of the markets, thus facilitating the market access for the producers of security technologies. The particularly pronounced problem of the **hurdles to market entry** in the security sector should subsequently be reduced.

This facilitation of market access should have an especially **notable effect on SMEs**. As previously stated SMEs have a more limited access to financial resources and suffer the

[96] An assessment of the implied costs can be fund in the Annex 8: Background to quantitative analysis of certification.

most from the burdens imposed by multiple CAC procedures. The reduction of costs associated with moving to a 'one-stop' system with mutual recognition of certification would be greater (in relative terms) for SMEs.

Harmonising the certification procedures for airport screening systems and alarm systems should also have a positive effect on the creation of a clearer European identity for these technologies, a possible "EU brand". This "EU brand" should contribute to enhancing the global competitiveness of the EU companies with regards to their US and Chinese competitors.

As confirmed by the stakeholder consultations[97], a single CAC procedure would considerably **reduce the workload associated to the administrative burdens** for security companies and public administrations, thus freeing-up human and financial resources.

8.2. Gap from research to market

The launching of dedicated policy measures with regard to **pre commercial procurement** would strongly help in better aligning R&D projects with security requirements and end-user needs, thus contributing in closing the gap between research and market.

A tentative assumption of a 1% increase in the annual growth rate due to R&D support through a PCP scheme would lead to extra sales of 2 billion € and to **an increase in employment of up to 31000** (excluding the services sector). The employment figure is based on the world employment of 2 million in 2009, projected assuming a constant sales/employment ratio. The calculations in the table below detail the possible evolution from 2012 to 2020, given that the first results of the use of PCP/POV schemes in EU security research cannot be expected earlier. It should be noted that these are conservative estimations based on the results of the US SBIR programme.

An overview on the estimations can be found in the table below as well as under Annex 9.

Possible impact of a PCP scheme on the European security industry

	2012	**Prevision on the 2020 market value without the use of PCP schemes**		**Prevision on the 2020 market value with the use of PCP schemes**		**PCP impact**
		growth (in %)	Projected value in 2020	growth (in %)	Projected value in 2020	
European security market value (billion €)	17	3.5	23	4.5	25	+ 2
European security industry production (billion €)	22.7	2.6	28	4.5	33	+ 5
European security industry employment (thousands)	140	2.6	172	4.5	203	+ 31

As regards **third party liability limitation**, the Commission services would study in depth what the pros and cons, as well as political, legal, financial and technical limitations, burdens and boundaries of possible future measures in this area would be, and how such a liability limitation would effectively help in closing the gap between research and market.

[97] See: Annex 1: Summaries of the Workshops.

Finally, regarding **civil-military synergies**, the downstream coordination should have a positive effect on reducing the gap between research and market[98]. The establishment of hybrid standards should enable industry to achieve a better value for money on their investment in civ-mil R&D, given that it should allow them to address two different markets with one technology. This improved cost to benefit ratio should in turn create a better climate for R&D funding and encourage companies to augment their investments. The estimated **sales increases for security technologies** exemplified for infrared cameras, Command, Control, Communications, Computers, and (military) Intelligence (C4I), Radio Communication and UAV are in the vicinity of **EUR 2.8 billion**.[99] The estimated **increase in employment in the security industry is expected to be at approximately 17.000**.

A detailed overview on the estimations can be found in the table below as well as under Annex 10.

The four following fields were analysed on their potential for civilian military synergies:

- Infrared cameras
- C^4I (Command, Control, Computers and Intelligence)
- Radio-communications

Estimations on the possible benefits through the exploitation of civil military synergies

Civil Military synergies	**Increase in sales**		**Added employments**	
	Defence and Security	Only Security	Defence and Security	Only Security
Infrared cameras	EUR 450 million	EUR 440 million	2.800	2.750
C4I	EUR 300 million	EUR 900 million	1.875	5.625
Radio Communication	EUR 1.000 million	EUR 1.500 million	-3.125	9.375
Total	EUR 1.7 billion	EUR 2.840 bilion	1550	17.750

(It should be noted that the sales for defence technologies for C4I and Radio Communications are estimated to decrease over the next years. The increases for security technologies thus exceed the estimations for defence and security combined)

Infrared cameras: the exploitation of synergies in this sector only necessitates a coordinated R&D effort, which could be achieved through the existing European Framework Cooperation.

C4I and Radio Communication: are sectors where a downstream coordination and the development of common/hybrid standards for civilian and military use would be needed.

---

98 See the CIV MIL synergies study:
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

99 See Annex 10 "background to quantitative analysis of Civ-Mil synergies.

8.3. Societal aspects

The introduction of a voluntary EU standard for privacy by design compliant production processes would not guarantee that "privacy by design" audits will take place for all products and would be undertaken by all companies. However, given the technical difficulties in translating **fundamental rights** into technical requirements (which in essence would also mean 'aligning' ethical considerations throughout the EU), the voluntary auditing or production processes would seem a more feasible and reasonable approach. Also it can be expected that peer pressure will lead many companies to introduce voluntarily such an auditing system, similar to what can be seen for example with regard to audit system in the area of bio foods.

It would be possible through adequate **PCP** schemes to "test" the societal acceptance of new technologies in advance of their actual commercialisation. This way all the concerned stakeholders, i.e. end users, industry, societal groups could be involved from the early stages, thus guaranteeing adequacy and acceptability of the final technologies.

List of Acronyms

CAC	Conformity Assessment and Certification
CBRN	Chemical, Biological, Radiological, and Nuclear
CCTV	Closed Circuit TV
CEN	European Committee for Standardization
CENELEC	Comité Européen de Normalisation Électrotechnique
COM	Commission Communication
C4I	Command, Control, Computers and Intelligence
DHS	Department of Homeland Security
EC	European Commission
EDA	European Defence Agency
EFC	European Framework Cooperation
EFTA	European Free Trade Association
EOS	European Organisation for Security
ESA	European Space Agency
ESO	European Standardisation Organisation
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
ETSI	European Telecommunications Standards Institute
EU	European Union
EUSECON	A New Agenda for European Security Economics
FP7	Seventh Framework Programme
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GDP	Gross domestic product
ISO	International Organization for Standardization
MS	Member State

PCP	Pre Commercial Procurement
POV	Pre Operational Validation
R&D	Research and Development
SECERCA	Study on Security Regulation, Conformity Assessment & Certification
SBIR	Small Business Innovation Research
SDA	Security and Defence Agenda
SME	Small and Medium Enterprise
SWOT	Strengths, Weaknesses, Opportunities and Threats
TFEU	Treaty on the Functioning of the European Union
UAS	Unmanned Areal Systems
UAV	Unmanned Areal Vehicles

Annexes

A series of documents related to this analysis have been made available on the website of the security research theme:

- The executive summaries of the three studies carried out by external consultants can be found under the following link (under studies and Workshops):

HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM

Annex 1: Summaries of the Workshops

Summary of CEN/CENELEC/ETSI Workshop Launching Programming Mandate EC-M/487 on the 29th September 2011

The workshop was attended by around 80 stakeholders from industry, national and European standardisation organisations, as well as a number of national ministries. The objective of the workshop was to kick-off the work under the programming mandate M/487 on security standards. In particular, the meeting aimed at getting feedback from stakeholders about future standardisation priorities in the area of security.

There was unanimity that more standards were required in the security domain and that these standards should cover the broad range from interoperability standards to test protocols, etc. As to domains that would require standardisation as a priority, different stakeholders considered different areas as their first priority. However, some areas came up in several presentations, such as for example standardisation with regard to CBRN detection, secure interoperable communications, as well as border surveillance activities and critical infrastructure protection (in particular buildings and energy networks).

Summary of the Workshop on Security Industrial Policy:

The Workshop was held on the 18th of October 2011 in the representation of the European Commission to Belgium.

The participants (~100 persons) to the Workshop included a large number of representatives and key stakeholders from the EU Member States (Ministries of research, defence, interior and economics), Business associations (European Organisation for Security, German European Security Association, AeroSpace and Defence Industries of Europe), industry representatives as well as EU institutions (The EU counter terrorism coordinator, various DG's of the Commission).

The aim of the workshop was to confirm and validate the results of the public consultation held from March to May 2011. The Workshop was divided in four thematic sessions: Certification and standardisation, Pre Operational Validation/Pre Commercial Procurement, Civ Mil Synergies and Third party Limited Liability.

Main messages from the sessions:

Certification and standardisation

- It was commonly acknowledged that a harmonisation of the currently fragmented certification systems and standards in the EU is crucial not only to improve the security of the European citizens, but also essential to guarantee the competitiveness of the EU security industry on a global scale.

- Harmonised certification systems should not only reduce the time to market, but also allow better cost to benefit ratios and reduce the current administrative burdens.

- The main areas identified by the stakeholders as potential areas for initial harmonised certifications procedures were security scanners and intruder alarms systems.

Pre Operational Validation/Pre Commercial Procurement,

- The majority of the participants expressed clear support for a wider use of POV/PCP schemes in the area of security research. This was underlined by those Member States who already gained first experiences with these schemes in security research (the Netherlands and Spain) and by a number of industry representatives and business associations. The importance of POC/PCP in terms of global competition was also emphasized by the participants. It was noted that the US has already made considerable efforts in this area, which resulted not only in the development of highly successful technologies, but lead also to the creation of a several new companies.

- Participants stressed that IPR issues needed to be thoroughly addressed in any future POV/PCP. Furthermore, the policy framework needed to be clearly set out when embarking on a POV/PCP.

Civ Mil Synergies

- The issue of a better exploitation of Civ-Mil synergies was described by the participants as an area where the EU is in its fledgling stages. While the US has already addressed this issue through the "Office of Technology Transition" in the Department of Defence, the EU has not yet developed a coherent approach on this issue. A regrettable negligence in these times of financial crisis.

- The potential and limits for Civ-Mil synergies should therefore be explored in a thorough way.

- There was agreement that developing hybrid Civ-Mil standards was a good idea, but that the area and type of standards (e.g. performance standards, interoperability standards) needed to be carefully chosen.

Third party Limited Liability.

- The issue of third party limited liability was the area in which the least empirical knowledge exists in the EU. Some participants argued that this is an area of great concern for the European security companies. This could however not be entirely verified, as no in depth study or analysis on this matter has been performed in the EU.

- There was agreement that liability issues were relevant both for products, as well as for services.

Summary of World Standards Day Round Table: "Standards as a tool for Security Industrial Policy"

The conference took place on 14 October 2011 at the Charlemagne building.

Main messages of the conference:

- The importance of an EU security industrial policy to overcome the very fragmented national and even regional markets in this field was underlined. Participants highlighted the importance of standards for SMEs producing goods and services in the field of emergency management.

- An overview on the content of the newly launched standardisation mandate M/487 was given. CEN, CENELEC and ETSI will address a broad field ranging form counter-terrorism to video surveillance and protection of critical infrastructures via a circumspect stakeholder inclusion encompassing end-users industry and researchers from Europe and beyond. The main goal will be to analyse these sectors through a set of clear criteria to identify suitable areas for standards in security.

- Industry representatives stated that the main goal for Europe in the field of security must be a harmonized market. Today fragmentation and lack of regulation would prevent industry from fully participating thus leaving Europe lacking behind the US and Asia in a steadily growing global market. Standards should already be part of security research projects as industry and researchers will need money to create standards.

- It was also underlined that security is not all about standards and technology but the foremost priority must be citizens "feeling more secure" in Europe. Security standards should include training standards as well as technological ones.

- The lack of certification in the EU was also named as one of the major hurdles in the European security industry environment. Also the creation of an equivalent to the IEEE where technicians and standard setters are sitting on the same table could be envisaged.

Annex 2: Results of the Public Consultation on an Industrial Policy for the Security Industry

1. Introduction

On the 14th of March the European Commission launched a Public Consultation in preparation of the upcoming Communication Industrial Policy for the Security Industry (planned for early 2012).

2. Consultation document

The objective of this consultation was to collect the stakeholders' views on the envisaged policy measures aimed at an enhancing the security of the European citizens through a dedicated EU security industry policy.

Stakeholders were invited to express their opinions on the main problems the EU security industry faces today, namely:

- The fragmentation of the EU security markets,
- The lack of EU wide standards.
- The fragility of the EU industrial base, and
- The integration of societal aspects in the development of security technologies.

Participants were given the possibility to add comments or suggest additional options to those suggested by the Commission on the majority of the questions. Respondents had furthermore the possibility to upload documents/position papers on a number of questions in the consultation. This opportunity was seized by a large number of participants; around 100 documents were uploaded by the respondents.

A number of stakeholders did not fill out the online questionnaire, but sent in position papers on possible policy measures for an Industrial Policy for the Security Industry. These position papers do not appear in the statistics, the content of these papers has nevertheless been taken into account in the overall analysis.

General remark on the analysis of the consultation: The text passages in *italic* are quotes taken from the contributions to the consultation.

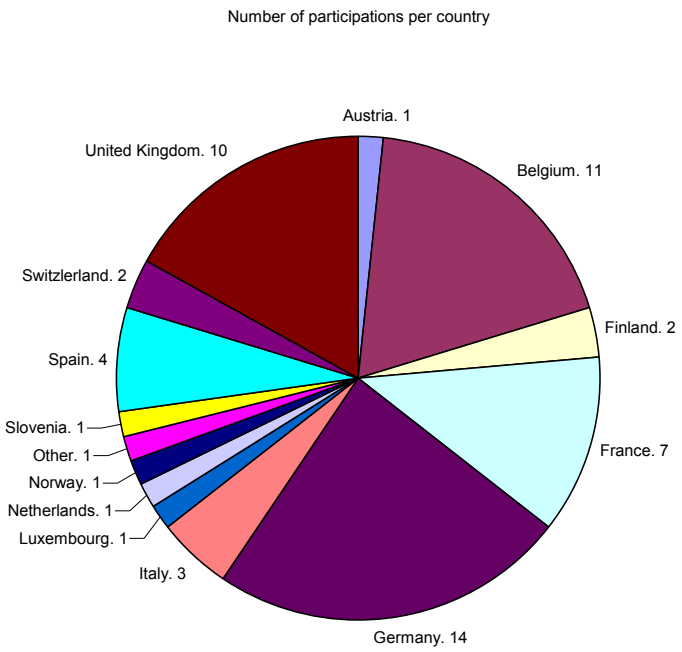
Respondents were able to rank their responses on a scale of 1 (do not agree at all/no effect) to 4 (agree very much/ very strong effect)

Two participants submitted a position paper, in which they explained that, according to their interpretation, security services should be a part of the questionnaire. Their submission to the questionnaire has therefore a different scope, which includes services.

3. Responses to the consultation

The European Commission received in total 59 responses to the public consultation. Contributions were received from stakeholders in 13 countries (one additional participant did not specify his country of origin), including 2 EFTA countries.

Table1: The respondent's countries of origin



Background of the respondents

The respondents can be classified into ten main categories: micro or small enterprises, medium enterprises, large enterprises, business associations, national administrations, Regional or local administrations, academic institution or think tank, non governmental organisation, individuals and others. The high participation of SME's (19%) should be noted.

Background of the respondents		
Stakeholder category	**Number of replies**	**Percentage**
Micro or small enterprise (fewer than 49 employees, turnover less than €10 million)	6	10.20%
Medium enterprise (between 50 and 249 employees, turnover less than €50 million)	5	8.50%
Large enterprise (more than 250 employees)	19	32.20%
A business association	13	22%
A national administration	4	6.80%
Regional or local administration	1	1.70%
An academic institution or think tank	3	5.10%
Non governmental organisation	4	6.80%
An individual	1	1.70%
Other	3	5.10%

4. Responses on the chapters

Subsidiarity principle

The initiative of the Commission to launch specific policy measures on a dedicated Security Industry Policy was met with a very large approval. A number of participating Member States explicitly welcomed and encouraged the proposals of the Commission, stating that the security industry should finally be recognised as a specific industrial sector with a need for dedicated policy mechanisms.

Market fragmentation:

The need for the EU to act on the issue of market fragmentation has been unambiguously agreed upon by ~ 86% of the participants. Only two out of 59 negated the need for an EU action.

2.6. Subsidiarity principle Do you consider that action by the EU would be necessary to reduce the market fragmentation?		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
Yes	39	66.10%
Yes, partly	12	20.34%
No	2	3.39%

Industrial base

On the question: "Do you consider that action by the EU would be necessary to reinforce the industrial base?" 86% of the participants either answered with "yes" or "yes partly". Not a single respondent answered with no.

3.9. Subsidiarity principle Do you consider that action by the EU would be necessary to reinforce the industrial base?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
Yes	38	64.41%
Yes, partly	13	22.03%
No	0	0.00%

4.1. Market Fragmentation

4.1.1 Certification/conformity assessment procedures

The vast majority of the consulted participants agreed with the problem definition of the Commission that "the lack of harmonised certification/conformity assessment procedures for security technologies affects the market fragmentation". Out of 59 replies 33 stated to agree very much and 15 stated to agree with the problem definition, only three did not agree. One national representative explicitly stated that a true internal market for security is still a vague and distant concept.

The majority of the participants emphasized the absolute urgency to act on the fragmentation of the EU security markets, underlining that this is the most pressing policy related concern.

This large approval was also clearly reflected in the rankings of the suggested options. The first option "no change", in which the certification would remain at a national level, was rejected by all participants. The most favoured option of the three possible choices was

option three the "Step by step approach". The Step by Step approach was considered by most to be the most realistic path to a harmonised certification system in the EU. One of the determining factors for this assessment seemed to be the new and diverse character of the security sector.

A certain number of participants also expressed their support for a more direct harmonisation of EU certification procedures, conceding however that the implementation of a drastic change would probably not be feasible: *"Option 2 would be the most desirable one but is unrealistic and might take too long to implement."*

Option 1: No change - certification/conformity assessment procedures will continue to be regulated by national systems.		
	Number of requested records	% Requested records(59)
Do not know	12	20.34%
1	46	77.97%
2	1	1.69%
3	0	0.00%
4	0	0.00%
Option 2: EU wide harmonised certification/conformity assessment procedures covering all (or at least as many as technically possible) security products		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	2	3.39%
2	15	25.42%
3	26	44.07%
4	8	13.56%
Option 3: Step by step: certification/conformity assessment procedures focused on certain priority areas or priority technologies where there is a clear EU added value.		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	5	8.47%
3	10	16.95%
4	32	54.24%

Central stakeholder positions on harmonised EU certification procedures

Independently of their background (SME, large industry, public authority etc.), the stakeholders underlined the clear added value of a European-wide certification regime. The main expected benefits being:

- Reduction of the duplication of certification procedures
- Reduction of the administrative burden for the supply and demand side
- Enhancement of the competitiveness and growth of the EU security industry and
- Support to the creation of an end to end European Security approach from research to commercialisation.

The question of an extension of a possible certification assessment procedure not only to products but also to systems was also received with a large support, 39 respondents qualified it as very useful, 10 as somehow useful and only 2 as not useful.

4.1.2. Standardisation

A vast majority of the participants agreed that the lack of standards affects the fragmentation of the EU security markets. Out of 59 participants 40 agreed very much, 7 agreed and only 7 disagreed on the problem definition (question 2.2.1).

The favoured option of the respondents was, similarly to question 2.1.2., option 3 the "Step by Step approach" (Step-by-step end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to ESO's) with an approval of 75% (30 very agree much 15 agree) followed by option 2 (Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry) with an approval of 30% and option 1 (No change: continue the ad-hoc, piece meal approach whereby the Commission mandates the ESO's to develop EU-wide standards based on immediate needs. In parallel industry develops on its own initiative EU-wide standards.) with an approval of 22%.

The majority of the participants agreed that the establishment of EU wide security standards can only be driven by end user requirements.

"An end-user driven process (Option 3) is crucial for the success of standards, and a step-by-step approach seems reasonable and realistic."

Option 1: No change: continue the ad-hoc, piece meal approach whereby the Commission mandates the ESO's to develop EU-wide standards based on immediate needs. In parallel industry develops on its own initiative EU-wide standards.		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	21	35.59%
2	17	28.81%
3	12	20.34%
4	1	1.69%
Option 2: Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	22	37.29%
2	12	20.34%
3	17	28.81%
4	1	1.69%
Option 3: Step-by-step end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to ESO's		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	1	1.69%
2	6	10.17%
3	15	25.42%
4	30	50.85%

A number of business associations also expressed their interest for a fourth possible option, in which standards would be developed within the framework of a Public-Private Dialogue and Cooperation.

Possible areas of interest for EU wide security standards

- Border management systems
- Cyber security
- Crisis management and civil protection
- Sensor and system limitations
- Identity management and biometry
- Critical infrastructure protection
- Aviation security (airport scanners)
- CBRNE
- IT security
- PKI (Public Key Infrastructures) standards or cryptographic mechanisms and secure protocols

4.2. Fragile industrial base

The responses to the problem definition on this specific point were relatively evenly spread over the possible answers. Categorising the EU security industrial base as generally fragile would not reflect the reality of the markets. Most participants stated that the EU security industrial base cannot be labelled as fragile, given that European security companies are among the market leaders in many high tech areas.

Do you agree that the EU security industrial base is fragile?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	3	5.08%
2	17	28.81%
3	17	28.81%
4	14	23.73%

The EU industrial base was however categorised as fragile in a number of specific areas by a majority of the participants, namely in terms of third country competition (64% approval) and to a lesser degree in terms of access to finance (61% approval). The main aspect on which the participants call for EU action is the strengthening of the competitiveness of the

EU industry on a global scale. A common statement on this issue was submitted by a series of different participants (mainly business associations).

"The industrial base across the EU is however fragile in the sense that it is currently losing out to industries in countries such as the United States in a fiercely competitive global security market; in significant part owing to the support industries outside receive from their host Governments. The industrial policy framework for helping companies in the EU to compete in the security market is currently insufficient. Subsidies and related initiatives such as the US Safety Act mean that the security industry across the EU is losing its competitive edge in the global market."

One of the participating business associations also pointed out two additional factors which, according to them, also contribute to the fragility of the EU industrial base, namely:

- "Fragile in that security solution and service providers operate in a restricted and highly specialized market"
- "Fragile in terms of large integrators' dependency on the sustainability and strength of European SMEs for innovative solutions and equipments […] Unfortunately Europe's SME base is increasingly vulnerable as administrative burdens and costs to comply with an increasing amount of legal regulations is becoming more and more enterprise-threatening. The Commission is therefore urged to engage in positive action to support the SME base, e.g. by easing their access to funding and by simplifying bureaucratic procedures."

3.1.2. Could you please elaborate on what this fragility of the industrial base consists of in your view:		
Fragile in terms of third country competition		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	2	3.39%
2	11	18.64%
3	13	22.03%
4	25	42.37%
Fragile in terms of development of state of the art technologies		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	9	15.25%
2	13	22.03%
3	12	20.34%
4	18	30.51%
Fragile in terms of access to finance		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	11	18.64%
3	12	20.34%
4	24	40.68%

Fragile in terms of dependency from the primes		
	Number of requested records	% Requested records(59)
Do not know	18	30.51%
1	5	8.47%
2	17	28.81%
3	12	20.34%
4	7	11.86%

4.2.1. Pre Commercial Procurement

The issue of Pre Commercial Procurement addressed in question 3.2. of the questionnaire generated an unequivocal response from the respondents.

- Option 1: No change Pre-commercial Procurement in the area of security would be solely done on a national level. Approval rate = 11%
- Option 2: Pre-commercial procurement activities would be carried out in FP8 but without specific financing instruments. Approval rate = 20%
- Option 3: A focused pre-commercial procurement scheme being built up via the possible future FP8 and/or CIPII funding. Approval rate = 76%

A number of participants underlined the crucial role Pre Commercial Procurement in the security sector could play in the future attempts to harmonise the EU security markets. Pre Commercial Procurement schemes could, in combination with certification and standardisation measures, bring together all relevant actors and ensure a better integration of the end users and their specific requirements.

"It is especially important for sectors such as security where the primary customers are public bodies and where applications of innovative technologies are highly regulated."

"[...] it would be a valuable "route to product" for end-users and security companies across the EU."

4.2.2. Defence and Security Procurement

The ratings of the respondents on the two options concerning the Defence Procurement Directive did not suscitate any distinctive majority, which could allow a clear assessment. One quarter of the participants choose the "do not know" answer, none of the options assembled a clear approval rate.

According to the statements made be the participants, this is largely due to the fact that the Defence Procurement Directive has only been in place for a relatively short amount of time. A judgement of its efficiency would therefore be premature.

Option 1: No change – The Defence Procurement Directive will now provide a clear and sufficient framework to contribute effectively to reducing market fragmentation.		
	Number of requested records	% Requested records(59)
Do not know	15	25.42%
1	15	25.42%
2	23	38.98%
3	4	6.78%
4	2	3.39%
Option 2: Encourage security customers to pool their investment resources in order to achieve interoperability and economies of scale.		
	Number of requested records	% Requested records(59)
Do not know	14	23.73%
1	9	15.25%
2	5	8.47%
3	16	27.12%
4	15	25.42%

4.2.3. Synergies between civil and defence technologies

Out of the three options proposed to the participants on synergies between civil and defence technologies, the second option "step by step approach" was clearly the one which received the most positive answers (53%). Option 3 (a dedicated civil-military research programme as part of FP8) had an approval rate of 30% and option 1 (No change) an approval rate of 15%.

The majority of the participants expressed their interest in an enhanced cooperation between the Commission and EDA on possible Civ-Mil synergies. The establishment of a dedicated defence theme was judged to be unrealistic and a possible threat to national defence research budgets. Most respondents agreed that an extended European Framework Cooperation would be the adequate platform for such an enhanced cooperation. It should be noted that most key actors from large industry groups, business associations to Member States supported this option.

"In general, we believe that the establishment of a dedicated civil-military research programme is not necessary, as dual-use research already exists in the present research

schemes. In addition, such a dedicated programme could incite national MoDs to cut their investments, which would have a globally counter-productive effect. […] has welcomed and supported the European Framework Cooperation (EFC) that has been created to systematically synchronize the R&T investment […]."

Two participants also expressed their concern regarding a possible "militarisation" of civilian research. They stressed that security research should only focus on the civilian dimension and that defence research should be explicitly excluded from EU security research.

Option 1: No change - the Commission would continue to coordinate research activities between FP7 and EDA on an ad-hoc basis		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	31	52.54%
2	9	15.25%
3	7	11.86%
4	2	3.39%
Option 2: Strengthening synergies between civilian and defence technologies in a step by step approach via more upstream coordination at the level of capability development and more downstream coordination at the level of development of standards		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	10	16.95%
2	9	15.25%
3	22	37.29%
4	9	15.25%
Option 3: In addition to option 2, this option would go beyond coordinated research activities by establishing a dedicated civil-military research programme as part of FP8		
	Number of requested records	% Requested records(59)
Do not know	13	22.03%
1	18	30.51%
2	10	16.95%
3	3	5.08%
4	15	25.42%

4.2.4. International markets

The results on the questions related to the possible options on international markets were unambiguous. The "no change" option was rejected by all but three participants. The two options which would incite action to open up the international markets for security products were both met with an approval of 77%. The third option was slightly favoured, with three more rankings "very strong effect" than the second option.

These results reflect also the importance accorded by the participants to the issue of third country competition in the context of question 3.1.2. "Fragile industrial base".

Option 1: No change - the EU would not undertake any specific activities to encourage access to third markets for the EU security industry		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
1	46	77.97%
2	2	3.39%
3	2	3.39%
4	1	1.69%
Option 2: Opening up of international markets for security products by making full use of the EU's trade policy strategy.		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	1	1.69%
2	6	10.17%
3	21	35.59%
4	24	40.68%
Option 3:In addition to option 2 - the Commission would aim at fostering the adoption of joint or common approaches at international level, notably in the area of standards via the International Standardisation Organisation. The approach would also provide an opportunity to raise the visibility of the European security industry around the world.		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%

1	2	3.39%
2	4	6.78%
3	18	30.51%
4	27	45.76%

4.2.5. Third party limited liability protection

The question of "Third party limited liability protection" was the issue with the highest amount position papers uploaded by the participants. The most active participants on this issue were the representatives from the various business associations and the large industry groups. They submitted exhaustive and detailed proposals on the creation of an EU Third party limited liability protection system for security technologies.

The importance attributed by the responders to the issue of liability was translated distinctively in the rankings. Option 1, under which the EU would not get active, was rejected by 80% and approved by only 3% of the participants. Option three, which would leave the introduction of liability related legislation to the Member States, was also met only with an approval around 25%. The only option, which was rated as having a strong effect, was option number 2 with an approval of 73%, according to which the EU would introduce harmonised rules at EU level on Third Party Liability Limitations.

It should however be noted that 50% of the participating representatives from national administrations judged the second option to be inadequate. A civil rights group also expressed their doubts on liability, stating that the manufacturers of security technologies should not be freed from all responsibility.

Option 1: No change - under this option the EU would not get involved in Third Party Liability issues		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	44	74.58%
2	3	5.08%
3	1	1.69%
4	1	1.69%
Option 2: Introducing harmonised rules at EU level on Third Party Liability Limitations for security products/processes/systems in case of a terrorist incident. Under this option the EU would define under which circumstances and conditions companies/system operators could invoke Third Party Liability Limitation. The EU would also define the minimum or maximum financial compensation up to which companies/system operators would be liable for		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	3	5.08%
2	4	6.78%
3	8	13.56%
4	35	59.32%
Option 3: Encouraging Member States to introduce such legislation at national level with the Commission as guardian of the Treaty ensuring that such a decentralised approach does not lead to internal market barriers. Under this option, the Commission would set out guidelines to help Member States in setting up Third Party Liability Limitation schemes that would not be contradictory between different Member States, thus leading to internal market barriers		
	Number of requested records	% Requested records(59)
Do not know	9	15.25%
1	9	15.25%
2	26	44.07%
3	10	16.95%
4	5	8.47%

4.3. Security of the citizen and the society

The problem definition, which stated that security products need to be privacy compliant from the development to the production (also know as "privacy by design"), was met with a large approval. Out of 59 responses 42 (71%) agreed with the problem definition and only 18% disagreed.

Do you agree with the problem definition, that security products need to be privacy compliant from the development to the production? (ranking from 1 do not agree at all to 4 agree very much)		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	6	10.17%
2	5	8.47%
3	15	25.42%
4	27	45.76%

4.3.1. How to ensure the integration of ethical/societal aspects in security technologies

The answers on the appropriate inclusion of societal aspects in security were spread to some extend over the various options. The only option which was clearly rejected was the first option, under which privacy by design would remain a voluntary effort for industry. This option was only approved by 17% of the participants and disapproved by 73%.

The differences between the other two options were relatively marginal, a slight preference for option 2 (voluntary system) was nevertheless expressed. Most representatives from large industry groups pleaded for a selected mandatory certification, which would only concern specific security technologies.

"We believe that a mandatory certification assessment (option 3) would only be reasonable in some areas, but not in all. Hence, a case-by-case decision, respecting the distinctiveness of the concerned products/processes, would be far more valuable. "

Three participants furthermore stated that the scope of the question was too restricted to privacy issues and that a broader approach would be more appropriate to ensure a successful inclusion of ethical aspects.

"Ethical/societal implications of security research are not limited to privacy issues. There are for example issues such as dual use goods, the militarisation of security, the ethics of end users (not exclusively in third countries) and reference to human rights and democratic governance in security policy. Beyond that, there is an issue about the privatisation of security with the easier access to cheaper but intrusive technology. Ethics must be an intrinsic part of programme and project design."

Option 1: No change - privacy by design would remain a voluntary effort for industry with no EU wide guidelines and/or requirements		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	35	59.32%
2	8	13.56%
3	1	1.69%
4	9	15.25%
Option 2: A voluntary certification/conformity assessment system. Under this option the economic operator wishing to have his product/process/system certified for being "privacy by design" fit, would have to fulfil a set of requirements defined by the EU. However, the certification/conformity assessment itself would remain voluntary.		
	Number of requested records	% Requested records(59)
Do not know	4	6.78%
1	11	18.64%
2	15	25.42%
3	11	18.64%
4	18	30.51%
Option 3: In addition to option 2 – the certification certification/conformity assessment would be mandatory		
	Number of requested records	% Requested records(59)
Do not know	10	16.95%
1	18	30.51%
2	12	20.34%
3	5	8.47%
4	14	23.73%

4.3.2. Certification procedures

A majority (66%) of the respondents agreed on the usefulness of a merger between a possible ethical certification procedure and a general certification procedure, instead of having two separate certification procedures.

4.2 Certification procedures Do you believe it to be useful to merge a possible ethical certification procedure as detailed in point 4.1. with the certification procedures outlined in point 2.1, instead of having two separate certification procedures?		
	Number of requested records	% Requested records(59)
Do not know	8	13.56%
Very useful	16	27.12%
Somehow useful	23	38.98%
Not useful	12	20.34%

4.3.3. Privacy compliant technologies

The respondents were finally given the opportunity to express their preference on the possible inclusion of the "privacy by design" concept in FP security research as mandatory evaluation criteria.

This mandatory inclusion was rejected by a slight majority (52%) of the participants. The preferred option of 58% was the inclusion of the "privacy by design" concept through targeted research projects in the Security Theme of the FP was supported by 58%.

Option 1: No change - Through targeted research projects in the Security Theme of the FP aimed at developing "privacy by design" technologies. These technologies could then be applied in future security products, processes or systems.		
	Number of requested records	% Requested records(59)
Do not know	7	11.86%
1	14	23.73%
2	4	6.78%
3	9	15.25%
4	25	42.37%
Option 2: Making the privacy compliance a mandatory evaluation criteria for all technology		

related research proposals under the Security Theme of the FP. Under this option, the EU would make it mandatory to address privacy by design in all technology related research proposals of the Security Theme of the FP.		
	Number of requested records	% Requested records(59)
Do not know	6	10.17%
1	13	22.03%
2	20	33.90%
3	8	13.56%
4	12	20.34%

Annex 3: Sectors of the Security Industry

This list is not exhaustive, the aim is merely to give an overview of the technologies which characterise the different segments.

Aviation Security

- Airport terminal security systems.
- Airport perimeter security systems.
- Passenger screening systems.
- Hand-held and checked-luggage screening systems.
- Application of RFID systems.
- Airport security command, control & communication IT and hardware infrastructure.
- Reinforced blast-proof aircraft containers.
- Explosives detection systems.
- Security-related renovations and construction projects.

Maritime Security

- Smart container systems.
- RFID container seal systems.
- Container explosives screening systems.
- Seaport perimeter protection systems.
- Nuclear/Radiological container screening systems.
- Cruise ship & ferry passenger screening systems, including hand-held and checked luggage screening systems.
- Deepwater security systems.
- Ship identification systems.

Border Security

- Border-perimeter interoperable communication systems.
- Virtual border systems.
- Checkpoint, fence and barrier hardware.
- Border-perimeter people screening systems.
- Border-perimeter people and workforce biometric identification systems.
- Explosives screening portals.
- Border-perimeter construction projects.
- Border-perimeter nuclear/radiological screening portals.

Critical Infrastructure Security

- Governmental critical infrastructure terror mitigation security systems.
- Medical and public health infrastructure terror mitigation security systems.
- Nuclear facilities terror mitigation security systems.
- Critical infrastructure workforce and visitors identification and surveillance systems.
- Communication infrastructure terror mitigation security systems.
- The government and private sector I.T. critical infrastructure security systems.
- Critical Infrastructure perimeter protection systems.
- Dams terror mitigation security systems.
- Large high volume structures terror mitigation security systems.
- Transportation industry terror mitigation security systems.
- Banking and financial industry business continuity.

 Energy infrastructure security systems.
 Workforce and visitor identification systems.

Counter-Terror Intelligence Market

 Command, control and communication systems.
 Cyber space monitoring systems.
 Cyber terror remediation systems.
 Perimeter security systems.
 Data fusion IT systems.
 Land-based imagery systems.
 Communication interoperability systems.
 Information analysis software
 Cyber security IT systems.
 Cyber surveillance IT systems.

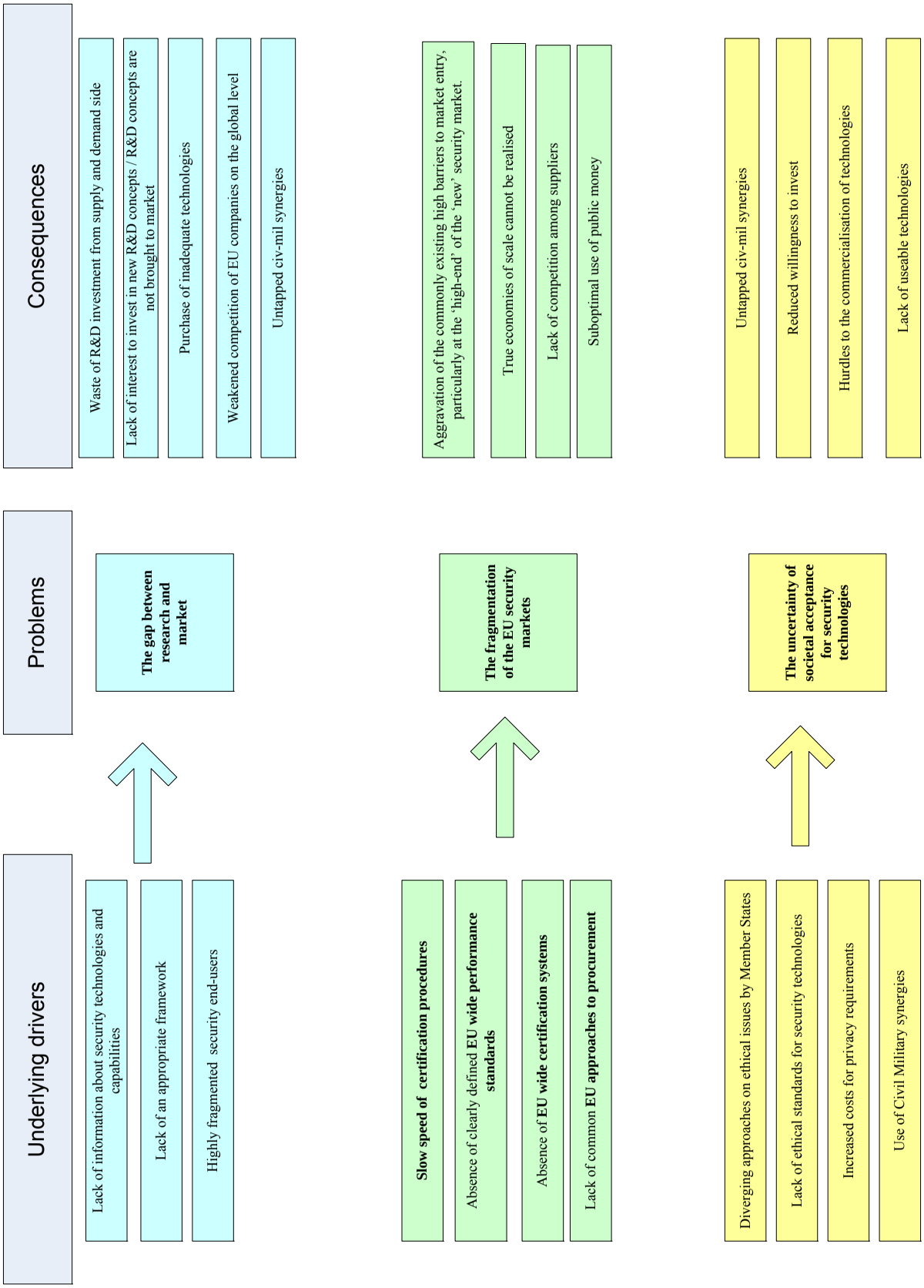
Physical Security Protection

 CCTV systems
 Fire alarm systems
 Intruder alarm systems
 Burglar alarm systems
 Communication systems.

Protective Clothing

 CBRN personal protection gear.
 CBRN air filtering systems
 Protective clothing for police forces
 Protective clothing for fire fighters
 Search and rescue equipment.

Annex 4: Structure of the Problem Definition



Annex 5: Overview of the most important challenges to the internal security of citizens among the EU 27.

SPECIAL EUROBAROMETER 371 "Internal security"

QC1 What do you think are the most important challenges to the security of (NATIONALITY) citizens at the moment?

	Economic and financial crises	Terrorism	Poverty	Organised Crime	Corruption	Illegal immigration	Petty crime	Natural disasters	Environmental issues / Climate change	Cybercrime	Nuclear disasters	Insecurity of EU borders	Religious extremism	Civil wars and wars	Other (SPONTANEOUS)	Dont know
EU27	33%	25%	24%	22%	18%	13%	13%	11%	11%	10%	8%	6%	6%	4%	9%	8%
BE	32%	20%	27%	15%	8%	23%	31%	11%	16%	10%	9%	7%	11%	3%	12%	2%
BG	48%	4%	60%	23%	24%	1%	26%	10%	4%	0%	2%	1%	2%	1%	19%	2%
CZ	38%	14%	16%	39%	38%	10%	8%	22%	12%	16%	8%	6%	4%	5%	3%	4%
DK	30%	55%	5%	19%	2%	9%	6%	5%	19%	4%	4%	5%	11%	5%	21%	4%
DE	28%	34%	19%	32%	14%	8%	9%	12%	20%	27%	10%	7%	10%	5%	6%	4%
EE	22%	9%	17%	9%	11%	3%	12%	5%	6%	9%	3%	12%	1%	4%	19%	14%
IE	61%	10%	30%	45%	25%	8%	17%	5%	9%	6%	4%	2%	1%	2%	5%	3%
EL	56%	7%	50%	13%	39%	28%	15%	6%	7%	2%	4%	10%	1%	3%	4%	0%
ES	57%	38%	35%	11%	37%	16%	7%	10%	7%	4%	5%	3%	4%	4%	2%	2%
FR	15%	16%	20%	7%	7%	10%	31%	7%	8%	4%	7%	3%	7%	3%	26%	19%
IT	44%	26%	18%	31%	19%	24%	7%	13%	13%	8%	10%	8%	5%	9%	2%	2%
CY	54%	6%	15%	26%	21%	55%	15%	5%	7%	7%	1%	8%	1%	1%	26%	
LV	27%	2%	41%	13%	28%	2%	23%	3%	4%	2%	1%	2%	0%	2%	5%	16%
LT	41%	5%	41%	25%	42%	4%	17%	9%	6%	7%	6%	2%	0%	2%	8%	6%
LU	16%	4%	10%	13%	5%	11%	37%	6%	9%	4%	7%	6%	1%	1%	21%	11%
HU	52%	5%	51%	20%	27%	4%	9%	20%	16%	3%	4%	3%	1%	1%	8%	2%
MT	27%	6%	15%	20%	27%	38%	12%	5%	12%	9%	1%	5%	3%	5%	9%	10%
NL	22%	26%	14%	23%	7%	7%	31%	8%	20%	22%	6%	6%	15%	3%	26%	4%
AT	40%	11%	20%	30%	9%	23%	15%	20%	21%	16%	14%	19%	6%	3%	3%	4%
PL	22%	9%	21%	13%	11%	1%	7%	16%	4%	3%	2%	1%	1%	4%	6%	27%
PT	41%	9%	42%	24%	30%	6%	11%	7%	6%	3%	4%	7%	2%	4%	2%	7%
RO	41%	14%	56%	14%	56%	2%	4%	19%	9%	4%	6%	3%	1%	5%	2%	4%
SI	46%	3%	30%	31%	47%	2%	6%	17%	15%	4%	3%	1%	2%	1%	9%	3%
SK	40%	11%	38%	24%	31%	3%	20%	46%	14%	5%	9%	3%	1%	3%	2%	1%
FI	27%	16%	11%	22%	2%	12%	10%	11%	14%	8%	15%	9%	2%	4%	27%	8%
SE	17%	30%	4%	23%	3%	3%	5%	7%	21%	6%	9%	1%	6%	3%	27%	9%
UK	24%	47%	14%	25%	6%	23%	9%	3%	7%	11%	2%	8%	10%	3%	6%	9%

Highest percentage per country
Lowest percentage per country
Highest percentage per item
Lowest percentage per item

Legend : Open/Unprompted question

Annex 6: Definition of Pre-Commercial Procurement

The EU definition as stated in the 2007 Communication on PCP:[100]

"For the purpose of this communication "pre-commercial procurement" is intended to describe an approach to procuring R&D services other than those where "the benefits accrue exclusively to the contracting authority for its use in the conduct of its own affairs, on condition that the service provided is wholly remunerated by the contracting authority" and that does not constitute State aid.

More specifically in pre-commercial procurement:

(1) The scope is R&D services only: R&D can cover activities such as solution exploration and design, prototyping, up to the original development of a limited volume of first products or services in the form of a test series. "Original development of a first product or service may include limited production or supply in order to incorporate the results of field testing and to demonstrate that the product or service is suitable for production or supply in quantity to acceptable quality standards". R&D does not include commercial development activities such as quantity production, supply to establish commercial viability or to recover R&D costs, integration, customisation, incremental adaptations and improvements to existing products or processes.

(2) The application of risk-benefit sharing: In pre-commercial procurement, the public purchaser does not reserve the R&D results exclusively for its own use: Public authorities and industry share risks and benefits of the R&D needed to develop new innovative solutions that outperform those available on the market.

(3) A competitive procurement designed to exclude State aid: Organising the risk- benefit sharing and the entire procurement process in a way that ensures maximum competition, transparency, openness, fairness and pricing at market conditions enables the public purchaser to identify the best possible solutions the market can offer."

A more pragmatic definition of PCP is:

PCP (pre-commercial procurement) is a procedure for the public procurement of R&D services. PCP schemes cover phase 1 to phase 3 of the innovation cycle from solution exploration definition to test-series production and field-testing, just before the commercial stage.

PCP is not simply a procurement of R&D services, which would imply that the IPR belongs to the procurer, because in the case of PCP the whole idea is that IPR should remain with the supplier, in order to enable him to develop other markets. But if in R&D service IPR procurement is left to the supplier, then it legally becomes R&D support, and 100% R&D support by public authorities would be considered as an illegal state aid.

The answer to this dilemma is to leave the IPR to the supplier, who in return must concede some advantage to the public procurer, either a price discount on the resulting product, or some modality of IPR sharing or royalty or licensing agreement. This amounts to an overall

[100] COM (2007) 799 on Pre-Commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe

sharing of the risks and benefits of the project between the public authorities and the private suppliers3.

In essence, pre-commercial procurement is a mutual learning process for the procurers, the users and the suppliers. When it comes to tackling a concrete public sector problem, it enables all concerned to get a firm confirmation, about both the functional needs on the demand side and the capabilities and limitations of new technological developments on the supply side.

Primary objectives of PCP are those bridging the gap between R&D and commercialisation, such as:

- Integrate the end-users in the R&D process (creating a link between R&D support programmes and procurement needs, coordinating funders, prescribers, procurers and end-users)
- Initiate demand-driven R&D procurement rather than supply-driven R&D procurement Secondary objectives of PCP are those intending to maximise the efficiency and effectiveness of the programme such as:
- Bring R&D concepts that are promising for the public sector quicker to the market
- Increase SME involvement in innovation
- Develop higher quality and better prices products thanks to competitive development
- Increase the degree of interoperability between participants. The desired degree of interoperability needs to be integrated as a key objective from the start. Indeed, efforts after each R&D phase to achieve interoperability and product inter-changeability between the alternative solutions being developed pave the way for open standards.

Annex 7: Competitiveness Proofing – Two illustrative cases

The EU Security Industry encompasses many different segments. The competitive situation of these segments varies.

This Annex aims at illustrating this variety of situations and likely effects by providing a more detailed analysis of two very different segments. 'Airport scanners' are part of what may be considered the high tech, high value 'new' security industry that has developed particularly in response to terrorism threats. By contrast the medium tech, lower value "alarm systems" represent part of what may be considered the 'traditional' security industry.

7.1. The airport scanners segment[101]

7.1.1. 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 Rapidscan in the EU, and L3, SAIC and AS&E in the US. 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.[102] Alongside the handful of leading players are a few medium and smaller companies that tend to be focussed 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.

7.1.2. Value chain

In terms of technology development and upstream linkages to component suppliers, the situation of providers of security inspection and screening equipment (OEMs - Original Equipment Manufacturers) 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 value added for security screening equipment.[103] A consequence of this situation is for OEMs to move away from vertically integrated

---

101 For additional background information on the airport security screening equipment sector see "Study on the competitiveness of the EU Security Industry" (2009) and the SECERCA study (2011).

102 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 Heinmann Systems in 2002; OSI acquisition of Rapiscan Security Products in 1993.

103 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).

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.[104]

Typical manufacturing activities – which increasingly relates to final assembly – is undertaken 'in-house' and at the main business locations of equipment suppliers (i.e. USA, W. Europe). This reflects the need for close oversight of product assembly and for maintaining proximity between manufacturing activities and technical and systems development activities.[105] Smaller companies (e.g. producers of specialised equipment) may outsource manufacturing/assembly activities but this is generally not the case.[106] 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.[107] Another aspect of production that may eventually become subject to outsourcing and/or off-shoring is software development, which can be extremely labour intensive[108]. 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).

7.1.3. Competitive position of the EU industry[109]

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.

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 player, with whom they must often develop partnerships to have access to broader market segments.

---

104 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.

105 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.

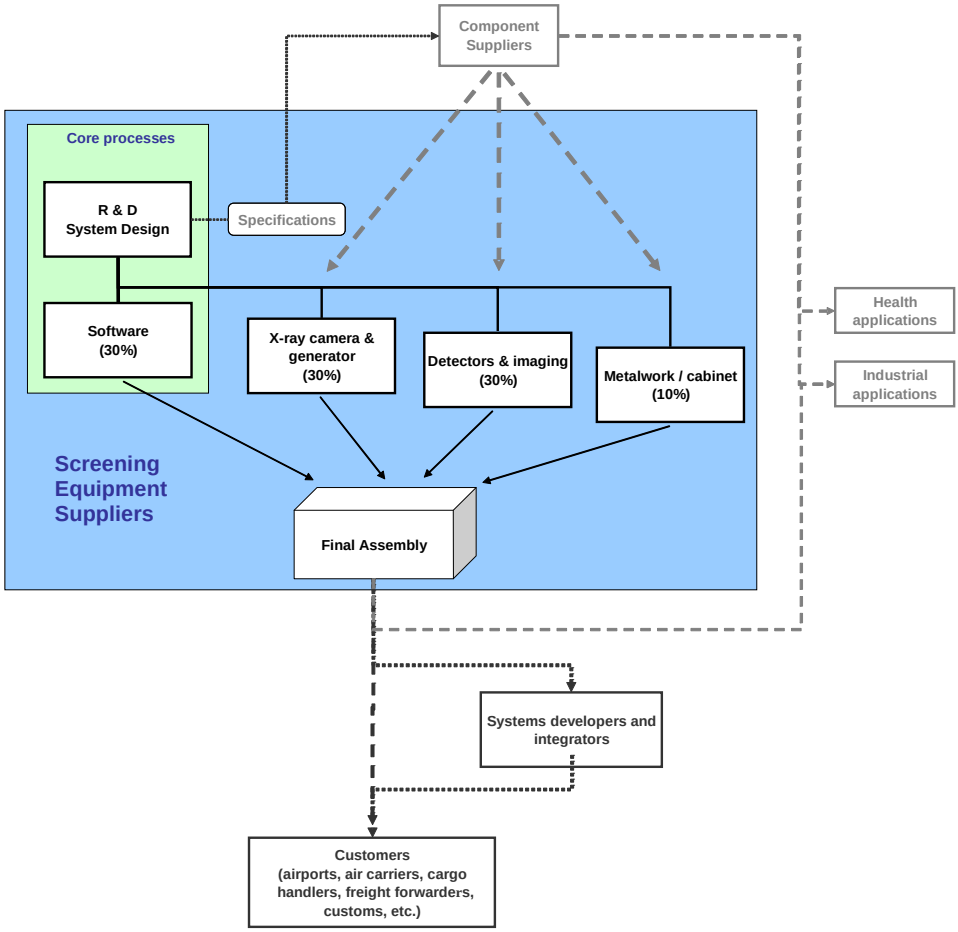
106 An exception is in the manufacturer of the cabinets in which equipment is housed, for which OEMs can look for 'low cost' supply opportunities; for example, Smith's Detection is sourcing cabinets from Eastern Europe.

107 For example, in 2006 Smiths detection opened an x-ray production/assembly site in St Petersburg to serve the growing Russian market

108 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

109 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 if international trade data.

Figure 1 Stylised supply/value chain for aviation security screening equipment[110]



In terms of other international competitors, the only significant company in the aviation security inspection and screening equipment sector is the Chinese company Nuctech[111]. 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

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

111 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.

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.

7.1.4. The EU industry's regulatory handicap

The current situation of security regulations, standards and procurement systems affecting aviation security screening equipment is considered to have a significant negative effect on market efficiency and the competitive situation of EU aviation security screening equipment sector. Lack of harmonisation creates fragmented markets that translate into higher costs and reduced opportunities for achieving economies of scale for equipment suppliers orientated towards European markets. In addition to the implications that this situation has for price competitiveness, there is concern that the fragmented nature of the European market might have the effect of reducing the overall level of R&D, technology development and innovation. Specifically, market fragmentation implies higher barriers of entry for the adoption of new technologies within the market, potentially reducing the return on investment in development. Consequently, there may be a negative effect on the competitive position of European suppliers as a result of insufficient investment in technological developments and innovation.

In general the business environment in the EU, including the negative consequences of market fragmentation, is seen as less supportive for the development of the security inspection and screening equipment sector than in the US.

Illustration: US comparison

The US represents the main competitor to the EU in the aviation security screening sector - and for the security industry in general – and is the largest single market for aviation security equipment and systems. In terms of factors shaping the business environment for suppliers of aviation security screening equipment and systems, two features of the US situation are of particular relevance:

- A single Federal authority – the Transport Security Administration (TSA) – is responsible for setting the approach to aviation security and technology adoption, for determining performance requirements, for evaluating and approving security equipment and, finally, for the procurement and deployment of equipment.
- The SAFETY Act provides for the reduction of liability risks for manufacturers and distributors of anti-terrorism technologies. Further DHS designation and certification[112] under the Act provides *de facto* approval of security equipment and technologies that is recognised in global markets.

Compared to the present EU situation, the US market is characterised by:

- Lower costs of supplying the market, both in terms of the costs associated with compliance (conformity assessment) and approval (certification) of equipment and systems, and more generally for securing markets.

[112] The Act provides for two levels of approval: (i) designation and a qualified anti-terrorism technology and, for more mature technologies, (ii) certification as a DHS approved product.

- Lower uncertainty over the potential market size for new security products and technologies; there is a single US positions on the utilisation of technologies and performance standards/requirements.

- Lower risk attached to investments in research, technology development and innovation activities, both because of more certain market potential and liability situation.

- Shorter 'time to market' for new security technologies and innovations.

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

- ***Disparities in legislation over airports and air carriers across Member States.*** 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 uniform security systems throughout the European market, which has the effect of increasing cost while making economies of scale unfeasible. Thus, companies and other organisations that need to comply with air transport security requirements must adapt to different Member States' legislations if their activities are cross-border and internationally oriented. This implies, 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. While the regulations are aimed at ensuring common minimum standards, it is argued that they have slowed down the introduction of new technologies such as LAG (liquid, aerosol and gel) screening equipment and security scanners (a.k.a. 'advanced imaging technologies' or 'body scanners').

- ***EU airport scanner producers confronted with a multiplicity of security standards and certification systems within the EU.*** 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 down 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 place EU equipment providers at a competitive disadvantage, as it deprives them from a large and integrated home market enjoyed by the US competitors[113].

Illustration: Costs of Conformity assessment and certification of screening equipment

An industry source has indicated, for example, that the cost of a single test of an Explosive Detection System (EDS) could be in the region of €65 thousand and for a liquid explosive system (LAGS) the figure may vary from €30 to €75 thousand; these figures relate to a single test procedure and do not take into account any repeat testing that may be required. The aforementioned products are relatively small systems and costs associated for larger systems are reputed to be significantly higher and may run into several hundred thousand Euros; for example, an amount of €100 thousand has been indicated for an 'imaging test' for a cargo scanner while a figure of €500 thousand has been indicated for the cost of the certification process for a biometric identity card model.

- ***Legal uncertainty about what legislation will consider as ethically or socially acceptable.*** 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

[113] See Annex 4 (Background to the quantitative analysis of certification) for a description of specific estimates of relevant cost items and cost impacts associated to conformity assessment and certification.

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 if security scanners are deployed "*health and fundamental rights must be safeguarded along with personal data, dignity and privacy*" [114] 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.[115]

While 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 EU companies insofar as they rely more on 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 sectors 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.

7.1.5. Competitiveness implications of the envisaged policy initiatives

- ***The impact of harmonized standards, conformity assessment and certification.*** The development of EU-wide harmonised standards and conformity assessment (testing) certification procedures should reinforce existing efforts (e.g. ECAC CEP) towards common approaches for testing conformity with EU performance requirements. A system enabling single EU certification (or mutual recognition of national certification) would remove the need for airport screening systems to undergo multiple national testing and approvals to be accepted in the EU market. This should reduce the associated compliance costs and reduce costs incurred to adapt products to comply with differing national requirements/specifications and national conformity assessment procedures[116]; notably if the latter are implemented on an ad hoc basis for specific technologies and solutions. Moreover, EU conformity assessment procedures and certification would reduce the need for potential customers (and relevant authorities) to undertake their own product trials.

  EU-wide harmonised standards and conformity assessment and certification procedures may facilitate more rapid product development processes and reduce 'time to market'. This possibility will, in part, depend on the extent that relevant regulations and standards serve to indicate performance (and other) characteristics required to meet future

---

114 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

115 Source: http://www.tsa.gov/approach/tech/ait/index.shtm

116 See Section 7.2 (Quantitative Comparison of the Options) and/or Annex 4 (Background to quantitative analysis of certification).

regulatory and market needs. Further, an EU infrastructure for conformity assessment may also support the development process; for example by engaging in development and pre-certification testing. This would move the situation closer to that in the USA where there is greater on-going interaction between the TSA and equipment suppliers throughout the development phase of new aviation security technologies and solutions.

It seems unlikely that an EU-wide approach would significantly affect market access for the major players in the sector that operate at a global level. But, by removing the need to submit to national approval, it may facilitate their ease of access. An EU-wide approach may have a positive effect on the competitiveness position of SMEs. In so far as EU certification serves as a recognised mark of product performance within the EU market, it may facilitate them in supplying systems to the major players in the sector.

To the extent that reduced conformity assessment and certification costs are passed on to consumers, an EU-wide approach would improve the price competitiveness of EU producers. Further, by reducing barriers to market access, an EU-wide approach should increase market openness and enhance customer choice.

Finally, an EU-wide certification scheme demonstrating compliance to all necessary EU requirements may reduce consumer 'uncertainty' over product performance that could occur with different national conformity assessment and approval procedures. It could therefore reduce transaction costs for producers and buyers, turning the EU into a more supportive home market.

- ***The impact of Pre-commercial procurement (PCP).*** The aim of a EU common approach on PCP is to help bridging the gap between research and markets. This is unlikely to have a major impact on this industrial segment as, for the most part, the ultimate purchasers of aviation security equipment and systems are private sector companies.

- ***The impact of third party liability limitation.*** As aviation security screening equipment and systems are employed primarily in an anti-terrorism context the issue of third party liability is of high importance to the sector.

- ***The impact of voluntary scheme for "privacy by design" audits***. The proposed policy actions envisage only a voluntary scheme for "privacy by design" audits. As such, suppliers of aviation screening systems are unlikely to implement such audits unless it is seen to be in their commercial interest to do so. However, if audits become a market requirement, this may impose significant additional costs on industry; in particular if compliance with audit processes necessitates significant reorganisation of development and production processes.

Implications for the international competitiveness of the EU industry. If successful in reducing market fragmentation in the EU, the proposed policy actions should raise overall EU market efficiency in the aviation security screening sector. However, an EU-wide approach to standards, conformity access and certification may also increase the openness of the EU market to non-EU suppliers. In this regard, For EU companies to take advantage of enhanced access to the EU market as a whole may require also responding to increased competition from non-EU suppliers.

Cost reductions resulting from an EU-wide approach would only have a limited impact on the price competitiveness of EU products on international markets in the short term. Nonetheless, there may be dynamic effects if a less fragmented EU market encourages investment in research, technology development and innovation. In particular, to the extent that the proposed actions are associated to a clear EU approach to aviation security (and regulation, thereof) then this should enhance the attractiveness of investments in relevant security technologies.

An EU-wide certification scheme (and corresponding EU security performance 'mark' or 'quality label') may strengthen broader international market awareness and acceptance of EU products.

7.2. The alarms segment[117]

7.2.1. 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.[118] Since the mid-90s the major players led an 'acquisition crusade', buying up medium and small security products manufacturers.[119] This resulted in considerable consolidation and rationalization within the sector. Bosch and Siemens[120] 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 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.

7.2.2. Value chain

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

117 For additional background information on the airport security screening equipment sector the SECERCA study.

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

119 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

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

contrast, significant activities connected to the related software systems are still undertaken globally.[121]

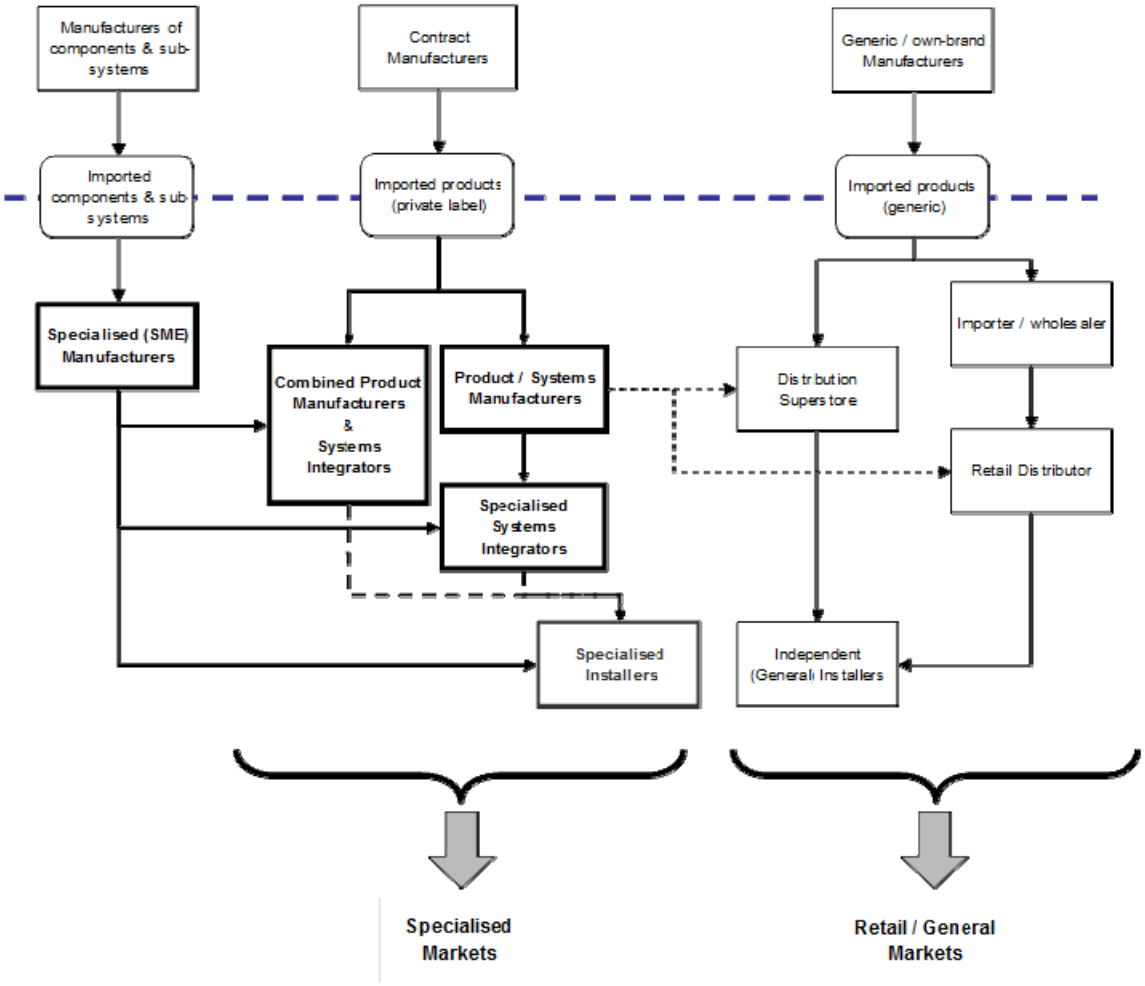
By and large, while the major players may still be manufacturers – albeit that they contract Asian manufacturers to supply of products and sub-systems under 'private labels' – the main focus of their activities is on systems integration. Other companies, which include most of those in the EU, are more focussed on 'services', including research and innovation to develop new high-tech products and product customisation for specialised 'high end' market segments.[122]

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 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.

121 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.

122 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.

Figure 2 Stylised supply/value chain for electronic security equipment (alarm systems etc.)



7.2.3. Competitive position of EU industry

International trade data[123] 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 for 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 (see Table 1 and Figure 3).

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 onwards[124].

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

124 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

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 nearly 35% in 2009; though this share appears to have fallen back in 2010. By contrast the share of the USA has steadily declined over the period (see Figure 4).

Table 1 EU external trade in burglar and fire alarms: total value ($US million)

Year	Total extra-EU exports	Total extra-EU imports	Trade Balance
2002	217.4	355.6	-138.2
2003	256.0	398.0	-142.1
2004	304.0	453.3	-149.3
2005	314.7	497.5	-182.8
2006	378.0	576.5	-198.5
2007	497.3	579.9	-82.6
2008	660.1	608.6	51.5
2009	665.3	554.8	110.5
2010	599.1	602.0	-2.9

Figure 3 EU external trade in burglar and fire alarms: total value ($US million)

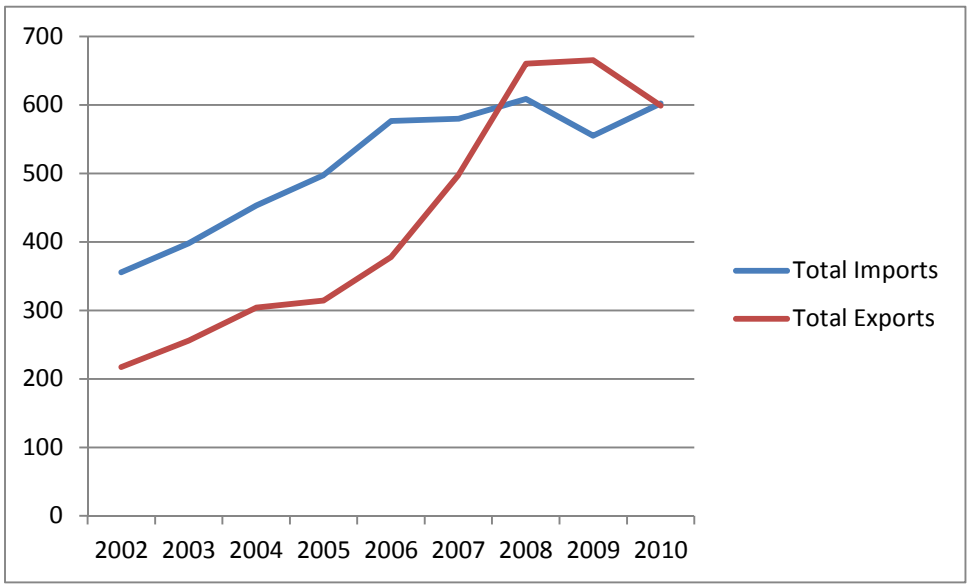
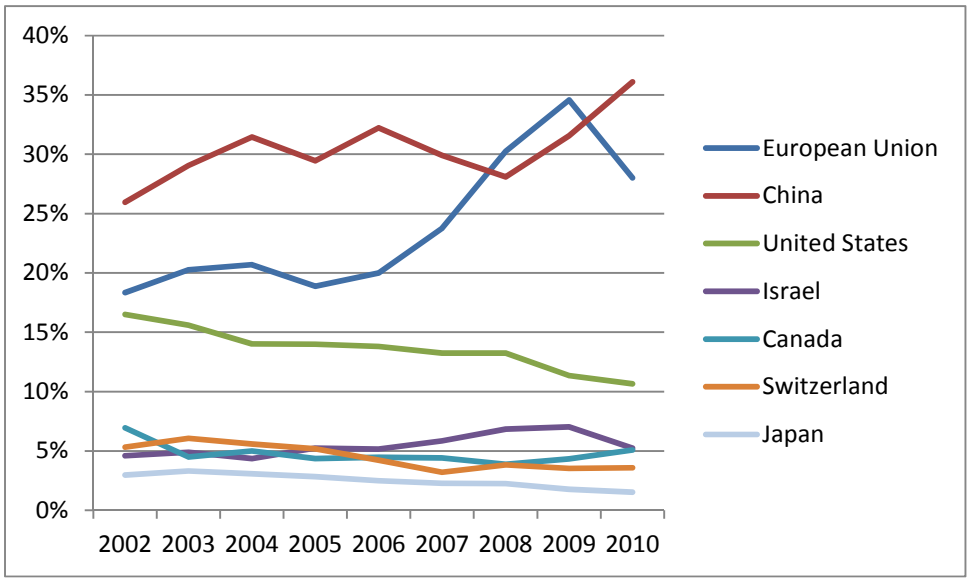


Figure 4 Shares of global trade in burglar and fire alarms: share of world imports by source county (%)



The EU's successful 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 Figure 5).

Revealed Comparative Advantage (RCA)

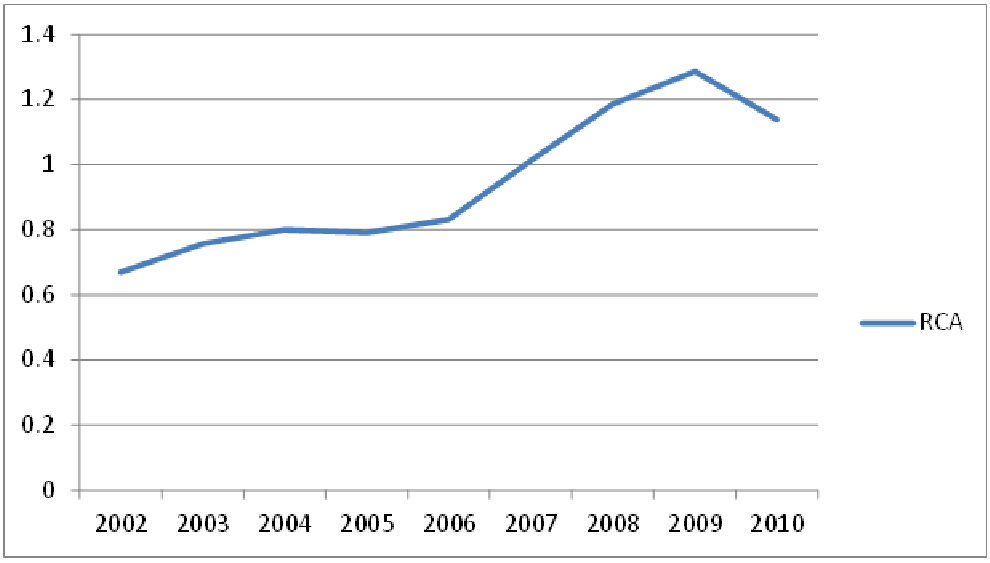
The RCA of a county is defined as follow:

'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:

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

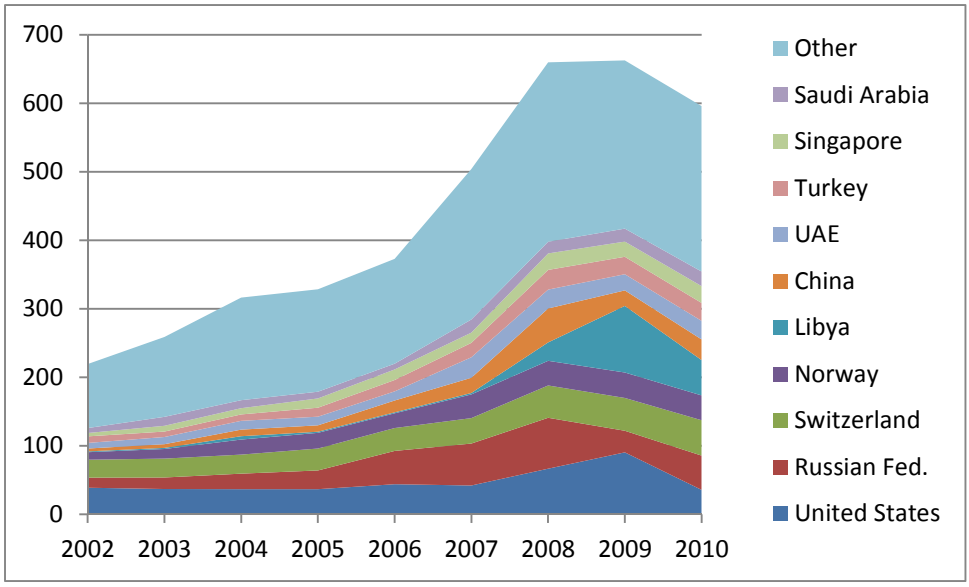
Where x_{ij} and x_{wj} are the values of country i's exports of product j and world exports of product j and where X_{it} and X_{wt} refer to the country's total exports and world total exports. A value of less than unity implies that the country has a revealed comparative disadvantage in the product.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

Figure 5 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 Figure 6). 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 6 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 40% in 2010[125] (see Figure 7 and

125 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 8). A further 7% 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 2010.

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 Table 2).

Table 2 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

Figure 7 Extra-EU imports of burglar and fire alarms by source country ($US million)

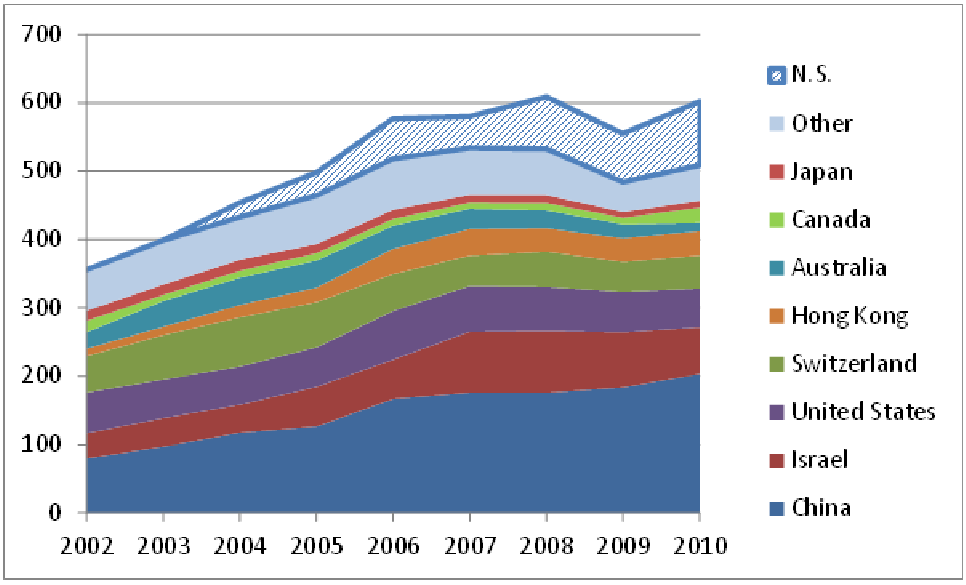
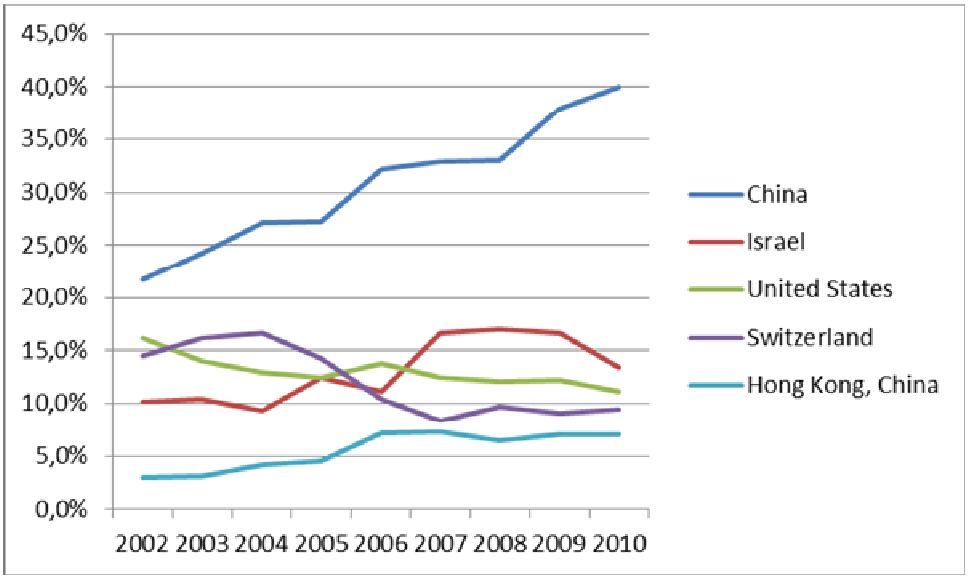


Figure 8 Extra-EU import shares of leading supplier countries of burglar and fire alarms (% of imports)



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 1.1 billion in 2010, remains significantly higher than EU external trade at approximately $US 600 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 in 2009 and 2009, extra-EU exports of fire and burglar alarms grew at an average annual rate of 20% (CAGR)[126] 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

126 Compound annual growth rate

only 2.3 times in 2008). This trend was reinforced in 2009 and 2010, where the ratio of intra-EU exports to extra-EU exports fell to 1.8 (i.e. the value of extra-EU exports rose to more than 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.

7.2.4. The EU industry's regulatory handicap

European Standards (EN) already exist for several product categories of electronic security and fire protection equipment.[127] Moreover, a limited number of security-related equipment (e.g. fire alarm and fire protection equipment) are covered within the scope of the Construction Product Directive/Regulation and, thus, fall with the provisions for mutual recognition of certificates of compliance with EU regulations. Otherwise, for other categories of electronic security products including specifically intruder alarms, the EU market is characterised by national schemes for conformity assessment and certification. For these product categories, there has been very little progress towards common certification schemes and/or mutual recognition of certificates. Consequently, suppliers have to submit their products to national conformity assessment and procedures, which may also require adapting products to country-specific requirements. This situation imposes costs higher costs on industry that would otherwise be the case if a common EU-wide system and/or mutual recognition across countries was in operation.

Illustration: Costs of Conformity assessment and certification of alarm systems

Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. The costs of certification of an alarm system are on average (with a large spread depending on the nature of the product) at the level of EUR 200-300 thousand for full access to Europe including all tests. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to EUR 40-60k.

7.2.5. Competitiveness implications of the envisaged policy initiatives

- ***The impact of harmonized standards, conformity assessment and certification***. For the intruder and fire alarms segment, the development of EU-wide harmonised standards and certification procedures is expected to be the most important element of the proposed policy actions. For suppliers serving multiple national markets in the EU, EU wide standards and certification procedures should reduce costs of demonstrating compliance with market requirements.[128,] Common EU-wide standards should also reduce cost

[127] For example: EN54 series for fire alarm systems and components; EN50131 series standards for intrusion and hold-up alarm system components; EN50132 series standards for CCTV systems and components; EN50133 series standards for access control systems and components.

[128] See Section 7.2 (Quantitative Comparison of the Options) and/or Annex 4 (Background to quantitative analysis of certification). For suppliers serving single national markets costs should be unchanged *ceteris paribus*; although, to the extent

incurred to adapt products to comply with differing national product standards and national conformity assessment procedures. Removing the need for multiple certifications should enable suppliers to more rapidly access different parts of the EU market which, in turn, may have implications for the organisation and scale of production activities. Increasing potential market size for products, reducing time to market and, hence, the risks that new innovations may be replicated by competitors are also factors that increase the potential return to investments in research and technology development. At the same time, in establish EU-wide harmonised standards that these standards do not operate in such a way that they inhibit technology development and innovation.

To the extent that reduced conformity assessment and certification costs are passed on to consumers this should improve EU price competitiveness. Further, by reducing barriers to market access for alarm products, an EU-wide approach should increase market openness and enhance consumer choice. Finally, an EU-wide certification scheme enables a supplier to demonstrate to potential customers that its product meets all necessary EU performance requirements. As such it may reduce consumer 'uncertainty' over product performance that arises as a result of existing differences in national product and conformity assessment standards and specifications.

The development of EU-wide harmonised standards and certification procedures should have a positive effect on the competitiveness position of SMEs. Conformity assessment and certification costs represent a proportionately higher share of total costs for SMEs than for larger producers with higher volumes of production/sales. Thus cost savings from removing multiple certification requirements will be proportionately higher for SMEs. Further, as the existing national systems present a greater market access barrier for SMEs, they should potentially benefit more from improved market access opportunities stemming from an EU-wide approach. Moreover, in so far as EU certification serves as a recognised mark of product performance('quality)' within the EU market then it may reduce the importance of 'reputation effects' of larger players and established local companies, thus facilitating SMEs trade within the EU.

- ***Public procurement approaches to bridge the research – markets gap.*** Public procurement plays only a limited role in the overall market for intruder and fire alarm systems. Public procurement approaches may be relevant, however, in the context of the integration of alarm systems (and other electronic security products) in larger projects for the supply of integrated security solutions including, where relevant, provision of associated services (e.g. alarm monitoring services). This could help bridging the gap between research and markets.

- ***Civil-military synergies.*** Possible synergies between civilian and military applications of technologies specifically associated to alarm systems appear to be limited. There may be greater opportunities by looking more broadly to other electronic security products (cf. example of the Israeli industry developing civil applications of surveillance systems, perimeter security, access control, developed for defence purposes).

Implications for the international competitiveness of the EU industry. By reducing market fragmentation the proposed actions should raise the EU overall market efficiency

---

that the EU wide approach covers markets (or market segments) that are not currently subject to certification then costs of supplying these markets would rise.

and industry performance levels. However, an EU-wide approach to standards, conformity access and certification may also increase the openness of the EU market to non-EU suppliers. In this regard, For EU companies to take advantage of enhanced access to the EU market as a whole may require also responding to increased competition from non-EU suppliers.

The reduction in costs resulting from an EU-wide approach could have a limited (positive) impact on EU price competitiveness in the short term. Nonetheless, there may be dynamic effects as a less fragmented EU market should encourage investment in research, technology development and innovation. An EU-wide certification scheme (and corresponding EU security performance 'mark' or 'quality label') may strengthen broader international market awareness and acceptance of EU products, to the extent that it obtains greater market recognition than existing national certification schemes. This could provide an alternative to (or complement) existing national/propriety safety and quality marks (e.g. the American 'UL Mark').

Annex 8: Background to quantitative analysis of certification

This Annex contains two different analyses of the reduction of costs associated to multiple testing to obtain national certification for: 1. alarm systems and 2. airport scanners:

1. Certification costs associated to alarm systems

Illustration: Conformity assessment and certification of alarm systems.

Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. The costs of certification of an alarm system are on average (with a large spread depending on the nature of the product)[129] at the level of EUR 200-300 thousand for full access to Europe including all tests.

With the introduction of one common CAC scheme with mutual recognition of the certificate across the Member States, these costs of conformity assessment and certification should be reduce significantly. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to EUR 40-60k. Compared to the current national schemes, the total savings for a single Type-1 product from a common EU scheme for conformity assessment and certification would amount to a figure in the region of EUR 160-240k.

Information obtained from industry sources in France indicate that the annual total direct costs (covering initial laboratory tests, factory process control and certification fees) to manufacturers for certification of intruder alarm systems (NF & A2P certification) is in the region of € 450 to € 500 thousand[130]. This, however, does not include preparatory costs or additional costs that may associated with product adaptations etc. required to meet different national approval/certification requirements, which are thought to double overall costs for manufacturers.

Quantification: The costs of certification and conformity assessment for producers in Europe: the case of intruder alarms

Based on the industry estimate as described above, the direct costs for certification have been estimated for France to be around EUR 500 thousand per year. This is the direct cost for certification, and the estimate is that the company costs in preparation for multiple listings and in different product specifications for the different approval needs could well cost this amount again. Hence total costs for certification and conformity assessment for intruder alarm systems are in the order of magnitude of EUR 1 million per year for France.

---

129 CAC costs vary significantly depending on the type of product and specific characteristics. There are also differences across countries in the fees charged for CAC.

130 This figure relates to (voluntary) certification NF & A2P. For more information on NF & AP2 certification see the joint AFNOR-CNPP document "Certification rules Electronic Security Equipment: Intrusion Detection, Access Control Management Systems" available at: HTTP://WWW.CNPP.COM/FR/MEDIATHEQUE/AUTRES-DOCUMENTS/CERTIFIER-IMAGE/H58/REFERENTIEL-NF324-H58-VERSION-ANGLAISE-OCTOBRE-2010.

Our estimate of the total market for intruder alarm systems is around EUR 1.1 billion in 2010. However, there is no information available how this is distributed over member states. It is assumed therefore that this value for France as indicated above is replicated across Europe and is roughly in line with the GDP. Given a share of France of 16% of EU economy, then this would suggest a total cost for producers in Europe of around EUR 6.2 million per year for certification and conformity assessment of intruder alarms.

Estimates from other sectors, suggest that the cost associated to differences in technical rules and multiple testing/certification are between 2% to 10% of production costs[131]. This is an estimate for different products outside the security sector, and has been applied in the Commission's impact assessment for the New Legislative Framework[132]. The same impact assessment indicates that in 2002 43% of enterprises in the area of burglar alarm systems have encountered problems with mutual recognition. From these sources it is unclear what costs are precisely included in the range of 2%-10%.

Therefore, in order to be conservative, the lower bound of the estimate is taken for this study of 2% of production costs. It is also not clear what proportion of the total market of intruder alarm systems of EUR 1.1 billion is covered by products/systems that require certification. If one assumes that 75% of the market is covered by certified products, this would give a market value of EUR 825 million.[133] At 2%, this would suggest a cost to the industry of EUR 13.2 million, where production costs have been taken at 80% of the total relevant market value of EUR 825 million.

Estimated cost savings

The total costs for certification and conformity assessment of intruder alarm systems is thus estimated to range between EUR 6.2 million and EUR 13.2 million per year. These costs cannot be reduced completely. After all, there is still need for a single certification and conformity assessment, and associated need for testing etc. It is assumed that a single EU system reduces the cost associated to differences in technical rules and multiple testing/certification by three-quarters (75%). This would suggest a saving of EUR 4.7 million to EUR 9.9 million per year.

2. Certification costs associated to airport scanners

Illustration: Conformity assessment and certification of screening equipment

It was not possible to obtain detailed information on the (direct) costs of testing for airport scanners. An industry source has indicated, for example, that the cost of a single test of an Explosive Detection System (EDS) could be in the region of €65 thousand and for a liquid explosive system (LAGS) the figure may vary from €30 to €75 thousand; these figures relate to a single test procedure and do not take into account any repeat

131 Fabienne Ilzkovitz, Adriaan Dierx, Viktoria Kovacs and Nuno Sousa, « Steps towards a deeper economic integration: the internal market in the 21st century ", European Economy, Economic Papers, No. 271. January 2007. European Commission.

132 European Commission, 2007, Impact assessment on Directive laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision 3052/95/EC, SEC(2007) 112/2.

133 The 75% certification coverage of the alarm systems market is an estimation of the Commission services, based upon data from EURALARM.

testing that may be required. The aforementioned products are relatively small systems and costs associated for larger systems are reputed to be significantly higher and may run into several hundred thousand Euro; for example, an amount of €100 thousand has been indicated for an 'imaging test' for a cargo scanner while a figure of €500 thousand has been indicated for the cost of the certification process for a biometric identity card model.

Quantification: The costs of certification and conformity assessment for producers in Europe: the case of airport scanners

In order to quantify the effect regarding the costs of certification and conformity assessment for producers of airport scanners and screening equipment, the first question is how many certification and conformity assessment procedures are currently carried out per year. There is limited information available on that subject. From statistics available it can be derived that there are at least on average some 20 certifications and approvals of this type of equipment per year.

However, this reflects only the awarded certifications and/ approvals, but does not reflect those products that did not get a certification or approval, and needed multiple re-iterations of the process. Furthermore, it is the certification and approval outcome of only two entities (DGAC and ECAC) in Europe. Therefore, it may be assumed that the annual number of airport scanning and screening products that go into a certification and approval procedure is higher than the 20 mentioned before. A conservative assumption would be 30 products, which is used in this study. In reality this could be even higher.

As the market size for airport scanners and screening equipment differs per country, producers will not offer all 30 products for a certification / approval procedure in each of the 27 Members States. After all, some small Member States with only 1 or 2 airports will not purchase equipment every year, and therefore producers will not or very limitedly enter a certification or approval procedure for new products if they don't expect to sell their products in short term. Apart from that, some countries don't have a formal certification or approval system, but would rely on certification or approval of other member states or ECAC, perhaps with some minor testing of the equipment before implementation.

On the other hand there are Member States with a large airport scanner and screening equipment market with a more rigorous certification and approval procedure, under which all 30 products may be expected to be offered for certification or approval on average per year. Finally, there is a category of countries in between these two ends of the spectrum sketched above, with a medium sized market for airport scanning and equipment products and a certification and some approval regime that thus does not address all 30 products every year. Based on this the 27 Member States have been allocated to three categories, which is presented in the following table.

Category	Airport scanner market size	Member states	Certification and approval regime	Number of countries
1	Large	DE, ES, FR, IT, UK	Full certification and approval of all scanners	5

2	Medium	AT, BG, EL, FI, HU, NL, PL, RO, SE	Some certification and approval half of the scanner	9
3	Small	BE, CY, CZ, DK, EE, IE, LT, LV, LU, MT, PT, SI, SK	Limited certification and approval of few scanners	13
				27

Subsequently, the certification and approval regimes have been further defined. For category 1, full certification and approval of all scanners, it is assumed that thus 100% of the 30 scanners will be certified and approved each year. For category 2, it is assumed that this is 50%, and for category 3 10% is adopted. Furthermore, as outlined above, there may be some variation of the costs of a certification, as this is strongly dependent on the product type. A range from EUR 35 thousand, via EUR 65 thousands, and EUR 100 thousand to even EUR 500 thousand has been mentioned by industry for the certification of a product.

The EUR100 thousand relates to a scanner and this value has therefore been taken in the quantification as a proxy for the costs for a full certification and approval, applying for the five countries in category 1. It has been assumed that the certification and approval process is relatively more light in category 2, and therefore costs have been determined at 50% of the full certification costs, hence at EUR 50 thousand. Finally, costs for certification and approval in category countries have been taken as 10% of the full value, hence EUR 10 thousand.

In this latter category it is anticipated that authorities in these countries would heavily rely on the certification and approval of products by large Member States, and would require themselves only some limited testing. Based on these assumptions, the annual costs for certification and approval of airport scanner and screening equipment in Europe has been estimated at EUR 22 million, which is further detailed in the table below.

Category	Number of countries	Number of certifications & approvals per year, per country	Number of certifications & approvals per year, in Europe	Costs of certification and approval for producers	Totals costs
Maximum annual number of products for certification and approval		30			
1	5	30	150	EUR 100K	EUR 15 M
2	9	15	145	EUR 50K	EUR 6.75 M
3	13	3	39	EUR 10K	EUR 0.39 M
Total	**27**		**334**		**EUR 22.14 M**

Estimated cost savings

A harmonisation of the certification and conformity assessment procedures for airport scanners would prevent all duplications at national level, which allows for considerable cost savings. The cost for certification and conformity assessment would thus amount to EUR 3

million (30 products * EUR 100 thousand). This implies that the impact of the harmonisation in terms of reduction of costs for certification and conformity assessment would amount to approximately EUR 19 million per year.

Annex 9: Background to quantitative analysis of PCP

The idea is to evaluate the impact that a European PCP programme comparable to the US SBIR programme could have on the European security industry. We have seen that R&D support schemes such as SBIR or PCP have a strong impact on growth of sales and employment, through more innovation coming into the market, which increases the competitiveness of the industry.

Thus it is reasonable to suppose that in the event of the EU implementing an efficient PCP scheme in the security field, the competitiveness and consequently the growth of the European security industry would be greater than in the event of the EU not doing so.

This could be translated in terms of a differential of growth for the European security industry over the next five years. With no PCP scheme, European industry will lose market shares to its competitors, whereas if a PCP scheme is implemented European industry may on the contrary gain market shares, or at the very least maintain its position.

There appears to be a reasonable consensus that the overall size of the world security equipment market has a value of approximately €100 billion, with an industry employing about 2 million people.

By geographical region, North America (mainly the US) is widely recognised as having the largest security market, with most available data sources indicating a current market share of around 40% or more. **Europe is ranked 2nd in the global security market, with a market share ranging approximately between 25% and 35%.** Although the recent financial crisis could imply a slowing of growth in 2009-2010, global demand for security equipment is expected to grow at around 5% annually through the coming years. Strongest gains are expected to occur in the less developed markets of Asia, Africa/Middle East and Latin America. The European market should grow faster than the American market, as it is still relatively undersized.

Estimating the possible impact of a PCP scheme

Implementation of a PCP scheme should improve the competitiveness of the European security industry on European and world markets. Compared to a no-PCP situation, this should lead to faster growth of the European security industry.

With no PCP scheme, security industry growth in Europe until 2016 should be around 5% per year, close to the world average. The studies mentioned above show that companies receiving R&D support through SBIR or PCP programmes grow faster than the others. But there is no easy way to quantify the increase in growth for the whole industry caused by this faster growth of recipient companies. However we have attempted to show what the effect of an increased growth rate could be on the sales and employment of the European security industry.

A tentative assumption of a 1% increase in the annual growth rate due to R&D support through a PCP scheme would lead to extra sales of 2 billion € compared to the baseline situation, and to an increase in employment of 40 000. The employment figure is based on the world employment of 2 million in 2009, projected assuming a constant sales/employment ratio. The calculations in the table below detail the possible evolution from 2012 to 2020, given that the first results of the use of PCP/POV schemes in EU security research cannot be

expected earlier. It should be noted that these are conservative estimations based on the results of the US SBIR programme.

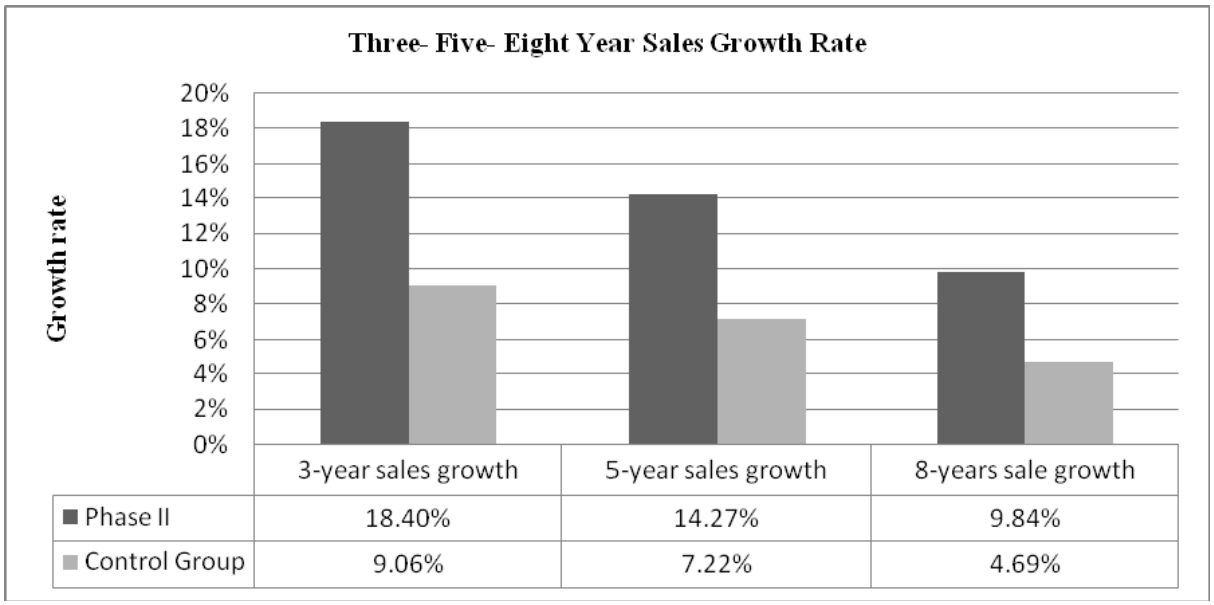
Possible impact of a PCP scheme on the European security industry

	2012	Prevision on the 2020 market value without the use of PCP schemes		Prevision on the 2020 market value with the use of PCP schemes		PCP impact
		growth (in %)	Projected market value in 2020	growth (in %)	Projected market value in 2020	
European security market value (billion €)	17	3.5	23	4.5	25	+ 2
European security industry production (billion €)	22.7	2.6	28	4.5	33	+ 5
European security industry employment (thousands)	140	2.6	172	4.5	203	+ 31
European security service employment (equipment related) (thousands)	283	3.5	372	4.5	406	+ 34

A brief overview on the effects of the US SBIR programme on growth and employment can be fund in the two tables below.

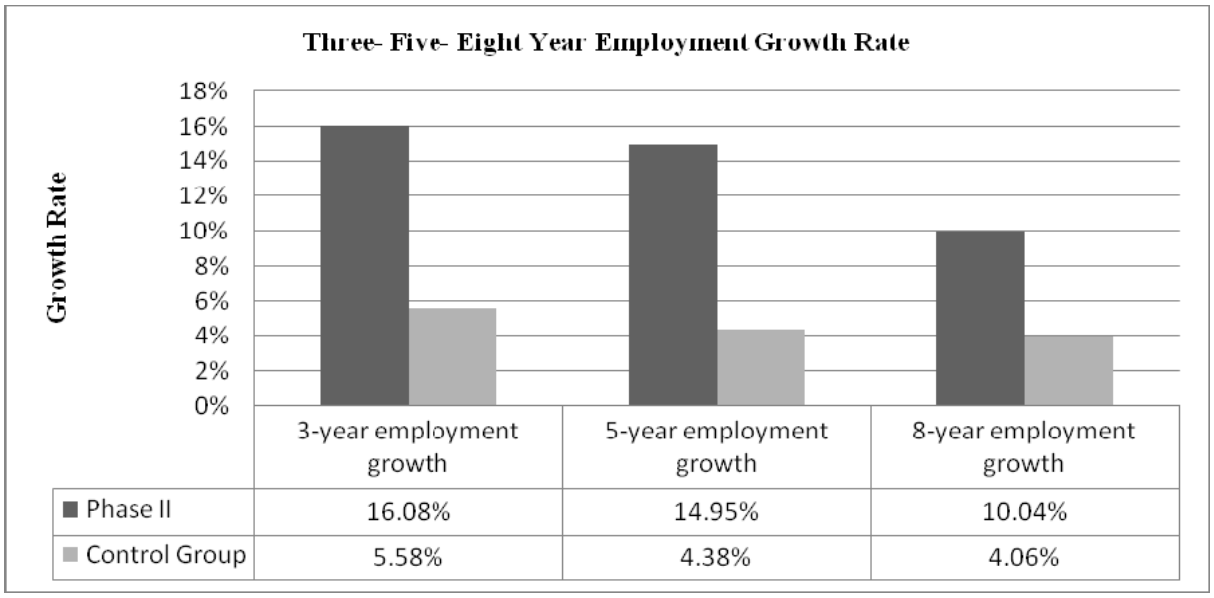
Metin Ege in his thesis on "How do grants influence firm performance? An econometric evaluation of the SBIR programmes at NIH" (2009) compared two samples of data, a test and a control one in order to check the effect of the SBIR programme on the average sales growth for the NIH projects for three, five and eight years. The results demonstrated at 1 % significance level that the average sales growth was higher in the groups of Phase II awardees than the non-recipients group. The following figure shows that the sales growth of the SBIR firms reaches 18, 13 and 8 % in three, five and eight years respectively. At the same time, the non-SBIR firms demonstrated a growth of 8, 7 and 5 %.

Results were similar when all recipients (Phase I and Phase II) were compared to all non-recipient applicants.



source Metin Ege

Metin Ege in compared two samples of data in the same way as described above for sales growth to check the effect of the SBIR programme on the average employment growth for the NIH projects for three, five and eight years. The results demonstrated at 1 % significance level that the average employment growth was higher in the groups of Phase II awardees than the nonrecipients group. The following figure shows that the employment growth of the SBIR firms reaches 16, 15 and 10 % in three, five and eight years respectively. At the same time, the non-SBIR firms demonstrated a growth of 6, 4.4 and 4 %.



source Metin Ege

Annex 10: Background to quantitative analysis of Civ-Mil Synergies

All data are based on the Civil Military Synergies Study.

The four following fields were analysed on their potential for civilian military synergies:

- Infrared cameras
- C^4I (Command, Control, Computers and Intelligence)
- Radio-communications

1. Infrared cameras

Infrared cameras were developed for the military. Civil markets will have more than doubled the military market by 2020.

Basically two technologies, both originated with the military:

- Cooled sensor camera, for high performance, and long range
- Uncooled sensor cameras, for lower performance

It is thought that considerable further market development could come if cooled sensor prices could be cut. With the proper investment in R&D, cooled sensor prices could be reduced by a factor 2 or 3, and that this would enable a tenfold increase in the market.

2. Command, Control, Computers and Intelligence - C4I

C^4I is a wholly dual domain. They are a particular field within the data processing and communications sector, centred on a particular application which originated in the military field using civilian technologies. It extends to security for similar needs, functions, equipment and software.

Quantifying the relative share of military and security is difficult, as the systems are more or less the same, and even the personnel involved are the same. The only way to differentiate the two is by the nature of the customer (military or security).

The applications differ however. Border security for example is very similar to military applications, whereas police, or fire-fighting are more decentralised, and use less sophisticated equipment.

The customer attitude is also different. The military have ambitious specifications, but they can accept a system that is not perfect at the start, but that will evolve and adapt. The civilian security market on the other hand will only accept a system that is perfectly operational right from the start.

A third, important, difference is in the field of standards. In the military market the NATO standards are used all over Europe. In the civilian security market there are no standards yet. The main question is developing common exchange protocol standards.

Thus it would probably be useful to harmonise civilian C^4I needs, and maybe to attempt to transpose the NATO standards, and to this end to integrate the military into the civilian security work groups. This is not done yet at the European level.

3. Radio-communications

Basically this sector is driven by civil technologies. PMR (Professional Mobile Radio) and CNR (Combat Network Radio) are tailored for specific security or military applications and constraints, but they use technologies developed for the general civil mobile telephony markets, and this will continue in the future.

The specific military need could be no more than 20%, in the total PMR-CNR segment. But this result would need to be organised, with common work on standards and specifications. In particular it will be necessary to consider military needs in the present phase of civil R&D so that the technologies developed can also be used by the military.

After the present peak in military demand due to renewal, the civil security market should be the driver (after 2015).

Assessing the impacts of the three segments

The examples we have looked at show several types of impact on the European industry. In the long term there seem to be cycles where civil and military markets or technologies are alternately the driving force and governed by these cycles, markets and activities fluctuate and change. This is in particular the case in radio-communications.

In the shorter term, and looking forward from today, civil-military synergies either open new civil markets to products developed for the military (infrared cameras), or they enable scale-effect cost reduction by the military using civil technologies (radio-communications), or they enable development of systems that are specific to the security and military fields (C^4I).

This is of course a very simplified view, focusing on the more immediate economic results measured on levels of activity and employment.

Table 1 Military-civil synergy impact on activity in examples studied

Spin-off generates additional civil markets	
Infrared cameras	Market +>30% of which security +10% up to today
Duality generates civil markets to relay military programme completion	
Radio-communications	Dual market, uses civil technologies Civil market growth will relay military market growth after 2015
C^4I	New dual market; Military market could drop by 2020, civil market needed to relay growth

The following table attempts to quantify the examples. These figures are rough estimates, designed to give orders of magnitude rather than precise indications. Moreover the civil markets given are not only security markets, they sometimes include some industrial or commercial applications, or even, in the case of infrared cameras, automotive applications. At this stage it is not possible to provide a final analysis.

At this stage we considered that all market growth up to 2020 could be ascribed to the benefits of duality. This is of course only partly true, as there could be some growth from market size increase in the absence of any duality. However, in the examples chosen, duality is at the heart of growth through spin-offs generating new markets (in these cases mostly civil, but also military in the case of radio-communications).

Table 2 Estimations on the possible benefits through the exploitation of civil military synergies

Civil Military synergies	**Increase in sales**		**Added employments**	
	Defence and Security	Only Security	Defence and Security	Only Security
Infrared cameras	EUR 450 million	EUR 440 million	2.800	2.750
C4I	EUR 300 million	EUR 900 million	1.875	5.625
Radio Communication	EUR 1.000 million	EUR 1.500 million	-3.125	9.375
Total	EUR 1.7 billion	EUR 2.840 billion	1550	17.750

Table 3 Market evolution in the 4 sectors covered, 2010-2020.(million €)

	World		**Europe**	
	2010	**2020**	**2010**	**2020**
IR cameras mil	2600	2800	530	540
IR cameras civ	1100	3300	220	660
IR cameras total	***3700***	***6100***	***750***	***1200***
C^4I mil	5800	3500	1700	1100
C^4I civ	1000	4000	300	1200
C^4I total	***6800***	***7500***	***2000***	***2300***
Radio-comms mil	2300	3800	1500	1000
Radio-comms civ	7900	9900	1000	2500
Radio-comms total	***10200***	***13700***	***2500***	***3500***
All examples mil	10700	10100	3730	2640
All examples civ	10000	17200	1520	4360
All examples total	**20700**	**27300**	**5250**	**7000**

(Source: Study on Civ-Mil Synergies:
HTTP://EC.EUROPA.EU/ENTERPRISE/POLICIES/SECURITY/DOCUMENTS/INDEX_EN.HTM#H2-3)

The examples considered only represent a small part of the security and military markets (around 5%). A number of other synergy domains exist, and will be studied later on. But with only these four examples dual synergies and market growth with no additional action should bring an increase in employment, not counting services, of nearly 3% by 2020.

Annex 11: Initial list of EU wide standards for security

Committee	Reference	Title
CEN Committees		
CEN/TC 169 - Light and lighting	EN 15193:2007	Energy performance of buildings - Energy requirements for lighting
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 726-1:1994	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 1: Systems overview
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 726-2:1995	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 1387:1996	Machine readable cards - Health care applications - Cards: General characteristics
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 726-7:1999	Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7: Security module
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 1546-2:1999	Identification card systems - Inter-sector electronic purse - Part 2: Security architecture
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 1546-3:1999	Identification card systems - Inter-sector electronic purse - Part 3: Data elements and interchanges
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 1332-5:2006	Identification card systems - Man-machine interface - Part 5: Raised tactile symbols for differenciation of application on ID-1 cards
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 15320:2007	Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework
CEN/TC 224 - Personal identification, electronic signature and cards and their related systems and operations	EN 1332-1:2009	Identification card systems - Human-machine interface - Part 1: Design principles for the user interface

CEN/TC 247 - Building Automation, Controls and Building Management	EN 13321-1:2006	Open data communication in building automation, controls and building management - Home and building electronic system - Part 1: Product and system requirements
CEN/TC 251 - Health informatics	EN ISO 21549-5:2008	Health informatics - Patient healthcard data - Part 5: Identification data (ISO 21549-5:2008)
CEN/TC 251 - Health informatics	EN ISO 21549-8:2010	Health informatics - Patient healthcard data - Part 8: Links (ISO 21549-8:2010)
CEN/TC 251 - Health informatics	EN ISO 27799:2008	Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)
CEN/TC 251 - Health informatics	EN 13606-4:2007	Health informatics - Electronic health record communication - Part 4: Security
CEN/TC 251 - Health informatics	EN ISO 21549-6:2008	Health informatics - Patient healthcard data - Part 6: Administrative data (ISO 21549-6:2008)
CEN/TC 251 - Health informatics	EN ISO 13606-5:2010	Health informatics - Electronic health record communication - Part 5: Interface specification (ISO 13606-5:2010)
CEN/TC 263 - Secure storage of cash, valuables and data media	EN 1300:2004+A1:2011	Secure storage units - Classification for high security locks according to their resistance to unauthorized opening
CEN/TC 278 - Road transport and traffic telematics	EN 12834:2003	Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) - DSRC application layer
CEN/TC 278 - Road transport and traffic telematics	EN ISO 14816:2005	Road transport and traffic telematics - Automatic vehicle and equipment identification - Numbering and data structure (ISO 14816:2005)
CEN/TC 278 - Road transport and traffic telematics	EN ISO 24014-1:2007	Public transport - Interoperable fare management system - Part 1: Architecture (ISO 24014-1:2007)
CEN/TC 278 - Road transport and traffic telematics	EN 15509:2007	Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC
CEN/TC 278 - Road transport and traffic telematics	EN ISO 24534-4:2010	Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO 24534-4:2010)
-	EN 15602:2008	Security service providers - Terminology

CEN/TC 384 - Project Committee - Airport and aviation security services	EN 16082:2011	Airport and aviation security services
CENELEC Committees		
CLC/TC 9X - Electrical and electronic applications for railways	EN 50126-1:1999	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process
CLC/SC 9XA - Electrical and electronic applications for railways	EN 50159:2010	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
CLC/SR 56 - Dependability	EN 61907:2010	Communication network dependability engineering
CLC/TC 57 - Power systems management and associated information exchange	EN 61850-7-2:2010	Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)
CLC/TC 79 - Alarm systems	EN 50130-4:1995	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
CLC/TC 79 - Alarm systems	EN 50130-4:1995/A1:1998	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
CLC/TC 79 - Alarm systems	EN 50130-4:1995/A2:2003	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
CLC/TC 79 - Alarm systems	EN 50130-5:1998	Alarm systems - Part 5: Environmental test methods
CLC/TC 79 - Alarm systems	EN 50131-2-3:2008	Alarm systems - Intrusion and hold-up systems - Part 2-3: Requirements for microwave detectors
CLC/TC 79 - Alarm systems	EN 50131-2-4:2008	Alarm systems - Intrusion and hold-up systems - Part 2-4: Requirements for combined passive infrared and microwave detectors
CLC/TC 79 - Alarm systems	EN 50131-2-5:2008	Alarm systems - Intrusion and hold-up systems - Part 2-5: Requirements for combined passive infrared and ultrasonic detectors

CLC/TC 79 - Alarm systems	EN 50131-2-6:2008	Alarm systems - Intrusion and hold-up systems - Part 2-6: Opening contacts (magnetic)
CLC/TC 79 - Alarm systems	EN 50131-3:2009	Alarm systems - Intrusion and hold-up systems - Part 3: Control and indicating equipment
CLC/TC 79 - Alarm systems	EN 50131-4:2009	Alarm systems - Intrusion and hold-up systems - Part 4: Warning devices
CLC/TC 79 - Alarm systems	EN 50131-6:2008	Alarm systems - Intrusion and hold-up systems - Part 6: Power supplies
CLC/TC 79 - Alarm systems	EN 50131-8:2009	Alarm systems - Intrusion and hold-up systems - Part 8: Security fog device/systems
CLC/TC 79 - Alarm systems	EN 50132-1:2010	Alarm systems - CCTV surveillance systems for use in security applications - Part 1: System requirements
CLC/TC 79 - Alarm systems	EN 50132-5:2001	Alarm systems - CCTV surveillance systems for use in security applications - Part 5: Video transmission
CLC/TC 79 - Alarm systems	EN 50132-7:1996	Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines
CLC/TC 79 - Alarm systems	EN 50133-1:1996	Alarm systems - Access control systems for use in security applications - Part 1: System requirements
CLC/TC 79 - Alarm systems	EN 50133-1:1996/A1:2002	Alarm systems - Access control systems for use in security applications - Part 1: System requirements
CLC/TC 79 - Alarm systems	EN 50133-2-1:2000	Alarm systems - Access control systems for use in security applications - Part 2-1: General requirements for components
CLC/TC 79 - Alarm systems	EN 50133-7:1999	Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines
CLC/TC 79 - Alarm systems	EN 50136-1-1:1998	Alarm systems - Alarm transmission systems and equipment - Part 1-1: General requirements for alarm transmission systems
CLC/TC 79 - Alarm systems	EN 50136-1-1:1998/A1:2001	Alarm systems - Alarm transmission systems and equipment - Part 1-1: General requirements for alarm transmission systems

CLC/TC 79 - Alarm systems	EN 50136-1-1:1998/A2:2008	Alarm systems - Alarm transmission systems and equipment - Part 1-1: General requirements for alarm transmission systems
CLC/TC 79 - Alarm systems	EN 50486:2008	Equipment for use in audio and video door-entry systems
CLC/TC 79 - Alarm systems	EN 50518-1:2010	Monitoring and alarm receiving centre - Part 1: Location and construction requirements
ETSI Committees		
ITS/WG 2 - Intelligent Transport systems	EN 302 665	Intelligent Transport systems; Communications Architecture
	EN 302 409	Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station
	EN 302 403	Digital cellular telecommunications system (Phase 2+) (GSM); GSM Cordless Telephony System (CTS), Phase 1; Service description; Stage 1 (GSM 02.56 version 7.2.1 Release 1998)
	EN 301 829	Private Integrated Services Network (PISN); Inter-exchange signalling protocol; Wireless terminal authentication supplementary service [ISO/IEC 15433 (2003), modified]
	EN 301 828	Private Integrated Services Network (PISN); Specification, functional model and information flows; Wireless terminal authentication supplementary services [ISO/IEC 15432 (1999) modified]
Broadcast	EN 301 790	Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems
	EN 301 132	Integrated Services Digital Network (ISDN); Security tools (SET) for use within telecommunication services

	EN 301 002-1	Integrated Services Digital Network (ISDN); Security tools (SET) procedures; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification
	EN 301 002-2	Integrated Services Digital Network (ISDN); Security tools (SET) procedures; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 2: Protocol Implementation Conformance Statement (PICS) proforma specification
	EN 300 396-4	Transmission and Multiplexing (TM); Fixed radio link equipment for the transmission of analogue video signals operating in the frequency bands 24,25 GHz to 29,50 GHz and 31,0 GHz to 31,8 GHz
TETRA 06	EN 300 396-6	Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security

General Annexes:

Tables:

1. Summary table: Main competitors
2. Breakdown US security industry market
3. Breakdown US security industry market (public and private involvement)
4. Overview top 10 US security companies (2008)
5. Overview of market characteristics for specific equipment segments
6. Overview of market characteristics for specific equipment segments (continued)
7. SWOT analysis of the European Security Industry
8. SWOT analysis of the European Security Industry (continued)
9. Overview of supply chain characteristics for specific equipment segment
10. Overview of supply chain characteristics for specific equipment segment (continued)
11. Number of annual certifications for aviation security products
12. Executive summary of the "European Security Research and Innovation Forum"

Figures:

13. Figure 1: Public-private involvement in 'traditional' and 'new' security markets
14. Figure 2: Characterisation of security equipment supply and demand
15. Figure 3: Overview of the security market: supply and demand characterisation
16. Figure 4: Europe's technological performance compared with North America and Asia
17. Figure 5: EU Patent shares 2000-2009
18. Figure 6: General Framework: Security Regulation, Conformity Assessment and Certification
19. Figure 7: Overview of ECAC Common Evaluation Process
20. Figure 8: Security ‘products’: specified requirements and conformity assessment

Table1 Summary table: Main competitors

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

TOTAL	**€ 103 bn**	**100%**	

Source: ECORYS based on different sources

Table 2: Breakdown US security industry market

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

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

Table 3 Breakdown US security industry market (public and private involvement)

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

Source: ECORYS based on Civitas (2006)

Table 4: Overview top 10 US security companies (2008)

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

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

Table 5: Overview of market characteristics for specific equipment segments

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

Table 6: Overview of market characteristics for specific equipment segments (continued)

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

Table 7: SWOT analysis of the European Security Industry

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

Table 8: SWOT analysis of the European Security Industry (continued)

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

Table 9: Overview of supply chain characteristics for specific equipment segment

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

Table 10: Overview of supply chain characteristics for specific equipment segment (continued)

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

Table 11: Number of annual certifications for aviation security products

	ECAC*	STAC**
2005		6
2006		1
2007		4
2008		14
2009		18
2010	14	3
2011	14	1
Total certifications	28	47

* HTTPS://WWW.ECAC-CEAC.ORG/ACTIVITIES/SECURITY/CIP_FOR_SECURITY_EQUIPMENT (these certifications have not been made by ECAC itself, but list only those certifications which were based on a ECAC performance standard.

** DGAC France, Service Technique de l'aviation civile: HTTP://WWW.STAC.AVIATION-CIVILE.GOUV.FR/SURETE/TABLOCERTIMAT.PHP

Table 12: Executive summary of the "European Security Research and Innovation Forum"

NEW POLICY INITIATIVES

The above should be supported by stronger articulation of demand, and delivery of the most appropriate solutions by the supply side.

4. New initiatives and programmes should include:
   - creation of knowledge centres such as CBRN expert groups to guide research.
   - preparations to meet foreseeable needs for pan-European network-enabled capabilities and complex systems in early warning and response readiness that deal with natural and man made incidents.
   - expanded critical infrastructure protection programmes.
   - evaluating the applicability and efficacy of the numerous initiatives available to the EU and its Members States such as: a Lead Market initiative, Trans European Networks for Security, the creation of an Internal Security Fund or a "European Security Label".
   - the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place.

INTEGRATED APPROACH TO SECURITY

Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.

5. A *holistic approach* must include:
   - efforts to ensure that the social, cultural, legal and political aspects of security research and development are taken into account. Research programmes should reflect relevant ESRIF key messages and thus promote overall 'societal coherence'.
   - the promotion of a *security by design* approach in any newly developed complex system or product, ensuring that security is addressed at the point of conception, as it has been the case for *safety by design*.
   - programmes to raise societal awareness of security threats, risks and vulnerabilities – and the security and safety impact of emerging critical technologies.

THE GLOBAL DIMENSION

The EU's civil security is a collective responsibility touching government, societal organisations, industry and individual citizens. It cannot stand in isolation from the world.

6. The *globally inter-related nature of security* calls for:
   - a strong and independent technological and scientific base for the EU to safeguard the interests of its citizens and ensure that its industry is able to provide products and services in a competitive manner.
   - giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.

SECURITY RESEARCH: THE FUTURE

The proposed European Security Research and Innovation Agenda – ESRIA – should be seen as a living document.

7. For *ESRIA to evolve* with Europe's internal and external threat environments:
   - A transparent mechanism involving all stakeholders should be set up to implement ESRIA in a balanced and rigorous manner.
   - ESRIA should be revisited and evaluated on a regular basis with special attention to evaluating any measures flowing from ESRIF key messages.

Europe stands on the threshold of a new global approach to security – and of ways to use scientific research and innovation to reinforce and implement that new thinking.

The security of Europe and its citizens is linked to internal and external events and threats, as well as to the increasing convergence of civil and defence capabilities. Above all, it derives from societal imperatives that demand a balancing of the state's policy and technological exigencies with privacy rights, European cultural values and the tenets of democracy.

ESRIF, the European Security Research and Innovation Forum, has spent the past two years analyzing the medium and long-term challenges that Europe faces. These range from natural disasters to organised crime to man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects.

Assisted by more than 600 experts, ESRIF and its 64 members from 31 countries have examined the full range of such threats and tied them to the EU's central civil security missions and to the capabilities required to carry them out.

This collective effort has resulted in a set of key messages that encompass the logic and necessity of future European security and its related research. These messages point to the essence, as ESRIF sees it, of what security research and innovation should flow from – and what it should deliver to society.

Security research should be grounded in an industrial policy that frames a systematic approach to capability development which, in turn, promotes interoperability among the 27 EU nations and establishes common standards. Ultimately this effort must increase societal security in a globalised world, while fostering trust between European citizens, governments and national and European institutions. These and other ideas are among ESRIF's main recommendations included in this executive summary.

To reach an interoperable, trust-embedded and resilient society, however, Europe needs an R&D roadmap, and a mechanism should be set up to implement it in a balanced and rigorous manner. ESRIF thus proposes its European Security Research and Innovation Agenda – "ESRIA" which should go a long way toward achieving that goal.

A research and innovation agenda cannot be created and implemented in a vacuum. The framework is defined by principles given in the Key Messages:

- **Societal Security**
  Human beings are at the core of security processes.
- **Societal Resilience**
  Certain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and must have the ability to recover.
- **Trust**
  Assuring security implies nurturing trust among people, institutions and technologies.
- **Awareness raising through education and training**
  Security is a common responsibility of all stakeholders, the citizen is at the fore front.
- **Innovation**
  Europe can only rely on its own scientific, technological and industrial competences.
- **Industrial policy**
  A competitive European security industry is a prerequisite for future security. The EU must address the fragmentation of its security markets.
- **Interoperability**
  A seamless approach to security is essential for Europe; Interoperability is essential to allow security forces to work together.
- **A systematic approach to capability development**
  The increasing complexity of security, demands increasing sophistication of our Response.
- **Security by design**
  Security features must become integral part of any given system: Europe's society needs a systemic approach to security.

ESRIF has defined a European Security Research and Innovation Agenda (ESRIA) that identifies and roadmaps key capabilities and research needs in line with the main work results.

The ESRIA has been organized into five content clusters and differentiates research topics according to short-, medium- or long-term needs.

The first cluster centres on the classic **security cycle preventing, protecting, preparing, responding and recovering.** It focuses on the securing of people, civil preparedness and crisis management.

The second cluster deals with the **countering of different means of attack,** as a way of dealing with specific, known and projected future risks. It examines ways to detect and identify conventional as well as non-conventional attacks, unintended impacts of other actions, and naturally occurring incidents, to mitigate their effects, and it analyzes potential dangers inherent to coming technologies.

The third cluster aims at **securing critical assets,** such as energy, transport and other crucial infrastructures. It examines security economics and outlines the necessity to analyze and cope with limited access to critical natural resources as well as securing the existence of key manufacturing capabilities and capacities in Europe.

The fourth cluster is about **securing identity, access and movement of people and goods.** It mainly centres on border security and secure identity management.

Lastly, the fifth cluster lists **cross-cutting enablers** of special interest, due to cross-cutting characteristics or prior political strategic decisions. The crucial role of Information and Communication Technologies (ICT) is examined, as are security implications of European space programmes.

ESRIF strongly recommends that the EU and its Member States launch new measures to enhance the security of its citizens. These should also aim to create amenable conditions for European excellence in research and innovation, and thus advance Europe's security. The below sets out policy and operational recommendations for achieving stronger security research and innovation results:

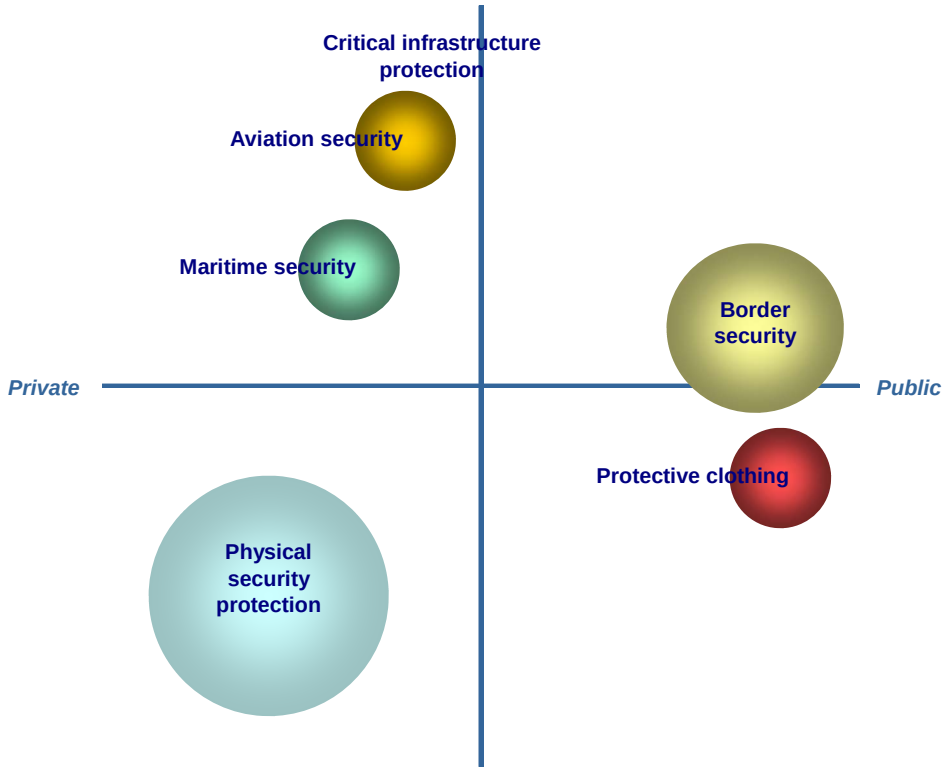
- **COMMON EUROPEAN CAPABILITIES**

The EU must draw on its collective strengths and knowledge by developing common capability via enhanced transnational co-operation.

1. This calls for *close consultation across Europe* among supply, demand and end-user stakeholders across the planning, execution and review cycles of security research policy. The demand side in particular – governments and end-users – needs organisational re-alignment to both shape and respond to security innovation.
2. *Resources and incentives* are essential to developing common capability. ESRIF recommends, notably with a view to the implementation of ESRIA, that the EU maintains the current rate of growth of its security research programmes – with the aim of reaching an annual budget of one billion euros as proposed in 2004 by the Group of Personalities. National programmes should reflect this degree of ambition. Regarding the necessary research and industrial synergies, technical compatibility and interoperability of new security solutions, a significant effort is required to ensure the coherence of national and EU efforts through enhanced coordination.
3. Research programmes should be complemented by additional implementation programmes. Success on the global market strongly depends on EU market procurement references. Pre-commercial procurement of innovative solutions should be exploited as a mechanism to bring research results closer to the market.

Figures:

Figure 1: Public-private involvement in 'traditional' and 'new' security markets

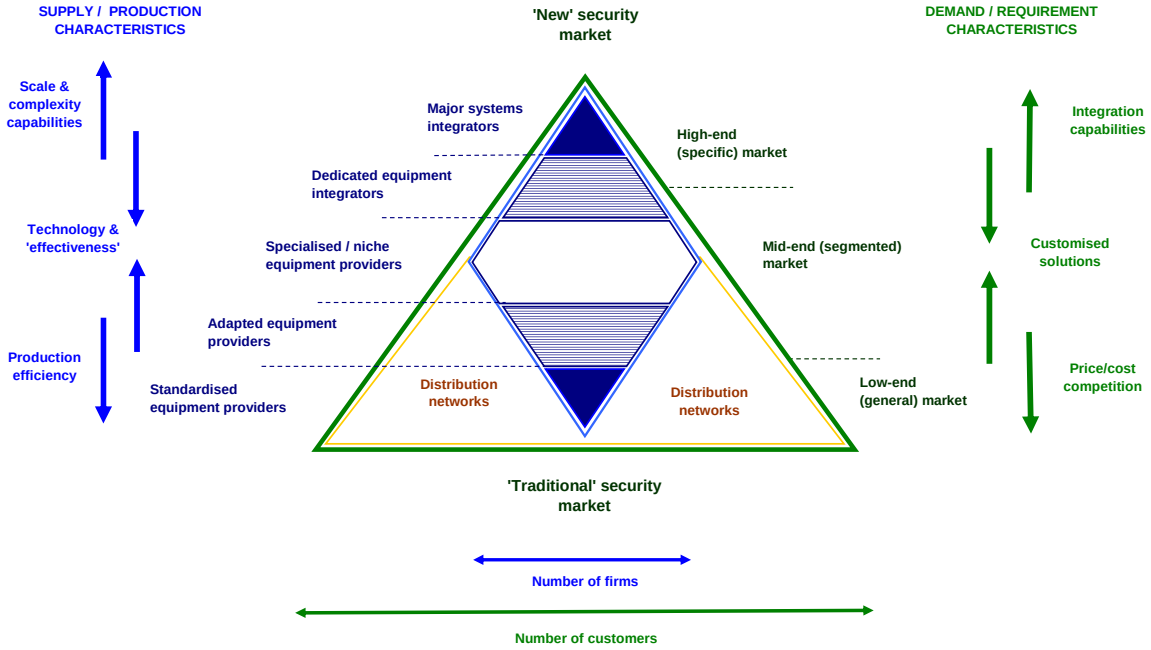


This figure translates in the following numbers:

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

Source: ECORYS

Figure 2 Characterisation of security equipment supply and demand



Description:

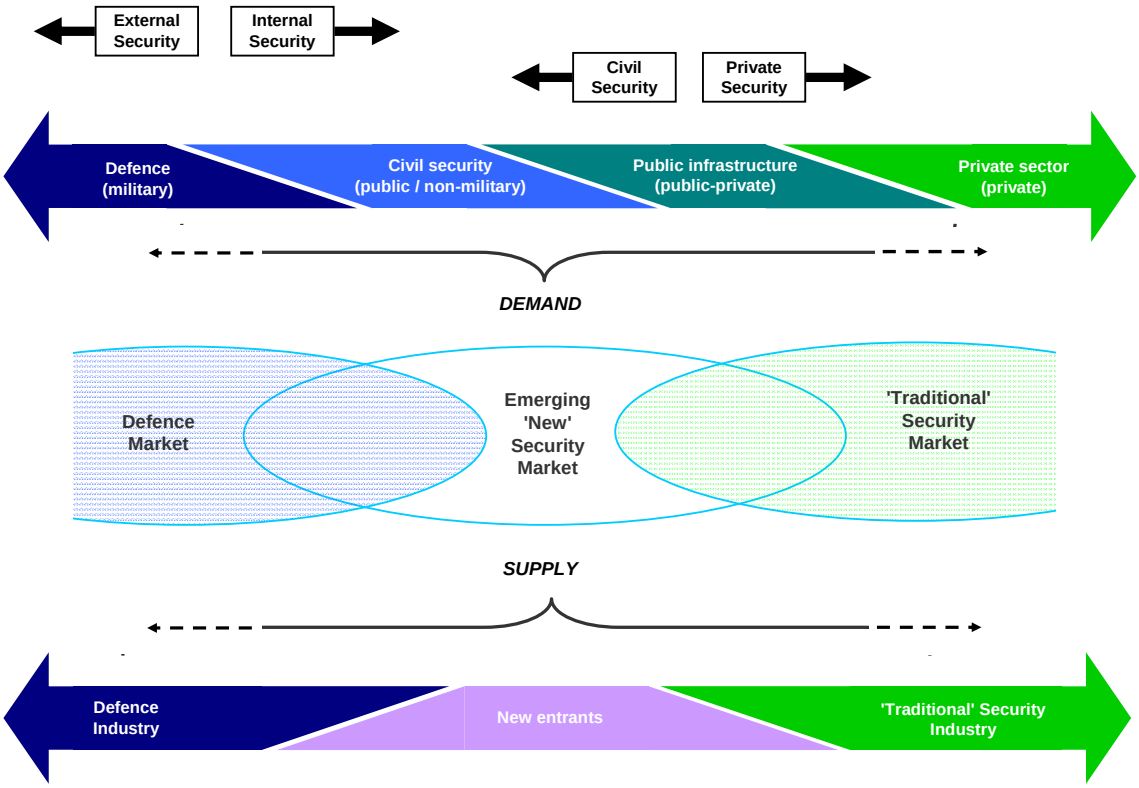
- **The demand-side** of the market is represented as a triangle with, at the bottom, a broad base of demand for general 'low-end' security equipment and systems. This would cover standardised products destined to a broad base of customers or customer segments; typically this segment of the market is seen as quite price/cost-sensitive. At the top of the triangle is the 'high-end' of the market, characterised by demand for specialised types of security equipment and systems, for which the number of customers (or customer segments) is relatively limited but where security 'projects' can be very large in terms of their individual size and can require high levels of integration between different types of security applications. In between the 'general' and 'specific' market segments, there is a 'mid-end' market with demand for customised equipment and systems providing larger security capabilities than provided by 'general' (or 'mass-market') type applications but that are not as highly specific as the top-end.

- **The supply-side** of the market (security industry) is represented by the central diamond; here we distinguish[134].

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

- **‘Standardised equipment providers’**. At the bottom of the diamond – corresponding to supply of standardised equipment aimed at the general/mass market, production tends to be limited to a few major companies (see above).
- **‘Adapted equipment providers’**. These providers typically supply products that are of a similar type to standardised equipment but with a greater degree of adaptation to different market/customer requirements (e.g. modular approaches or partial customisation).
- **‘Specialised / niche equipment providers’**. These are providers of specialised and highly-customised security equipment and systems, typically for particular market segments with specific sector-based or technology-based requirements. Given the high customer-specific requirements (which imply relatively small demand base for individual equipment/systems) there tend to be many suppliers but each addressing specific segments/niches. Alternatively, such providers may provide security applications on the basis of technologies that have wider applications in other fields.
- **‘Dedicated equipment integrators’**. These are also providers of specialised security equipment and systems but typically have a broader portfolio of products (or customer base) than specialised providers.
- **‘Major systems integrators’**. These are the major security systems integrators responsible for coordinating the implementation of major security projects/solutions (e.g. systems of systems). Their main characteristic is the capability to manage large-scale and complex projects and they may provide only a limited part of the security equipment and systems themselves, but ‘buy-in’ systems from other (dedicated or specialised) providers.

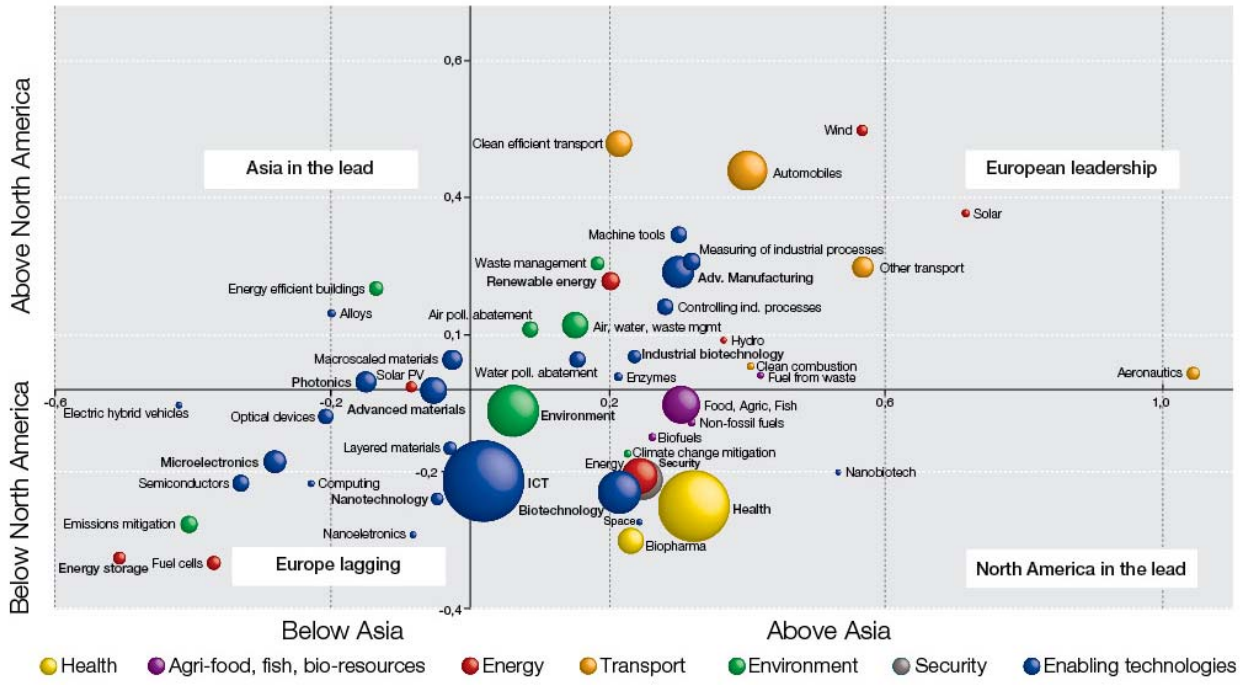
Figure 3: Overview of the security market: supply and demand characterisation



Three broad segments of the EU security market can be identified:

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

Figure 4: Europe's technological performance compared with North America and Asia [135]



Source: *DG Research and Innovation*

Data: *OECD patent database and specific studies*[136]

If one takes a combined look at Europe's relative performance in both science and technology across various fields (Figure 4), one sees that it is ahead of the US in terms of both science and technology output in the field of aeronautics and space. However, Europe is weaker than the US in the fields of security, nanotechnology, biotechnology and ICT, as well as in health and new production technologies.

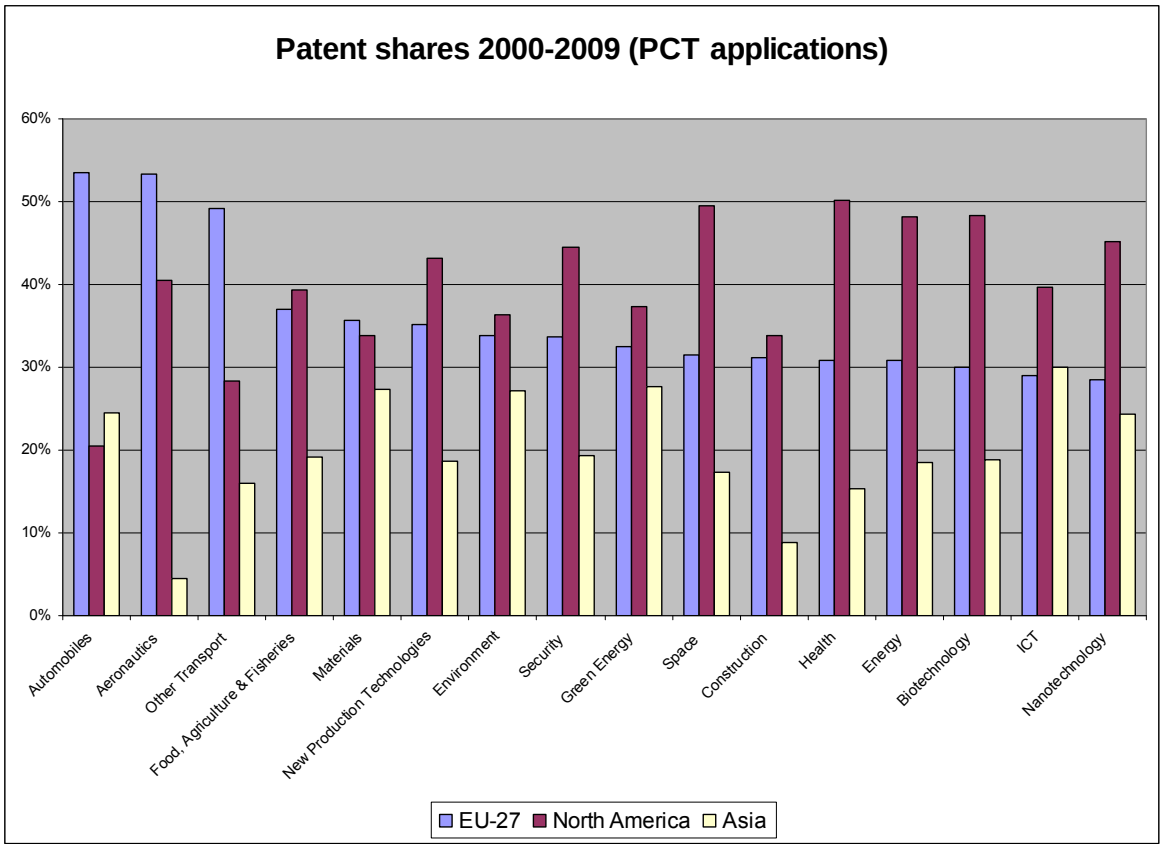
[135] For each technology field the graph shows on the X axis the global market share of Europe in terms of EPO/PCT patents compared with the market share of Asia (expressed as a logarithm), and the Y axis shows the market share of Europe compared with the market share of North America (expressed as a logarithm). (2) The broad technology domains are shown in bold

[136] Data for broad technology domains taken from a study by Research Division INCENTIM, MSI, Faculty of Business & Economics, KULeuven, Università Commerciale Luigi Bocconi, KITES); Data for enabling technologies taken from "European Competitiveness in Key Enabling Technologies" by Birgit Aschhoff, Dirk Crass, Katrin Cremers, Christoph Grimpe, Christian Rammer (ZEW, Mannheim), Felix Brandes, Fernando Diaz-Lopez, Rosalinde Klein Woolthuis, Michael Mayer, Carlos Montalvo (TNO, Delft), May 28th, 2010 (Study commissioned for European Commission DG Enterprise); All other data from OECD Patent Database.

When it comes to the development of new technologies, Europe needs to rise to the challenge of global competition. It is relatively strong in certain more traditional fields such as automobiles, aeronautics, other transport and construction, where it must seek to maintain its large share of global patents (see Figure 5). However, in a number of technology areas Europe is behind its competitors. This is certainly true for some key enabling technologies: for example in nanotechnology the EU has

28% of world patents compared with 45% for the US and 24% for Asia; in biotechnology it has 30% versus 48% for the US and 19% for Asia; while in ICT the EU has 29% of global patents, the US 40% and Asia 30%. The EU also lags in terms of patents in key areas for the future, notably health, energy, space and security.

Figure 5 "Patent shares 2000-2009:



Data: EPO PATSTAT database (from a study by Research Division INCENTIM, MSI, Faculty of Business & Economics, K.U.Leuven, Università Commerciale Luigi Bocconi, KITES)

Figure 6: General Framework: Security Regulation, Conformity Assessment and Certification

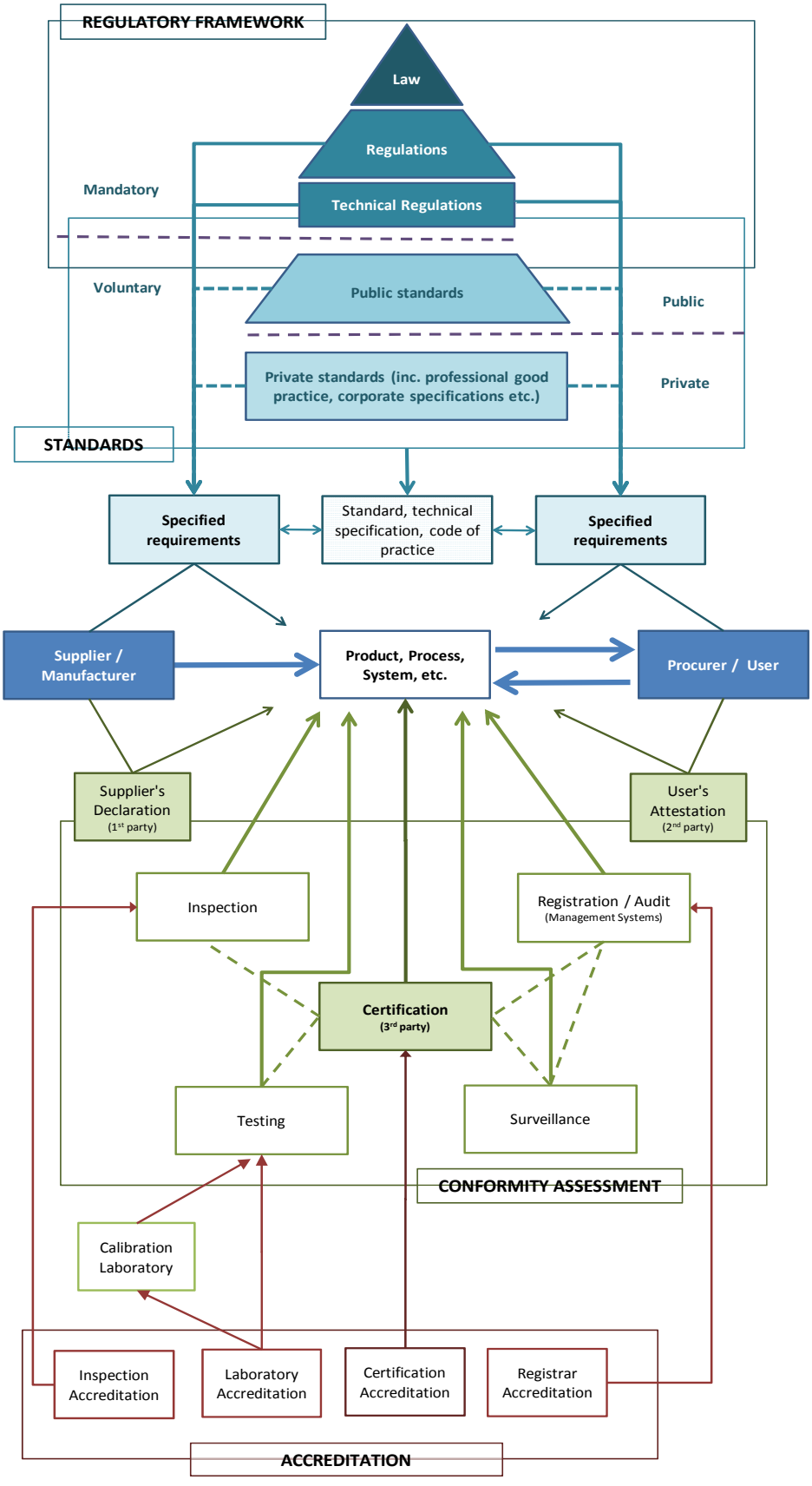


Figure 7: Overview of ECAC Common Evaluation Process

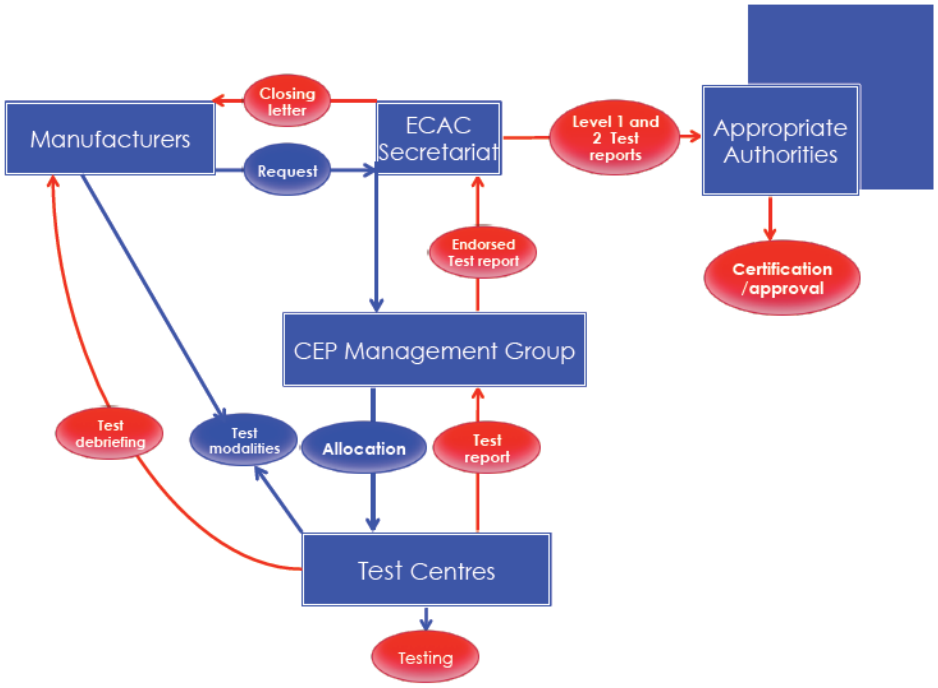


Figure 8: Security ‘products’: specified requirements and conformity assessment