15-06-10

Istituto Affari Internazionali

Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence

(Contract no. SI2. 516182)

Final Report

Content

Annexes

Tables

Executive Summary

Context

This is the Final Report on "The industrial implications in Europe of the blurring of dividing lines between security and defence", initiated on 22nd December 2008 by the European Commission, Enterprise and Industry Directorate-General (Aerospace Security Defence and Equipment, H1/D), under Contract No ENTR/08/023, SI2.516182. The Study has been coordinated by the *Istituto Affari Internazionali* (IT) with partners from the Manchester Institute of Innovation Research (UK) and the *Institut des Relations Internationales et Stratégiques* (FR).

This study was launched as a result of the significant role played by the European Commission (EC) in the field of security over recent years. Various initiatives have been launched, the most visible and important being:

- the European Security and Research Programme (ESRP)
- the Security Theme of the 7th Framework Programme
- the European Security Research and Innovation Forum (ESRIF)
- the European Programme for Critical Infrastructure Protection (EPCIP)
- Directives on European Critical Infrastructures for Maritime and Air Transport, and
- the Instrument of Stability for External Security.

In addition, the EC has started to be active in the defence market. In 2008, two directives were adopted as part of the so-called "defence package" and research efforts have begun to be coordinated with the defence community, in particular with the European Defence Agency (EDA).

The EC has identified converging activities between the security and defence markets and has therefore initiated this study to explore the potential implications.

Concept

The Consortium's working hypothesis is found in the title of the study, which assumes that there is a progressive blurring in the traditional division between the security and defence sectors. The aim of this study is to analyse the truth behind the hypothesis, understand its impact on the industrial base operating in both sectors and make recommendations for future EC decision-making.

Security and defence have traditionally been dealt with separately, as the internal and external aspect of what is called the SECURITY of a state or society. Our thinking, our political institutions and our political and economic activities have all been deeply influenced by the fundamental distinction between the two. Thus defence was considered as a response to an external threat from a foreign adversary and implied the use of force by military actors; (internal) security, on the other hand, was rather linked to domestic threats such as crime or public order and safety, requiring a moderate use of force, but also protection of civil rights and privacy. Different actors were responsible, such as the police, disaster relief services and law enforcement agencies.

The clear-cut distinction between security and defence has also had important industrial implications. Given their different equipment requirements, security and defence forces have traditionally been supplied by different industries. While public security providers could often use commercially available products that required little or no adaptation, the military relied on a specific defence industrial and technological base capable of delivering sensitive and complex weapon systems. Such companies specialised in two things; the development and manufacturing of bespoke equipment exclusively for a single customer (MoDs) and the management of long-term processes, rather than the development of rapid responses to a market with short-term changes.

Since the end of the Cold War, and even more since 9/11, however, the distinction between the concepts of security and defence described above has been progressively blurring. The reasons are generally well known and are very much linked to the rise of new threats of a trans-national and trans-border nature, such as international organised crime or terrorism. This has led actors traditionally responsible for "internal" security, such as police forces, to intervene outside their national territory and participate in missions which were traditionally under the responsibility of the armed forces, jointly or in cooperation with them. For the same reasons, armed forces have started to become involved in the security of the national territory, alongside security forces. However, security and defence actors also continue to maintain their traditional responsibilities

with, for example, Ministries of Defence (MoDs) and Ministries of the Interior (MoIs) having differing portfolios, sometimes making cooperation difficult.

There is therefore a clear overlap between the security and defence sectors, as is often recognised in public debate, but its specific nature and scope has never been deeply analysed. Against this background, the study team decided to begin its research by questioning the assertion made by the title of the study and conducting a critical analysis of the concept of blurring, before addressing its potential impact on industry.

Objectives

Accordingly, the starting point of the study has been to define the area of blurring between security and defence, understanding in particular its scope, its nature, importance and potential evolution. Based on these findings, we have analysed the impact of this overlap on market structure (customers and suppliers). Finally, we have assessed whether this blurring could present opportunities or challenges in the future for companies involved in the security and defence sectors.

In so doing, the research team has worked on five questions that have shaped the analysis presented in the chapters of this report:

- *To what extent are the dividing lines between security and defence blurring?*
- *Which market segments are particularly affected by the blurring?*
- *What are the drivers and barriers to blurring?*
- *Is blurring a positive or negative factor for the industry?*
- *Should the Commission intervene in this blurred market segment to strengthen the competitiveness of the European industry and, if so, how?*

Main Findings

Chapter 1 defines the scope of the security and defence sectors, looking at why and how the process of blurring between the two markets has gradually increased over the past two decades.

After the Cold War and the attacks of 9/11 2001, new, transnational threats, such as terrorism and organised crime, largely supplanted conventional military conflict as the major threat to Europe's security. The emergence of such threats blurred the lines dividing internal and external security, and forced a rethinking of European security and defence policies. EU Member States are now developing a new, comprehensive approach which combines both military and non-military actors. As a consequence, defence and security actors have been increasingly involved in a number of missions which are, to a large degree, shared.

Missions can therefore be considered as the first driver for blurring. In order to identify missions in which there is an overlap between the two dimensions, we started by listing military missions and security missions. In these two categories we have identified missions which either require the joint intervention of both military and civilian actors, or require military actors to perform tasks similar to those of civilian security actors:

- "Post Cold War" missions for defence actors (crisis management, support of civil protection).
- "High-end" missions for security actors (crisis management, border control, contrast to terrorism and organised crime, protection of critical infrastructures, etc).

The blurred character of these missions has led to the development of some overlapping capability needs between defence and security actors, because of shared functional requirements - for example, the need for detection, identification and authentication capabilities.

A deeper analysis, however, clearly indicates that the amount of overlapping of equipment used in the "blurred" missions is limited. In both categories actors do need products which perform the same functions (i.e. equipment for situational awareness and communications), but persistent differences in operational requirements limit the amount of products purchased and used by both civilian and military actors. The "blurred" market for equipment appears to be narrower than expected.

However, some common security and defence functional capabilities can be fulfilled through the adoption of new technologies. This is a blurred area with the potential for development. Information gathering and data integration are two extremely significant functions for the “Post 9/11” defence and “High-end” security missions. They signify the need for a large range of technologies, such as sensors and integrated systems. Industries (civilian, security and defence industries, large companies and SMEs) can draw on their markets of origin (defence or civilian) for the technologies and products to be developed in this blurred area.

Chapter 2 is dedicated to technological issues. Based on the typology of missions developed in Chapter 1, we have identified technologies that may contribute to the blurring. We have found a number of **technologies having likely applications across the defence and security fields**, especially in areas such as structural materials/technologies and structural effects analysis, photonic and optical materials and device technology, sensor technology, communication and information technologies, information security technologies and biotechnology.

Technology is a blurring enabler, because many of the assets with cross-cutting application are generic: certain technology investments were originally not made with defence or security mission objectives in mind, being funded and conducted by a variety of private and public sector organisations. This, we argue, is a necessary (but not a sufficient) stimulus for companies to diversify into the security and/or defence markets. In the light of this, we have identified processes and barriers to the transfer of defence-origin technologies to security applications.

Chapter 3 deepens the analysis of the demand-side structure of the markets, comprising security and defence customers and regulators, and identifies the main obstacles and challenges to be addressed in the future**.**

We begin by analysing the structure of demand in the defence and security sectors, attempting in particular to demonstrate the wide variety of actors operating in the security field. The **fragmented nature** of demand in this sector represents a negative force for blurring. Fragmentation acts as a barrier to entry for defence companies seeking to exploit blurring opportunities within the security market.

We have also observed that there is a **structural heterogeneity between defence and security demand:** the analysis of defence and security customers and their purchasing logic (long term planning versus off the shelf acquisition) shows that the demand side has different structures in the defence and security markets, and that this difference **limits the blurring of boundaries**.

A further factor to be considered is the different procurement regulations affecting defence and security actors. Until recently, defence actors tended regularly to circumvent European common market procurement rules for their acquisitions. This had a negative impact on competition at EU level. This has also been the case for security customers, albeit on a smaller scale. New European initiatives and regulations, such as the EC Interpretative Communication on art.296 of December 2006 and the Directive on public procurement in the field of security and defence adopted in 2008, are likely to encourage greater competition in both markets by setting common and clear procurement rules for some security and defence activities, but this will not necessarily have a meaningful impact on the blurred area between the sectors.

As far as budgets are concerned, and as we also comment in Chapter 5, the few existing figures related to the security market show limited growth in the “High-end” sector. This is a further factor reducing the chances for increased blurring between security and defence in future. If this “High-end” security market does not develop in Europe, it cannot then produce synergistic blurring effects for the defence side of the market, as defined in “Post Cold War” missions.

The creation of coordinated European demand through the European Security Research Framework could have a significant impact on the market, but has not yet been followed by any programme for equipment development. This would serve to strengthen demand further.

Standardisation is a further area of consideration for the development of demand in the security sector. A lack of regulation and market standards characterise the market, although in recent years some regulations have been introduced in specific segments, often in response to accidents or attacks. While this lack of norms may favour SMEs operating in local markets, it is also likely to prevent the emergence of transnational markets which allow industry consolidation and enhance competitiveness on an international scale.

Chapter 4 analyses market segments from the supplier perspective. Here, we **observed different reactions to potential blurring.** In general, large system integrator companies coming from the defence sector encounter difficulties in trying to access the "blurred" market segment. They were generally optimistic in evaluating the potential of the security market in the aftermath of 9/11, but have seen no meaningful results. This is why they consider blurring as more of a potential opportunity than a reality. Only firms with dedicated security units and with long-standing experience prove to be relatively successful. This unfulfilled blurring not only has the same impact on SMEs operating as subcontractors to larger companies, but also when they operate autonomously. They too consider blurring as a potential growth market, rather than a present reality.

Those companies who have approached the potential blurred market, have done so by adopting different strategies. Large companies (system integrators) try to influence the demand dynamic by recreating in the security field the same conditions that were favourable to them in the defence sector. Others make use of their defence origin technology, exploiting their technological knowledge in order to offer interoperable solutions to different security customers. Others still, access the market directly through the acquisition of players already operating in the security market, in order to exploit industrial synergies. Despite such attempts, the security market is still at an early development stage, making it difficult to evaluate. This is a potential barrier to any defence company considering the risk of operating in both markets.

Security companies trying to enter the defence market also face many difficulties and barriers to entry. Their knowledge of defence customers and defence procurement rules often remains limited. Lack of knowledge of the defence customer culture (for example, the close relationship with defence organisations), market fragmentation in closed national markets, and the high cost of complying with defence customers' procurement requirements and standards, are all factors that create difficulties for security companies. It is to be noted, though, that security companies seem to be more and more involved in the "High-end" security market, in response to the changing international environment and especially to the introduction of security related regulations made after 9/11.

Technology also has an influence on the potential blurring of the supply side. We have argued that the dynamics of technological development contribute to structural changes in some industrial

sectors (i.e. biometrics). Such a development may help strengthen European industrial competitiveness through the expansion of a dual-use market and the commonalities on the research side. This chapter continues by examining the business conditions for such a technological transfer.

Chapter 5 assesses the **opportunities and challenges** created for industry by the blurring of the dividing line between security and defence. Given the complexity of the blurred area that our research has identified, it seems impossible to draw general conclusions for industry as a whole. Market-specific challenges and opportunities certainly exist on both sides of the dividing line. At the same time, however, challenges and opportunities are also different for each company, determined by its specialisation, experience, size, nationality and know-how.

In general, however, it seems fair to say that there are more realistic opportunities for security and civilian companies in the defence market than for defence companies in the security market. The reason for this is twofold: 1) defence budgets are still considerably higher than security budgets, and 2) defence procurement is increasingly organised in a way which aims explicitly at opening new possibilities for newcomers from non-military markets.

The defence market is currently undergoing an important shift from an equipment-based to a capability-based procurement approach. This shift shatters traditional procurement models and mechanisms and represents an important challenge for established defence suppliers which are used to operate in a relatively stable and predictable business environment. At the same time, these companies face reduced production volumes, which increase in particular the pressure to limit R&D expenditures per unit. This, in turn, fosters the use of civil technologies and components in defence and creates new market opportunities for civil and security suppliers. An emphasis on cost saving, driven by sluggish defence budgets, also helps civil (security) companies enter defence markets, in particular in the service sector.

The security market, and especially the “High-end” segment, is a challenging market characterised by strong fragmentation and little visibility. Fragmentation is to a large degree structurally determined and will therefore persist in many areas and at many levels. As a consequence, systematic capability planning will probably also remain absent for some time. All this means that

the security market is likely to remain a market with strong challenges and uncertain opportunities in particular for defence companies, which face strong competitors in key technology areas such as ITC. At the same time, defence companies will find it difficult to exploit their specific strengths, because demand for technologically sophisticated equipment is limited to certain segments and, even in these segments, production volumes are rather limited.

The complexity and fragmentation of the blurred area between defence and security makes it difficult for a public actor to intervene. **Chapter 6**, though, provides recommendations to the EC on how to maximise opportunities and overcome challenges to strengthen the EU's security and defence industries and provide European stakeholders and citizens with the best array of security tools.

Recommendations

This study has found the extent of blurring between the defence and security sectors to be more limited than expected. We have nonetheless supported the notion that to further this blurring in some areas could strengthen European industry. From the defence industry point of view, a deepened blurring could open new market segments in the security fields, which require technologies that the defence industrial base can already provide (i.e. UAVs and advanced sensors). Moreover, the defence industry could also exploit its capability as system integrator to make available integrated security systems for security missions such as border security or critical infrastructure protection (it is already happening, albeit on a very small scale and mainly in the foreign market). These market opportunities could help the defence industry cope with the sluggish trend of European defence budgets: however, as already said, structural issues in the security market (lack of a structured demand, insufficient degree of standardisation) and the limited size of the demand constrain possibilities for the defence sector.

The security industry could seek to enter the defence market by supplying off-the-shelf products in selected fields (especially in IT, less advanced sensors for force protection, etc.). As the security industry generally operates with cheaper products already available in the market, it could equally benefit from the financial constraints facing defence budgets to gain entry into the market. Our

analysis, however, has demonstrated that the structural differences between the defence and security markets are the main factors influencing the limited development of a blurred defence and security segment. In particular, the heterogeneity and fragmentation of demand in the security sector emerges as a major obstacle to the maturation of the market; moreover, it strongly discourages the entry of defence actors into the market, thereby limiting the convergence between the security and defence sectors.

This is the reason why we have designed a series of recommendations to develop and reinforce the security side of the market. We have considered this issue as a pre-condition to fostering any further blurring between the sectors in terms of governance (better coordination between security and defence players), industry (facilitating access of security and defence players to the blurred market segment), and technology (supporting technological blurring thought research activities).

We have argued that the European Commission should play a pivotal role in the development of the security sector within the European Union. This view has been reinforced by stakeholders interviewed for this study, who stress how technology research projects sponsored by the EU in the security domain will be a critical starting point for nurturing the blurred market segment. Follow-up Commission activity will also be necessary to sustain this opening initiative.

Recommendation 1: The European Commission should establish European Technology Platforms (ETPs) in the security domain in order further to structure the development of mission-oriented technologies. Since a single Technology Platform for security would be too complex to be realisable, we have proposed that these ETPs should focus on the specific missions which have emerged as particularly sensitive within this report, such as Border Security.

Recommendation 2: Having identified that a high level of fragmentation has affected the development and maturation of the security market, we have recommended that the European Commission promotes European standards in the security domain. Common European standards would significantly reduce the fragmentation of the security market, by defining levels of interoperability required between security products. Both large companies and SMEs proved to be particularly supportive of this issue.

Recommendation 3: Additional research programmes should be launched by the Commission through Joint Calls between security and other 7th Framework Programme (henceforth 7th FP) cooperation themes and an expanded 8th FP Security Theme. Health, nanotechnology and new production technologies, socio-economic and humanities appear to be fields where the Commission's efforts could enhance a more comprehensive understanding of security, to be translated into new industrial activity.

Recommendation 4: At the Member State level, we have noted an emerging effort in the development of national threat and risk analysis capabilities. We have suggested that these efforts should be raised to EU level, in order to achieve a common approach to risk analysis. A combined approach such as this could then be at the heart of common security policy-making and common security-related investment decisions. We therefore recommend that the EU develop (within the Commission) its own analysis and planning capabilities. This recommendation would help suppliers focus their production on common requirements, thereby closing the communication gap that we found to exist between suppliers and end-users.

Recommendation 5: In Chapter 3, our analysis has shown that there is a lack of European institutional coordination of security demand. This is a very sensitive policy issue. Therefore, we have recommended that the Commission establish a European Security Congress to launch a process of improvement of governance in the security sector as a whole. This would represent an additional step to the ESRIF approach and would provide industry with a coherent agenda for cooperation and a structure within which to bring together the heterogeneous security end-users within 7th FP activities.

Recommendation 6: Finally, our study has produced converging analyses showing that the European Commission should step into the procurement phase of technology development, shaping the security market not only as a founder of research, but also a buyer. This is why we have recommended that the role of the Commission as a customer should be developed, focusing its

activity on already mentioned blurred missions and fostering the introduction of dual-use equipment. Space systems are a key example of how this process should work (***Recommendation 6.1***).

The above 6 recommendations are dedicated to the consolidation of the security market, which we consider as a key issue in fostering blurring between the defence and security sectors. We have also, however, considered that the Commission should in parallel develop other initiatives to strengthen the link between the defence and the security segments, in particular the following two:

***Recommendation 7*:** For this purpose, we have recommended the institutionalisation of the cooperation process already launched between the research activities of the European Commission and those of the EDA (including ESA for space-related issues). There is already an ongoing framework for coordination between the two institutions, but we have supported the positive effects of this cooperative approach in paving the way for the development of dual-use equipment.

Recommendation 8: Finally, having stressed the importance of efforts towards institutional coordination, we have also support the potential for the Commission to play an active role in the development of defence technologies. This would clearly drive blurring towards the security segment. We are aware this is a sensitive issue and we have therefore recommended a process of reflection on the possible inclusion of defence matters in 8th FP research projects.

Introduction

Context

This is the Final Report on "The industrial implications in Europe of the blurring of dividing lines between security and defence", initiated on 22nd December 2008 by the European Commission, Enterprise and Industry Directorate-General (Aerospace Security Defence and Equipment, H1/D), under Contract No ENTR/08/023, SI2.516182. The Study has been coordinated by the *Istituto Affari Internazionali* (IT) with partners from the Manchester Institute of Innovation Research (UK) and the *Institut des Relations Internationales et Stratégiques* (FR).

This study was launched as a result of the significant role played by the European Commission (EC) in the field of security over recent years. Various initiatives have been launched, the most visible and important being:

- the European Security and Research Programme (ESRP)
- the Security Theme of the 7th Framework Programme
- the European Security Research and Innovation Forum (ESRIF)
- the European Programme for Critical Infrastructure Protection (EPCIP)
- Directives on European Critical Infrastructures for Maritime and Air Transport, and
- the Instrument of Stability for External Security.

In addition, the EC has started to be active in the defence market. In 2008, two directives were adopted as part as the so-called "defence package" and research efforts have begun to be coordinated with the defence community, in particular with the European Defence Agency (EDA).

The EC has identified parallel activities between the security and defence markets and has therefore initiated this study to explore the potential implications. As a result, the EC intends to understand the consequences for industry of the potential overlap between the security and defence sectors and identify possible responses and tools that it could provide at EU level to address future challenges. From this study, the EC expects a review of definitions and concepts currently used in various contexts to describe security and defence areas. This requires an analysis

of the major changes currently being experienced in these sectors, allowing identification of the key drivers for operational, technical, organisational and industrial change. Finally, the EC expects the report to evaluate the technological and industrial consequences and challenges arising from this change, especially for Research & Development (R&D) and industry, and to provide relevant recommendations for use by national and EU stakeholders to best adapt their strategies to the evolving environment.

Concept

The Consortium's working hypothesis is based on the title of the study, which assumes that there has been a division between security and defence in the past. The distinctness of this division has been blurring progressively and, as a consequence, may have had an impact on companies operating in both sectors.

It is true that security and defence have traditionally been dealt with separately as the internal and external aspect of what is called the SECURITY[1] of a state or society. Our thinking, our political institutions, and our political and economic activities have all been deeply influenced by the fundamental distinction between the two. Thus defence was considered as a response to an external threat from a foreign adversary and implied the use of force by military actors; (internal) security, on the other hand, was rather linked to domestic threats such as crime or public order and safety, requiring a moderate use of force but also protection of civil rights and privacy. Different actors were responsible for internal security, such as the police, disaster relief services and law enforcement agencies.

The clear-cut distinction between security and defence has also had important industrial implications. Given their different equipment requirements, security and defence forces have traditionally been supplied by different industries. While public security providers could often use commercially available products that required little or no adaptation, the military relied on a specific defence industrial and technological base capable of delivering sensitive and complex weapon systems. Such companies specialised in two things: the development and manufacturing of bespoke equipment exclusively for a single customer (Ministry of Defence, MoD) and the

[1] Capitalisation is used in the Introduction and the following chapter to distinguish the broader sense of the term "security" from the narrower meaning as, for example, in "security and defence sectors".

management of long-term processes, rather than the development of rapid responses to a market with short-term changes.

However, since the end of the Cold War and even more since 9/11, the distinction between the concepts of security and defence described above has been progressively blurring. The reasons are generally well known and are very much linked to the rise of new threats of a trans-national and trans-border nature, such as international organised crime or terrorism. This has led actors traditionally responsible for "internal" security, like police forces, to intervene outside their national territory and participate in missions which were traditionally under the responsibility of the armed forces, jointly or in cooperation with them. For the same reasons, armed forces have started to become involved in the internal security of the national territory, alongside security forces. However, security and defence actors also continue to maintain their traditional responsibilities with, for example, Ministries of Defence and Ministries of the Interior having differing portfolios requiring sometimes difficult cooperation.

There is therefore a clear overlap between the security and defence sectors, but its specific nature and extent remains unclear. Thus we have decided not to accept the assertion of the title of the study without question, but to start with a critical analysis of the concept of blurring before turning to the impact it may have on industry.

Objectives

Accordingly, the starting point of the study has been to define the area of blurring between security and defence, and in particular its scope, its nature and importance and potential evolution. Based on these findings, we have analysed the impact of this overlap on the market structure (customers and suppliers). Finally, we have assessed whether this blurring could present opportunities or challenges in the future for companies involved in the security and defence sectors.

In doing so, the research team has worked on five questions that have shaped the analysis presented in the following chapters:

To what extent are the dividing lines between security and defence blurring?

This question addresses the underlying assertion of the study. Our answer defines the scope of the defence and security sectors separately, assesses whether the boundaries between the two have blurred and determines its extent.

Which market segments are particularly affected by the blurring?

In answer to this question, we assess the demand characteristics of the defence and security sectors (structure and behaviour of customers and regulators), supply specificities (size, trends and dynamics) and the technological environment. The result is an analysis of which market segments and technologies are at the heart of the blurring effect between the sectors.

What are the drivers and barriers to blurring?

Based on the previous analyses, we identify the market forces that favour blurring and the obstacles that hinder it. The identification of these factors has allowed us to do two things; first, analyse their implications on the business strategy of companies involved in these markets and second, define possible European policy measures.

Is blurring a positive or negative factor for the industry?

The analysis carried out throughout the report allows us to identify a set of opportunities and challenges for industry that emerge from the potential for blurring between the defence and security sectors. Moreover, starting from the assumption that there are limits to the effects of blurring which are likely to remain, we try to assess which challenges can be turned into opportunities, possibly by public intervention, and which conditions will require industry to adapt its strategy to succeed in the blurred segment.

Should the Commission intervene in this blurred market segment to strengthen the competitiveness of the European industry and, if so, how?

There are three aspects to this question:

- Is the blurring between defence and security a phenomenon which creates opportunities and/or challenges for European companies?
- If so, are these opportunities so important that the Commission should intervene in order to promote certain trends and/or overcome specific problems?
- If so, how should the Commission intervene and on which trends and which problems?

Concrete recommendations on these three issues are provided in this report.

The questions have been addressed in the Final Report, according to the following structure:

Chapter 1 defines the scope of the security and defence sectors, looking at how and why the gradual process of blurring between the two markets has evolved over the past two decades. We classify and analyse security and defence missions and highlight the growing commonalities between some of them. This allows us to identify the potential for blurring in certain market segments and technologies. We will adopt such "mission oriented" approach also in subsequent chapters.

Chapter 2 is dedicated to technological issues. Based on the typology of missions developed in Chapter 1, we identify technologies that may contribute to the blurring. Particularly, we discuss the processes (and barriers) to the transfer of defence-origin technologies to security applications and vice versa, and identify conditions that are critical for a successful technology transfer.

Chapter 3 deepens the analysis of the demand-side structure of these markets (security and defence customers and regulators) and identifies the main obstacles and challenges to be addressed in the future**.**

Chapter 4 analyses the market segments from the supplier perspective. An overview of the structure of the defence and security supply chain is described in the first section of the chapter. We then examine the different approaches of defence and security players, thereby highlighting the challenges that each group of companies might face in the future.

Chapter 5 assesses the **opportunities and challenges** that the blurring of the dividing line between security and defence creates for industry. Given the complexity of the blurred area, it seems impossible to draw general conclusions for industry as a whole. Market-specific challenges and opportunities exist on both sides of the dividing line and, at the same time, challenges and opportunities are different for each company, according to its specialisation, experience, size, nationality and know-how.

Finally, **Chapter 6** provides recommendations to the EC on how to maximise opportunities and overcome challenges to strengthen the EU security and defence industry and provide European stakeholders and citizens with the best array of security tools.

In addition, **Annex 1** provides the list of all the stakeholders interviewed during the research work. **Annex 2** offers a list of the main defence and security customers involved in blurred missions. **Annex 3** analyses the implications of the Lisbon Treaty for security and defence. **Annex 4** is a summarising table for the membership of three security industrial initiatives. **Annex 5** comprises a series of country studies of the 4 countries participating in the study (France, Germany, Italy and the United Kingdom). Finally, **Annex 6** presents a brief review of the US approach to the blurring.

Methodology

The findings that have emerged from this study are based on a two-phased approach. First, a review of the available literature on these issues has been undertaken, sourced from relevant European institutions and from the four Member States whose defence and security sectors have been examined in detail.

Second, detailed interviews with relevant stakeholders have been conducted. The study is limited to the relevant European institutions and the four EU Member States which are the main security and defence players in terms of public spending and industrial capabilities (France, Germany, Italy and the United Kingdom). The study does not include a comparative analysis between Europe and the US, since the US market situation is completely different. However, a brief review of the most important developments of the US approach to the blurring lines between security and defence is

included as an annex. It proceeds along the same lines as the overall report, and comments on missions, technology, demand, and supply in the United States.

This approach has allowed us to gather and sort information, formulate hypotheses and then test them in the marketplace. The analysis and interpretation of our results remain the responsibility of the research team. Two points should, however, be noted. First, reliable, precise data are difficult to source in the defence and security sectors, particularly in the highly fragmented security sector. Second, there is an (understandable) reluctance on the part of industry insiders to disclose potentially sensitive information.

Analysis of existing literature and official documents

The first methodological elements of our study are a comprehensive analysis of the existing literature (primarily, but not solely academic) on the issue, and a thorough investigation of the conceptual developments emerging from official documents both at the EU and at the Member State levels. Among these materials, we highlight the particular relevance of:

- White Papers since 1990 (see country studies, Annex 5)
- Key documents on industrial policy since the 1990s (see country studies, Annex 5).
- EC Directives, studies, regulations on security and industry since 1990 (EC) (see analysis of the EC Defence package, Chapter 3).
- Analysis of which new institutions or changes have occurred with regard to military-civil relations within Member States and at the EU level (see Lisbon Treaty analysis, Annex 3).

A further essential source of data was the analysis of European company (both large corporations and small and medium enterprises, SMEs) budgets and strategic documents. These have given real insight into the conditions of the sectors we are reviewing.

This first phase of our analysis therefore provided a conceptual definition of security and defence;

an appraisal of the relevant connections between the two sectors; a theoretical understanding of the EU and Member States' policies related to security and defence; an initial mapping of the industry and technologies available in the two sectors.

Stakeholder engagement plan

The findings from phase one of the study were used to shape phase two: the stakeholder engagement plan. Our research team scheduled interviews and meetings with a wide European network of security and defence stakeholders (the list is detailed in Annex 1), coming from joint work with think tanks, institutions and companies. Our objective for these interviews was to test our initial theoretical assessments and evaluations.

This dialogue-based approach with a network of security and defence stakeholders enabled our team not only to gather new data, but also to explore potential future scenarios and challenges for the sectors. We were able to draw out general truths about the current state of the markets in Europe and clearly map different Member State practice and strategy.

A single research questionnaire was designed by the team (a questionnaire/guidelines), but application of the questionnaire was customised by each interviewer, as in previous studies we have experienced the reluctance of some communities to engage in formulaic data gathering. Responses have been used in the text of our report to illustrate arguments, but have also been summarised into explanatory tables to highlight a number of the report's key messages.

This work has been made possible thanks to the extended network of security and defence stakeholders developed in recent years by the team's partners. We have been able to maintain a constant dialogue with the different communities (institutional, industrial, operational and academic) involved, allowing us to validate our conclusions.

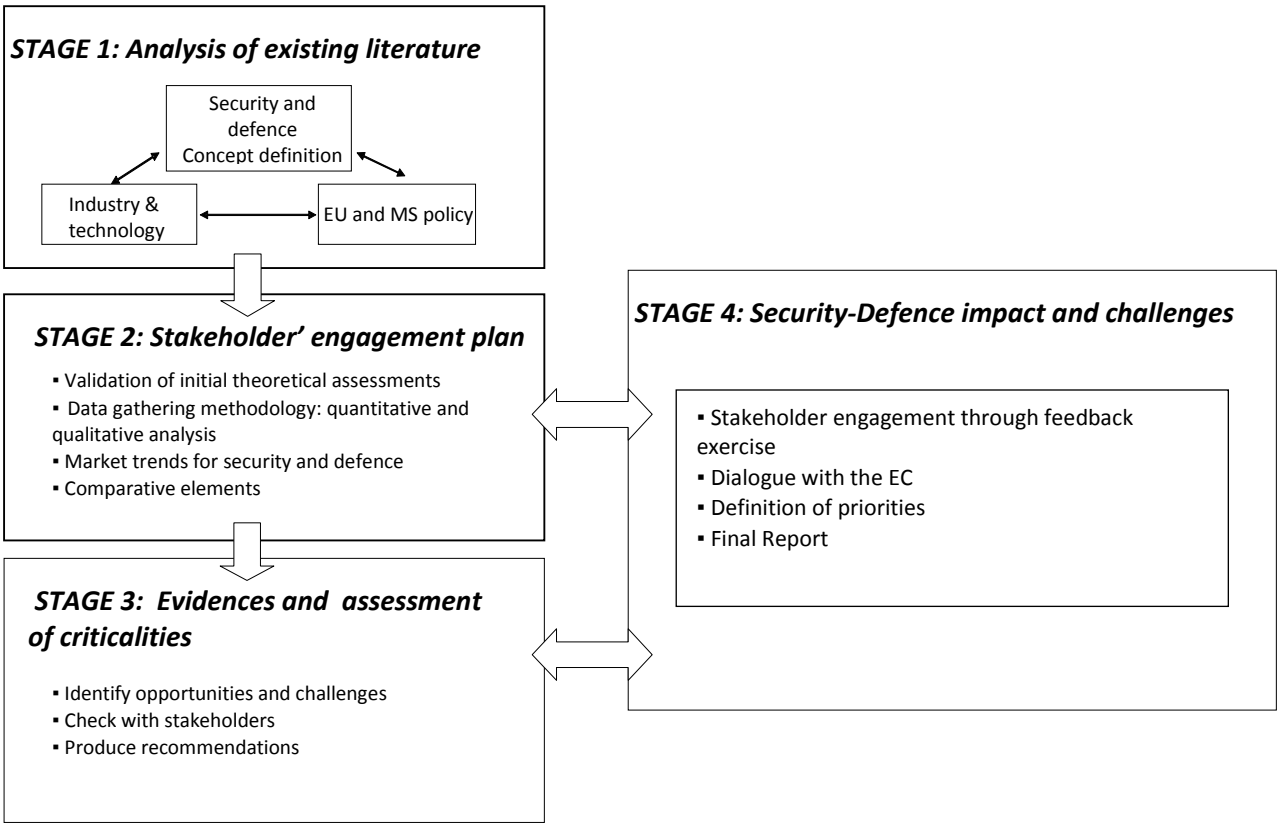
Limitations and concerns

In gathering quantitative data, we have experienced numerous practical challenges. The research methodology we have employed recognises that there are limitations in the quantitative data publicly available in the sectors we are studying, particularly in the security sector which is highly fragmented. Any study at the European level will therefore have to rely heavily on expert analysts with deep knowledge of the sector and the willingness of industry and stakeholders to share information.

Our initial effort was focused on building a taxonomy of blurred missions between the security and defence sectors. Our aim was to identify where and how demand may arise in the blurred segment between the sectors. As has been confirmed by other studies, however, we found that it is impossible precisely to quantify the size of the security sector, as market definitions vary among security suppliers and data is very rarely verifiable. A data gathering effort of this magnitude is beyond the scope of this study, which aims to understand the impact of a phenomenon and not to perform a quantitative analysis (as stated in our proposal)[2]. Moreover, it would necessitate a considerably larger research team, dedicated to a full-time effort on data gathering. It would be worthwhile launching a dedicated study on data gathering in the sector, as this may help its development.

[2] Page 9 of the proposal: "*As far as quantitative element is concerned, there are numerous practical challenges to collecting information at the European level. This methodology* ***recognises that the limitations on the hard quantitative data publicly available*** *at the European level means that any study at the European level will have to rely heavily on experts analysts with deep knowledge of the sector and the willingness of industry and stakeholders to share information"*.

Synthesis of the methodological approach



1. The blurring of missions between security and defence

This chapter opens with a definition of the scope of the security and defence sectors, based on a review of the existing literature. Second, it analyses the process of blurring between the two sectors. It shows in particular the reasons why the blurring has occurred and identifies whether the overlap is to be considered limited or, on the contrary, significant. Finally, the analysis focuses on the identification of those missions and functions where the division of responsibility between security and defence players appears less clear than in the past. We consider that starting from missions and tasks is particularly important since they have a major impact on demand (responsibility and interaction between security and defence customers) and supply side organisations (strategy and structure of security and defence companies), issues which will be addressed in the course of the report.

1.1. Traditional scope of the security and defence sectors in Europe

In the broadest possible sense SECURITY is the condition of being secure, i.e. of being free from care, apprehension or anxiety.[3] Semantically, SECURITY has three components: a subject (who or what could become anxious), a perceived object (what is regarded as a danger), and a provider (who is thwarting the danger and providing or generating SECURITY)[4]. The condition of being secure can be endangered as a result of an unintended disaster, or by (malignant) intended human action.

If SECURITY is endangered as a result of a disaster or an accident, we use the terminology "safety".[5] Safety is concerned with all dangers that arise as a result of unintentional events (natural disasters such as flooding) or of unintended consequences of human action (manmade disaster). Manmade disasters can result from an operational failure of technical systems, as in the case of the Chernobyl accident, but can also be totally unintended as in the case of pandemics such as swine

[3] OED, Oxford English Dictionary, www.oed.com
[4] Andreas Osiander, *Begriffsgeschichte: Sicherheit, Frieden Und Krieg*, in *AMI*, Vol. 5, No. 13-35, 1998.
[5] Thee European Security Research and Innovation Forum (ESRIF) Final Report speaks of "civil security", see ESRIF, *European Security Research and Innovation in Support of European Security Policies. Final Report*, Brussels, 2009. Available at: http://www.esrif.eu/documents/esrif_final_report.pdf

flu spread by tourists.[6] Our societies have developed numerous strategies to deal with such threats: we counter them through fail-safe procedures; prevention and mitigation; crisis and consequence management; business continuity planning; built-in resiliency and redundancy; reconstruction and recovery plans. Specific institutions are entrusted with preventing and reacting to such security threats, ranging from fire fighters and disaster relief organisations, such as the Red Cross, to civil protection forces. The private sector provides safety also through designing, constructing and adapting its operational procedures and systems with due consideration of possible failures (and attacks). Private business, such as the pharmaceutical industry (for vaccines) or the logistical service sector (for transportation and evacuation measures), can also play an active safety role.

If SECURITY is endangered as a result of intentional human action, then European States have traditionally distinguished between security and defence[7], depending respectively on where the threat was perceived to originate: inside the territory of the state (i.e. crime, disturbance of public order) or outside (i.e. conventional armed conflicts, nuclear attacks or other unconventional attacks by other states). Internal security is synonymous with "non-military (civil) security", while external "military security" is associated with external SECURITY. The territorial border of the country provides the basis for the dividing line between them.[8] This division is deeply ingrained in the public thinking and is characterised by a multitude of factors:

- Importance: given the threat of nuclear annihilation or large-scale conventional attacks during the Cold War, much more attention and resources have been devoted to defence over security. Defence budgets have priority in the conscience of governments and public opinion, and are higher than security budgets.
- Institutions: different institutions are responsible for the two areas and they are mainly

[6] There is of course the possibility that i.e. a virus is used as a weapon in order to infect a particular population and to weaken a state or disrupt communications and trade. This case would be the subject of security and defence rather than safety.

[7] Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner, London, 1998.

[8] See, for example Barry Buzan and Ole Waever, *Regions and Powers: The Structure of International Security*, Cambridge, Cambridge University Press, 2003. European Commission, *Security Research: The Next Steps*, Brussels, 2004. Stephan Böckenförde, *Die Veränderung Des Sicherheitsverständnisses*, Opladen & Farmington Hills, Verlag Babara Budrich, 2009. The concept of territorial defence can also help specify those boundaries, with a specific role for the protection and resilience of military organisations in case of nuclear or conventional attack.

public actors (police and law enforcement authorities vs. military) with limited reasons for interaction.

- Tasks and missions: “internal security” forces are generally involved in investigation, protection and prosecution activities, while the focus of military actors is almost exclusively on deterrence, defence and attack assignments.
- Rules which guide activities and regulate authority and responsibility: national law applies to police and law enforcement organisations. In contrast, military forces are subject both to *ad hoc* military codes and international law.
- Equipment: while police forces generally rely upon commercially available or technologically limited equipment, armed forces are equipped with sophisticated weaponry of the highest technological standards, competing for supremacy in warfare technologies.

The divide, illustrated above, touches not only the political, but also the industrial and scientific realms. Industry has traditionally played an important role in the provision of security as a supplier of equipment to public security and defence providers. Private companies develop, manufacture and support the equipment and systems that are procured and used by police forces, fire fighters and disaster relief organisations, as much as by military services. However, the companies that operate in the two sectors have always been rather different because of the nature of their respective markets. The defence industry has been characterised by the production of large, high tech platforms, specialising in the development and manufacture of equipment specified exclusively by single institutional customers (MoDs). This type of specialised production has been considered as a “strategic asset” by several countries. Security firms, on the other hand, have remained smaller and less specialised in *ad hoc* developed high tech products, operating mainly in the free market and responding to its short term changes (as will be detailed in Chapter 4).

1.2. The process of blurring between security and defence: the rise of new risks

In order to identify how and to what extent the division between security and defence has started

to blur, it is useful to explore the evolution of the strategic scenario since the end of the Cold War and its implications on the convergence between these traditionally separated areas. As identified in the EU Security Strategy[9], new key risks have emerged as a consequence of the economic, political and technological evolution in Europe and worldwide, driven in particular by the effects of globalisation:

- The increased interdependence of countries, due to greater exchange of goods, persons, capital and information, has made the tight control of borders extremely difficult, given the immense volumes and enormous complexity of movements and interactions.[10] These effects on national borders have been particularly pronounced in Europe, as interdependence among formerly independent states has increased significantly due to processes of European economic and political integration. Globalisation has created further interdependencies and relies on the openness of trade routes, so that risks such as viruses and conflicts in far away regions quickly have repercussions in European countries. As a result, territorial borders have become much more porous and their control presents a bigger challenge for security policy.

- New technologies, such as the spreading use of the internet and mobile communications, have introduced changes in business and social practices, but also offered new tools for the use of non–state violent actors. Communication networks have become central to the functioning of society, creating new vulnerabilities such as piracy or new forms of espionage and sabotage, for which the territorial border is irrelevant.[11]

The various and heterogeneous effects of both globalisation and technological developments have

[9] Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*, Brussels, 2003. Available at: . http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[10] Bundesministerium der Verteidigung, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, Berlin, 2006. http://merln.ndu.edu/whitepapers/Germany_White_Paper_2006summary.pdf.

[11] Stephan Böckenförde, *Sicherheitspolitischer Paradigmenwechsel Von Verteidigung Zu Schutz*, in Europäische Sicherheit, Vol. 8, 2007.

maximised the opportunities for non-state actors to pose threats to states. Non-state actors can now move more easily across borders, use new technologies to do harm (cyber warfare, non-kinetic weapons), organise themselves (through the internet, encrypted mobile phones), or even acquire knowledge on how to manufacture weapons (especially explosives and potentially CBRNE devices). These developments require control of the entire territory, rather than only at certain border entry and exit points, thereby increasing the need to ensure security rather than traditional defence**.** In fact, in this changing global context, traditional military risks, like large scale aggression against EU Member States, have become improbable. Instead, according to the 2003 European Security Strategy[12], new risks of a non-military nature, and so-called "asymmetric" risks have become predominant:[13]

- **Terrorism** imposes a growing strategic risk to Europe, global in its scope, arising out of complex causes of very diverse nature (political, societal, religious, etc.).
- **Proliferation of weapons of mass destruction** is identified as potentially the greatest risk to European security.
- **Regional conflicts** that destroy human lives and social and physical infrastructure, threaten minorities, fundamental freedom and human rights, leading to extremism, terrorism and state failure.
- **State failure**, as a result of bad governance, corruption, abuse of power, weak institutions and civil conflict, with significant repercussions at regional level (and potentially even global).
- **Organised crime,** an internal threat to Europe with also an external dimension, cross-border trafficking in drugs, illegal migrants and weapons, often associated with weak and failing states.

[12] *A Secure Europe in a Better World. European Security Strategy*, 2003.

[13] Adapting to the European Union case the "Operational definition of asymmetric threat" provided by C.A. Primmerman, an "asymmetric threat" must involve a weapon, tactic, or strategy that a State or non-State enemy both could and would use against an EU Member State. Characteristics of this weapon, tactic or strategy are: the EU Member States would not employ it; they would not combat it by retaliating in kind and, therefore, could not deter by threatening to retaliate in kind; it is not already countered by systems designed to deal with symmetric threats and, therefore, if not countered, could have serious consequences. C.A. Primmerman, *Thoughts on the Meaning of "Asymmetric Threats*", Massachusetts Institute of Technology, Lincoln Laboratory, 2006.

In particular, since the terrorist attack of 11th September 2001, it has become clear that these new threats can be as serious as military threats and constitute a challenge even to the essential security interests of states. The fact that Article V of the North Atlantic Treaty was invoked for the first and only time following 9/11 illustrates that non-military security threats have reached an unprecedented dimension and can attain almost the same severity as military risks.

Moreover, these new risks are transnational, diverse, less visible and less predictable than conventional ones. They are not classified anymore according to the location in which they arise - inside or outside the borders of a state. Any management of these non-military security threats therefore requires a variety of responses, the use of a combination of military and civilian means and the involvement of numerous actors, public and private, military and civilian. As a result, the distinction between "internal" and "external", civil and military security is increasingly losing its significance in SECURITY policy. This erosion of traditional barriers is explicitly acknowledged in the European Security and Defence Policy (ESDP – now the CSDP since the entry into force of the Lisbon Treaty), which remains limited to the external dimension of security, but combines civil and military perspectives. Civil security actors play an increasingly important part in "external security" missions abroad. Defence actors, although still performing a number of traditional tasks (protection of the territory against military attacks), are increasingly requested to perform, or at least support, non-military tasks inside (support to civil protection[14]) and outside the national territory (reconstruction, peace-keeping). There is a clear evolution in the use of military organisations. The so called "comprehensive approach" paradigm[15] advocates the combination of military and non-military tasks as a key element in the success of crisis management and stability operations.

[14] Italy and France have a long tradition in this area, in particular thanks to the role of Military Police forces, while the German legal framework is less permissive in respect of the use of military forces in the homeland.

[15] According to U.S. military doctrine, "a comprehensive approach is an approach that integrates the tool of statecraft with military forces, international partners, humanitarian organization, and the private sector to achieve unity of effort towards a shared goal" Field Manual 3-07, *Stability Operations.* U.S. Department of the Army, October 2008, pp. 1-4 and 1-5. Available at: http://usacac.army.mil/cac2/repository/FM307/FM3-07.pdf Also the UK's Ministry of Defence stressed the importance of a comprehensive approach under which: "the realisation of national strategic objectives inevitably relies on a combination of diplomatic, military and economic instruments of power, together with an independent package of developmental and humanitarian activity and a customised, agile and sensitive influence and information effort". The comprehensive approach, Joint Discussion Note 4/05, Joint Doctrine & Concepts Centre, Ministry of Defence, January 2006. The necessity of a comprehensive approach is today largely shared also at the NATO level: http://www.nato.int/cps/en/natolive/topics_51633.htm

The transnational nature of such risks also brings a growing involvement of supra-national institutions, in particular the European Union, as potential providers of solutions. In fact, non-military solutions to security risks are considered more and more as a public good, not only by governments but also by the European Union. In that sense, a clear example is the Schengen border control agreements and the consequent necessary exchange of information on international terrorist cells. In order to respond to the new security demand coming from Member States and European citizens, the European Union is therefore developing a new paradigm of security, the "security of the citizen" (see in particular the ESRIF Final Report and the EU Security Strategy)[16], where the security needs of the person are central, along with, for example, border and infrastructure security.

1.3. The blurring of missions between security and defence

This paragraph discusses in further detail the security and defence sectors' response to the new strategic environment, underlining the emerging commonalities of missions. In order to do so, we have developed a classification of defence missions and security missions based on the existing European documents (European Security Strategy, EDA Long Term Vision, ESRAB report, STACCATO report)[17], national strategic documents (national security and defence strategies) and information provided by stakeholders during interviews. Based on this classification, we then identify which defence and security missions and functions are blurred, and to what extent.

[16] ESRIF, *European Security Research and Innovation in Support of European Security Policies. Final Report*, Brussels, 2009, and Javier Solana, *A secure Europe in a better world: European Union Security Strategy*, 2003, http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

[17] EDA Long Term Vision Available at: http://www.eda.europa.eu/webutils/downloadfile.aspx?fileid=105; European Security Research Advisory Board (ESRAB), *Meeting the challenge: the European Security Research Agenda*, 2006, available at: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf; Staccato research group, STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities, 2008, available at: http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf

1.3.1. A taxonomy of current defence and security missions

In order to identify the area of blurring (overlap) we have started by drawing a list of the various missions of military actors (Army, Navy, Air Forces, Gendarmerie-like forces) and civilian security actors (police forces, civilian intelligence, fire brigades, etc.).

Based on a comprehensive analysis of the national strategic documents[18] of the four countries reviewed for this report, we have been able to identify the following as the main missions of the armed forces today:

- Traditional defence of the territory and deterrence.[19]
- Crisis management operations (mostly within ESDP and/or NATO frameworks).
- Support to civil protection as an auxiliary mission.

While obviously traditional defence tasks remain the sole responsibility of armed forces, crisis management abroad and supporting civil protection measures are missions in which both military and non-military security actors are involved. In these two categories of missions, therefore, we can hypothesise a tendency for blurring. We have defined these two categories as "Post Cold War" defence missions, as their relevance has seemed to increase since the end of the Cold War.

The identification of security missions is more difficult, as the number of risks to be addressed and the institutional players involved are more complex. Over the past 5 years, many studies and

[18] For a detailed description of these documents see Annex 4. See also Italy's Ministry of Defence, *Libro Bianco*, 2002. Available at: http://www.difesa.it/Approfondimenti/ArchivioApprofondimenti/Libro+Bianco, France's *Défense et Sécurité Nationale, Livre Blanc 2008*: http://lesrapports.ladocumentationfrancaise.fr/BRP/084000341/0000.pdf, or Germany's *White Paper on German Security Policy and the Future of the Bundeswehr*, 2006: http://www.bmvg.de/portal/PA_1_0_LT/PortalFiles/C1256EF40036B05B/W26UWAMT995INFODE/W+2006+eng+DS.pdf?ywrepository=youatweb

[19] According to a general interpretation, territorial defence is an exercise of the right of self-defence, and consists of the protection of sovereignty in the territorial land and territorial sea against imminent threats and violations perpetrated by third countries' armed forces. It includes the protection of people's lives and properties in the national territory, which is the area to which the State's sovereignty extends. For most EU countries, territorial defence is their responsibility under Art.5 of the NATO Treaty, regarding collective defence.

working groups have discussed the issue and published proposals to categorise the missions and functions falling within the security sector.

The ESRAB report and the STACCATO report[20] are among the main contributors to this debate, and have thus been taken as our point of reference, blending them in order to cover the whole spectrum of potential blurring between security and defence. The STACCATO taxonomy includes both defence and security missions, as it has been developed according to a common categorisation of capabilities and technology. The ESRAB process, which focuses only on the security dimension, derives capabilities and technology from a mission and function driven approach.

The ESRAB report's typology does not include the traditional security missions/tasks involved in internal security: protection against ordinary criminality (law enforcement) and disturbance of public order, mostly having police forces as players. It also does not refer to security provided by the private sector for the private sector, for the purposes of business protection (except where risk to critical infrastructure is concerned). The degree of blurring experienced at that level is so limited as to be irrelevant, with some exceptions like Italy, where the Army has been employed in seven major operations in support of security forces since 1992.

Hence, as far as security is concerned, and according to the ESRAB report, security missions can be clustered into four categories:

- Protection against terrorism and organised crime
- Border security
- Critical infrastructure protection
- Restoration of security in case of crisis.

[20] ESRAB, *Meeting the challenge: the European Security Research Agenda*, 2006, and Staccato research group, STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities (STACCATO), 2008.

The four categories of missions of the ESRAB report correspond to new or redesigned needs in response to the post Cold War and post 9/11 agenda, as the threat of large-scale military aggression has been substituted by these new risks, described as "multifaceted, interrelated, complex and increasingly transnational in their impact".[21] The paradigm of this "High-end" security has also contributed to an expanded "security" agenda, where all elements of society are considered as potential targets for attack. As a result, "security" has become a rather holistic category or an umbrella term, under which many types of activities can be grouped. In effect, this represents a wide area in which both defence and security players need to cooperate and where we can therefore identify a potential for blurring.

To sum up all of the above, we can identify four categories of defence and security missions, according to their sensitivity:

- **"High-end" defence** missions include traditional missions of the armed forces, such as deterrence and territorial defence in case of an attack. Though they are less likely in the current environment, they remain key missions of the military.
- **"Post Cold War" defence** missions include missions which armed forces (Army, Navy, Air Forces) have always performed, but which have become increasingly complex in the post Cold War environment, requiring the participation of security forces. An example would be ESDP tasks, including crisis management operations abroad. These missions often require a demanding range of functions and capabilities that can be delivered by cooperation between military and security players. Support to civil protection is also a task performed by military actors.[22]
- **"High-end" security** or "Post 9/11" security missions, which became increasingly relevant after the terrorist attacks of 9/11, are performed by security and defence forces. They include protection against terrorism, organised crime and other aspects of internal security provided by public institutions for civil society, such as border security (including maritime security), critical infrastructure protection and civil protection.

[21] ESRAB, *Meeting the challenge: the European Security Research Agenda*, September 2006, p. 14.
[22] With some exceptions, i.e. Germany, where the separation between military and civilian actors is stricter.

- **“Low-end” security** refers to the traditional police and law enforcement missions/tasks, provided by the private sector for the private sector for the purposes of business protection (physical security protection, including CCTV and surveillance, intrusion and fire detection, access control, data and information protection) with the exclusion of critical infrastructure protection.

Table 1 summarises the views of the stakeholders listed in Annex 1 regarding their perception of the existence of a blurring for these missions. Based on the findings from Table 1, we can observe that blurring is considered as a potentiality for most of the “Post Cold War” and “High-end” security missions. Crisis management missions are often considered by analysts as having a blurred character, since they require the participation of both civilian and military actors. Nevertheless, stakeholders clearly indicate that blurring is happening only at certain levels, for example, at the conceptual level. At the operational level, blurring remains limited, as will be demonstrated in the following paragraphs.

Table 1: Opinions about the blurring between security and defence for missions.[23]

Mission	Opinion
TERRITORIAL DEFENCE	UNLIKELY TO HAPPEN
CRISIS MANAGEMENT	REALITY: Blurring at the theoretical level and in terms of functions. Still very limited on the operational side, with some exceptions (NATO /EU operations Afghanistan).
SUPPORT TO CIVIL PROTECTION	POSSIBILITY: Blurring more potential than real, with defence and security actors operating side-by-side but with separated operational tasks.
PROTECTION AGAINST TERRORISM AND ORGANISED CRIME	POSSIBILITY: These remain security tasks under the responsibility of civilian police forces. One-off military support cannot be considered the proof of an already effective blurring.
BORDER SECURITY	POSSIBILITY: It is commonly considered an area in which defence and security could converge towards a consistent blurring. These convergences have to be proved at the operational level.
CRITICAL INFRASTRUCTURE PROTECTION	POSSIBILITY: It is already an area where defence actors and security operators share a combined responsibility. It currently remains more cooperation than blurring between the two sectors.
CIVIL PROTECTION	POSSIBILITY: Blurring more potential than real, with defence and security actors operating side-by-side but with separated operational tasks.
LAW ENFORCEMENT	UNLIKELY TO HAPPEN
PRIVATE SECTOR SECURITY	UNLIKELY TO HAPPEN

Three categories are considered: REALITY, POSSIBILITY, UNLIKELY TO HAPPEN.

[23] Drawn from interviews. See list in Annex 1.

1.3.2. Blurring trends within defence missions

We will now analyse in greater depth the degree of blurring that actually occurs in the two categories of defence missions identified as blurred, crisis management and support to civil protection (the "Post Cold War" defence mission category). We attempt to distinguish between what is expressed at conceptual level concerning the blurring and what is in reality happening on the ground, in order to identify the importance and the nature of the overlap between security and defence.

1.3.2.1. Crisis management

Crisis management is a generic concept covering a broad spectrum of operations with very different levels of military engagement.[24] The use of force required in ESDP crisis management operations appears to be limited. The spearhead of EU military crisis management, EU Battlegroups, is designed for scenarios such as the delivery of humanitarian aid, evacuation operations, conflict prevention, stabilisation operations and the separation of hostile parties by force.[25] Only the latter scenario deals imminently with the threat of non-occasional physical violence. Indeed, it has been argued that the EU approach, based on a holistic and comprehensive involvement of civilian and military elements performing intermingled, mixed duties, is leading to the emergence of a specific EU military ethos. Such ethos is characterised by a focus on typical civilian skills and an inclination towards less intensive forms of military enforcement: "an EU soldier is not supposed to fight, but to manage a variety of complex situations as part of a larger multinational, civil-military machinery".[26]

Even in high-intensity operations, such as Afghanistan, however, military forces, non-military security providers and civilians often cooperate closely**.** National experiences and multinational operations in crisis management over the past 10 years are largely pointing to the issue now falling under the term "comprehensive approach", meaning the need to integrate military and

[24] In a broad sense, the concept of crisis management includes also the ability of security forces to restoer the situation after the stabilization of the crisis.
[25] See G. Lindstrom, *Enter the EU Battlegroups*, EU ISS Chaillot Paper no. 97, February 2007, pg. 18.
[26] Tommy Koivula, *From Warrior to Manager: EU crisis management as a force for change in the European militaries*, paper presented at the Isa Annual Convention, 15 February 2009.

civilian efforts into a coherent strategy. Even NATO, arguably the most effective purely defence organisation, is embracing "a comprehensive approach that promotes cooperation and coordination between international organizations, individual agencies and NGOs, as well as with the host government".[27] As is the EU, NATO is increasingly involved in "crisis response operations", which include peacekeeping and peace enforcement, as well as conflict prevention, peacemaking, peace building and humanitarian operations. The NATO ISAF mission in Afghanistan is actively involved in reconstruction and development efforts through the Provincial Reconstruction Teams (PRTs), formed by both civilian and military personnel to support the activities of Afghan, international and NGO actors in the field. Moreover, PRTs can also be involved upon request in humanitarian relief activities, distributing medication, food and winter supplies. ISAF also cooperates with local security forces on counter-narcotics efforts, on disarmament, and on the training of Afghan National Police forces.

If we limit our analysis to the conceptual level, utilising official concepts and functions, it would be natural to conclude that crisis management missions have become a shared responsibility between security and defence actors. A closer look at the way crisis management missions are conducted abroad, however, shows that the degree of blurring, while considerable at the conceptual level, may in fact be more limited in real operations.

The EU experience in crisis management missions illustrates the difference that we have found between the theory of blurring missions in crisis management and the reality on the ground. The development of Petersberg tasks under the ESDP (humanitarian and rescue tasks, peacekeeping and combat forces in crisis management) which are less "military-oriented" than the NATO missions, have somehow influenced the general idea that there is a blurring of tasks at EU level, a sort of joint "civilian-military" approach. If we look at the military scenarios[28] and civilian scenarios[29] developed by the Council, there could be a theoretical blurring. When looking at the way the missions are de facto conducted, however, the dividing line between military and civilian

[27] As in the speech of NATO Deputy Secretary General Claudio Bisognero at GLOSEC Conference, 2008. Available at: http://www.nato.int/docu/speech/2008/s080117a.html.

[28] These include conflict prevention, separation of parties by force, stabilisation, reconstruction, evacuation operation, and assistance to humanitarian operations.

[29] These include police, rule of law, civil administration, civil protection, monitoring and support to the EU special representative.

roles in these missions clearly persists at all levels, with only limited exceptions: long-term planning (civilian and military headline goals), short term planning (deployment), competences, tasks, objectives, conduct of operations, budgets and equipment used.

The 22 ESDP military and civilian operations undertaken so far have not been conducted jointly. The military and civilian operations were either conducted successively or in parallel and in few cases have they been coordinated. The same is true for the equipment used. Usually, there is first a stabilisation phase with military means, then a reconstruction phase, which is civilian in nature and may require the support and participation of military forces. Stakeholders involved in the 6 EU military operations[30] indicate that they do not usually need much "civilian" equipment[31]. Even if the operations do not require the use of force, "classic" military equipment is deployed by the participating Member States under their own budget. The so-called "organic means" remain military (uniforms, arms, vehicles) as well as the personnel, while all the remaining needs for the operation come from the civilian market.[32] .

The same is true for civilian operations, which are more numerous, around 20 so far, but of a smaller scale than the military ones. In all cases, the equipment used was primarily civilian, provided mainly by private civilian companies: armoured vehicles up to B6/APC (therefore non-military but civilian with a limited protection), 4x4 vehicles, minibuses, IT/PC, printers, communication assets and VHS radios, cell phones, office equipment, fuel, generators, GPS, security equipment such as video cameras, ballistic flack jackets, helmets, detectors, stocks of water and various services such as security guards and audit.

In the light of the above examples, we could conclude that in the majority of cases there is no blurring in EU crisis management missions, either concerning the responsibilities of security and defence players on the ground or the equipment used. Nevertheless, there are some exceptions where a limited blurring exists:

[30] CONCORDIA, former Yugoslavia Republic of Macedonia. ARTEMIS, Democratic Republic of Congo. EUFOR ALTHEA in Bosnia, following SFOR. EUFOR RD Congo in support of Monuc. EUFOR Chad-RCA. EUNAVFOR - ATALANTA.

[31] Information gathered during interviews with officials from the European Commission, Council and military.

[32] In all military missions, it is possible to identify, via the identification of the material financed by ATHENA, the type of civilian equipment used and provided by civilian companies: communication (internet, computers, GSM mainly service contracts), electrical generators, transport (maritime and air), heavy-airlift assets to transport containers and deploy troops and material, 4x4 cars, trucks, camp services (laundry, etc.), works infrastructure (camps), fuel, food.

- In the case of the military operation in Chad[33], which was accompanied by EU humanitarian action under the ECHO programme (DG development), planning was conducted in common, since the military were asked to protect refugee camps. All other functions were separated.

- The military naval operation in Somalia[34], aimed initially at protecting boats delivering humanitarian aid, was then broadened to cover the general protection of maritime boundaries and the capture of "pirates". The process of arresting pirates and bringing them to trial has been "outsourced" to the public authorities of Kenya and the Seychelles, who have received funding for this purpose from the Community budget of the Stability Instrument.

- In Afghanistan, the NATO ISAF[35] military mission and the EU civilian mission (EUPOL)[36] are in charge of ensuring the security of the country. The military mission is located mainly in a remote zone, while policemen have been located in the less hostile urban environment. Nonetheless, civilian forces need to use military airlift capabilities and to have secure military-style communications in order to communicate between missions (satellite phone, VHF radios, SECTRA communication system). They have also requested armoured vehicles.

- The Guinea-Bissau mission[37] is the only one defined as a "civil-military" mission. This, though, was an advisory mission bringing technical assistance to local authorities, conducted by military and police officers without any specific equipment, except vehicles and telephone communications.

- In Kosovo[38], police and gendarmerie forces in charge of the maintenance of public order

[33] European Union military operation in the Republic of Chad and in the Central African Republic (EUFOR Chad/RCA) established with the Council Joint Action 2007/677/CFSP of 15 October 2007. Available at: http://www.consilium.europa.eu/showPage.aspx?id=1366&lang=en

[34] European Union military operation to contribute to the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast (EUNAVFOR Atalanta) launched by the Council Decision 2008/918/CFSP of 8 December 2008. Available at: http://www.consilium.europa.eu/showPage.aspx?id=1518&lang=en

[35] NATO's International Security Assistance Force (ISAF) official webpage: http://www.isaf.nato.int/

[36] European Union Police Mission in Afghanistan (EUPOL AFGANISTAN) established with the Council Joint Action 2007/369/CFSP of 30 May 2007. Available at: http://www.consilium.europa.eu/showPage.aspx?id=1268&lang=EN

[37] European Union mission in support of security sector reform in the Republic of Guinea-Bissau (EU SSR GUINEA-BISSAU) established with the Council Joint Action 2008/112/CFSP of 12 February 2008. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:040:0011:0015:EN:PDF,

[38] European Union Rule of Law Mission in Kosovo (EULEX KOSOVO) established with the Council Joint Action 2008/124/CFSP of 4 February 2008, http://www.consilium.europa.eu/showPage.aspx?id=1458&lang=en

needed to communicate with local police forces, European military forces and KFOR[39] forces and therefore established a minimum level of interoperability.

In the new strategic context described above, maximising capabilities to restore security in case of crisis is becoming an urgent necessity. Governments and first respondents need new, innovative and affordable solutions to respond to unpredictable catastrophic events, both inside the national territory and abroad. They also have to be prepared prior to an event, and require improved tools, infrastructures and procedures to respond and recover more effectively both during and after an accident or an attack.[40]

The ability to restore society after a crisis is a role in which the armed forces were active during the Cold War. The eventuality of a nuclear war pushed countries to set up resilience capabilities to protect the essential functions of their society: defence, political and administrative institutions and, to a lesser extent, the population as a whole. Even though the concept of security has evolved, military organisations will still play an important role in Europe in restoring key functions in case of a crisis/massive disruption. A network of protected bases, autonomous capabilities of energy production and telecommunications, transportation and medical capabilities are some features of the civil protection plans of each Member State. To that extent, the renewed role of defence organisations within the traditional remit of the security services is indeed the indication of a blurred mission. Still, even though the missions may appear to be blurred, defence and civilian organisations will continue to draw on separate capabilities and equipment to perform these tasks, despite the need for increased cooperation being evident.

Military organisations have a capability to project and deploy key sets of essential infrastructures and to enforce public order. This is a unique portfolio of capabilities, extending from engineering (i.e. roads, bridges buildings, and hospital deployment) to typical public order tasks, such as patrolling and controls. These capabilities were designed for war scenarios, in which military organisations were supposed to engage in battle and be able to project huge numbers of personnel into territories without infrastructures. Today, this war hypothesis seems remote, but this unique

[39] NATO's Kosovo Force (KFOR) website: http://www.nato.int/KFOR/
[40] ESRAB, *Meeting the challenge: the European Security Research Agenda*, 2006.

set of organisational and enforcement capabilities is proving to be an important asset both for crisis management and post crisis restoration phases.

The new feature is not so much a shift in military responsibilities, for which these capabilities have always existed, but the growing presence of civilian actors intervening in post crisis scenarios. Moreover, the restoration phase is increasingly implemented in a semi equipped context, in which a certain number of infrastructures and institutions continue to work (both at an EU internal or external level). This is the reason why this mission has some blurred characteristics, mixing both defence and public security actors. Procurement activities, though, appear still to be divided, as military organisations prefer to rely upon their *ad hoc* portfolio of capabilities.

1.3.2.2. Support to civil protection

As we have recalled in paragraph 1.3.2, crisis management abroad and support to civil protection are missions in which both military and non-military security actors are involved.

In recent years, military actors have increasingly been involved in support of activities to civil protection missions, as demonstrated during the 2004 South-East Asia tsunami, the L'Aquila earthquake in Italy and the forest fires in Attica, Greece, both in 2009. During all these natural disasters, national and international military troops worked side-by-side with civilian actors (civil protection, fire brigades and police) in order to overcome some operational deficiencies which still characterise civilian-led security activities. Armies, Navies and Air Forces provided, according to operational needs, some logistics (camps) and transportation (planes, helicopters, ships) capabilities, in order to ease and improve search and rescue and recovery activities.

In the same way as we have found for crisis management missions, however, blurring is also limited for civil protection activities. Military and civilian tasks remain largely separate. In fact, the assessment and evaluation of risks and threats have generally been carried out by civilian authorities and experts, who have also been charged with the overall management of the mission. Furthermore, even though basic coordination between defence and civil protection has been enhanced[41] at the "high level", in order to define general operational and tactical requirements,

[41] During international missions, coordination between military and civilians is generally guaranteed on a national basis. A higher degree of transnational cooperation at European level is enhanced by the role of the EU Monitoring and Information Center (MIC), but its activity does not affect/involve the role of national military forces.

command and planning capabilities have remained clearly separate. Separation is an issue highlighted by the Italian Ministry of Defence during the first response efforts to the earthquake in L'Aquila, stressing that "*during public calamities Armed Forces use their own personnel, means and materials to perform activities that are identical or similar to those that they normally carry out*".[42] Moreover, the Ministry stressed that "*the Armed Forces' role has to be considered complementary to that of civil protection*".[43]

A further point of ambiguity to emerge from the analysis of civil protection missions is the technical interoperability of civilian and military equipment. For instance, during the tsunami, incompatible communication systems had a significant impact on the effectiveness of exchanges of information between military and civilian forces deployed in the field. It is generally agreed that interoperability represents a key feature for the success of civil protection missions, but not all the actors involved in such missions seem to support the idea of integrating or sharing technological capabilities. This is mainly a political issue and not a technological one: some military decision-makers are reluctant to consider the possibility of sharing operational capabilities, highly technical and secure assets, with non-military actors. Moreover, as explicitly stressed by Italy's and France's armed forces officials involved in the tsunami response[44], the military consider their support to these civil protection missions as time-limited and marginal, and do not see themselves as an ongoing part of such operational efforts.

In these circumstances, the blurring between security and defence is more theoretical than real. In theory, satellite-based communication, mapping, localisation and monitoring technologies are considered key requirements both by civilian and military end-users involved in the field. However, the two groups do not agree on the level of interoperability which should characterise such technologies. On the military side there is still tangible resistance to the introduction of fully interoperable and reconfigurable systems. In contrast, civilian actors would enjoy the possibility of sharing and exploiting highly technical and reliable assets at the military's disposal, with a special reference to their logistic support and transport capabilities. Only "political" dialogue and new coordination mechanisms both at the levels of the Member States and the European institutions

[42] Italian Ministry of Defence, Operazione Gran Sasso: http://www.difesa.it/Operazioni+Militari/Operazioni+sul+territorio+nazionale+in+corso/Operazione+Gran+Sasso/
[43] Ibidem.
[44] Off the records interviews.

could push further the issue of interoperability in the direction of integrated technological solutions.

In conclusion, we can still identify clear dividing lines between military and civilian operations at various levels of civil protection missions. Short term planning and command structures, competences, tasks and equipment remain generally separate. At least at the theoretical level, however, there could be overlaps between the equipment requirements of military and civilian teams, but this depends on political decisions as will be explained later in the study.

1.3.3. Blurring trends within security missions

We intend in this section to go through the same exercise for the "High-end" security missions defined in this report. Protection against terrorism and organised crime, border security and critical infrastructure protection also present, at least potentially, a degree of blurring. Traditional law enforcement and security activities are not considered here, since these missions do not present a blurred character.

1.3.3.1. Protection against terrorism and organised crime

Protection against terrorism and organised crime implicate a wide range of activities; terror attacks, drugs and weapons smuggling, money laundering, individual and private sector fraud, and also the illegal movement of equipment and technologies that could be used in the development of weapons of mass destruction. ESRAB underlines their symbiotic relationship, whereby terrorists benefit from the infrastructure that organised crime can provide, while criminal groups can benefit from terrorism's financial links. Illegal activities of this kind are now facilitated by the use of easily accessible technologies (i.e. encrypted telephones to protect their communications, sophisticated trade transactions and communication through the internet). Moreover, the international and transnational nature of these crimes requires the ability of Europe's Member States to work together. The prevention of terrorist actions perpetrated by international terrorist organisations against citizens within the national territory and abroad is largely the result of a successful coordination of many elements, including situational awareness, surveillance and intelligence sharing between security agencies, defence organisations and intelligence services operating

outside the territory and internal security structures (police, intelligence agencies). [45]

Primarily, however, protection against terrorism and organised crime is a "security" mission under the responsibility of police forces. Only in exceptional cases, military forces are requested to participate in such security missions within the national territory of Member States. For instance, this has been the case for special events such as the Olympic Games in Greece, D-Day memorial commemorations in Normandy or the 2006 World Cup in Germany[46]. We have also noticed an increased recourse to armed forces in well-structured inter-forces operations, such as the operation "Strade Sicure", which involved the Italian Army, Navy and Air Force in surveillance and patrol activities in cooperation with internal police forces.[47] In total, roughly 4,250 Italian troops were deployed around the country to prevent or counter criminal activities and possible terrorist attacks. Also "Vigipirate", France's national security alert system, enables police-military anti-terrorist surveillance and patrol operations in subways, train stations and other vulnerable locations. Sometimes armed forces intervene in the case of a one-off attack, as happened in London in 1980, when the British Special Air Service had to storm the Iranian embassy captured by Iranian revolutionaries.

Although, in these circumstances, defence and security organisations share more or less the same technical requirements, armed forces continue to use the same *ad hoc* developed equipment they use for military operations, in order to control communication, detect and identify potential threats and manage information coming from different situation awareness systems.[48] For instance, military forces continue to use communications networks installed during the Cold War, in order to be in the best position to respond to a large-scale attack. This approach allows them to maintain secure intra-military communications but, *de facto*, makes any interoperability effort difficult with traditional security actors involved in the field. The same conclusions can be reached regarding cyber-defence, where the military possess particularly sophisticated tools for the

[45] We will provide details about actors involved in these missions in Chapter 3.
[46] For these major public events, governments requested NATO Airborne Warning And Control System (AWACS) support and their surveillance capability. www.nato.int/docu/awacs/awacs-e.pdf
[47] Italian Ministry of Defence, Operazione Strade Sicure, http://www.difesa.it/Operazioni+Militari/Operazioni+sul+territorio+nazionale+in+corso/Operazione+Strade+Sicure/
[48] This is due both to legacy and identity reasons.

protection of their own IT centres and for protection against a cyber-attack coming from hostile sources. Increasingly, moreover, military IT security is ensured by the use of open-source software (such as Linux), which has the advantage of being customised by the user himself. Therefore, military actors are more and more using unique solutions designed and/or customised by themselves. It is possible that particular civilian actors involved in highly sensitive missions such as anti-terrorism (for example, civilian intelligence agencies) do require a level of sophistication similar to that of the military actors; however, information on sensitive procurement is not available to the public for obvious reasons.

1.3.3.2. Border security

Border security has taken on a higher profile with the increase in major acts of international terrorism and in cross-border flows of illegal goods, people and substances. The Schengen Agreement, moreover, guarantees entrants to the Union a European wide mobility, with the consequences that: a) the protection of the external borders of a Member State assumes an additional relevance for all other Members, and b) border security has an increasing requirement to be complemented by internal security policies. Border management needs also to be balanced between security requirements and those necessary to facilitate legitimate trade and people flows, which are the basis of socio-economic development itself. ESRAB focuses particularly on the control of illegal immigration and trafficking in drugs, weapons and illicit substances. In securing maritime borders, blue-water navy surveillance and intervention capabilities must coordinate with brown-water operations by the coast guard and other police-type security forces in order to guarantee an overall response to potential risks.

Border control is another example of potential blurring between defence and security. As we will illustrate in the following paragraph about the function of "detection", territorial borders have always represented a point of contact between defence missions (the protection of the territory) and security missions (crime prevention customs controls). The European need to enhance border controls in order to combat trafficking and illegal immigration has fostered the development of institutions[49] and joint multinational operations. Maritime border control and land border control

[49] Such as Frontex, see Chapter 3.

are the two dimensions where users and companies feel the need to develop integrated systems. For example the Operamar (*An InterOPERAble Approach to the European Union MARitime Security Management)*[50] Preparatory Action for Security Research (PASR)[51] illustrates the need for interoperability between defence and civilian actors, also translated into the need for new systems which can manage information and data coming from both security and defence forces of different European States. Another 6th FP programme, LIMES[52] (Land and sea Integrated Monitoring for European Security) takes into consideration the commonalities of needs in the defence and security sectors to propose services such as maritime surveillance or land and infrastructure monitoring. These significant examples come from the 6th and 7th FP security research programmes, pointing out the importance of European security research in shaping the technology for this mission. They also indicate the constraints of the blurring argument, which is still limited to research programmes. Besides the EU efforts, some Member States have started setting up intergovernmental frameworks in order to exercise more effective control. This is the case of operation Nettuno, a joint patrol mission carried out in the central and eastern Mediterranean Sea, by the navies and police forces of France, Italy, Malta, Spain and the UK.

This trend is also evident at the Member State level. Italy, for instance, is highly exposed to migratory fluxes from the Mediterranean basin and has put the control of its borders (southern, in particular) in the hands of different forces belonging both to defence (Navy) and security institutions (Police) as well as hybrid corps such as Gendarmerie, Carabinieri and Guardia di Finanza. In this context, it is important to note the subdivision of the aero-naval service of the Guardia di Finanza into two separate departments: first, the high-water division, whose role is to combat the rise in human, drugs and arms trafficking in the so-called "sea highways"; second, the regional division, which patrols national territorial waters along the coastline and in ports. This emerging operational blurring is not, however, accompanied by any decision to expand and adapt procurement to the new requirements coming from the field.

[50] Operamar official webpage: http://www.operamar.eu/
[51] PASR was a pilot program to develop the processes and procedures used in 7th FP.
[52] LIMES official presentation: http://www.fp6-limes.eu/uploads/docs/LIMES-PRS.004-TPZ%20%5BInfosheet%5D.pdf

1.3.3.3. Critical infrastructure protection

Critical infrastructure protection covers a diverse number of physical and organisational systems, from sensitive buildings to train and subway stations, sensitive factories, energy production sites, information and communication networks and so on. Many of these systems are interlinked, so that a failure in one component could cause a general infrastructure failure. The protection of critical infrastructure is a combined responsibility of defence organisations, in particular as far as certain attacks are concerned (i.e. Air Forces are normally responsible for air space control), and security operators, both public and private. The combined responsibility is caused by two factors. First, some types of surveillance are not feasible for public or private security actors and require the intervention of defence actors who possess the adequate capabilities: this is the case for air surveillance. Second, because of privatisation, ownership of many critical infrastructures has been transferred to private companies, which therefore have a direct commercial interest in ensuring the proper functioning of the infrastructure, other than the mere responsibility *vis-à-vis* public end-users for keeping the infrastructure open and functioning.[53] However, critical infrastructure operators also need to make profits, and may decide to implement less-than ideal security measures, especially if not required by regulations and standards.

Critical infrastructures have always been considered by defence planners as potential targets in case of a war. Moving to a post 9/11 paradigm, those infrastructures are now potential targets for terrorist attacks or disruption. The protection of the air space is a clear example of this evolution towards a security mission, but it is not the only example where defence assets and personnel are used for anti-terrorist protection activities.[54] We also note the fact that defence organisations have developed specific technical know-how which contributes today to key security functions, such as in the field of CBRNE.

[53] Here again, the defence has a long tradition in terms of resilience during the Cold War. Some of the Cold War capabilities in terms of resilience of military systems and government against a nuclear attack represent a know-how and capabilities to be taken into consideration to minimise the effects of the disruption of a critical infrastructure network. This aspect was particularly analysed during the SeNTRE project.

[54] Seen the Annex 2 for national examples, such as *Vigipirate* plan in France.

For instance, NATO exhibits increasing concern for the protection of critical infrastructures. As clearly emphasised by Rear Admiral Mario Bartoli[55], NATO is currently taking measures to prepare for possible disruption to NATO and national infrastructures, since the protection of critical assets has both civil and military implications. Despite the clear interest expressed in this issue[56], however, NATO's operational involvement in such activities remains limited.

A single European approach to critical infrastructure protection is still being defined, as shown by an analysis of how single Member States deal with the issue. There is no single approach at the European level. For instance, in the UK, the Ministry of the Interior created the Centre for the Protection of National Infrastructure (CPNI)[57], in order to coordinate all the Government's initiatives for protecting critical infrastructure from cyber attacks. Representatives of the Ministry of Defence sit on CPNI's board, contributing to the definition of common policies to tackle threats to critical national infrastructure. However, at the empirical level, this Ministry of Defence commitment does not lead to an active operational involvement of the British armed forces in protecting critical assets. In Italy the situation is rather different. Since the institutional authority in charge of ensuring the protection of critical infrastructure is the Department of Public Security of the Ministry of the Interior, internal police forces would be in general assigned to such duties. However, armed forces reporting to the MoD are also involved in the protection of sensitive targets such as airports, train stations as metro stations. This is also the case of the Army's contribution to the "Vigipirate" plan in France. In this context, the military has tasks similar to those of the police, but they still deploy equipment generally used on defence missions. Hence, it is quite common to run into troops patrolling urban areas or surveying critical targets shouldering assault rifles. In the French case, we could therefore argue that some sort of operational blurring is emerging, but it is not yet accompanied by sufficient convergence in the procurement of equipment.

1.3.4. Common functions in the blurred area

In the previous paragraphs, we have identified some blurring trends between defence and security

[55] RAdm Bartoli is former NATO Deputy Assistant Secretary General Director of the Armaments Directorate.
[56] The topic was proposed by the Belgian Minister of Defence at the Berlin Informal Meeting in September 2005 and was recently added to the DAT Programme of Work.
[57] Centre for the protection of National Infrastructure official webpage: http://www.cpni.gov.uk/default.aspx

missions, emphasising in particular how this tendency is more evident at the conceptual level than in operational reality. In so doing, we have examined the two categories of "Post Cold War" defence and "High-end" security missions:

- Crisis management
- Protection against terrorism and organised crime
- Support to civil protection
- Border security
- Critical infrastructure protection (including private infrastructures).

To complete each of these missions, they require the following functions/capabilities identified in the ESRAB report:

- *Detection, identification, authentication* of personnel, vehicles, ships, as well as specific dangerous goods (i.e. arms, drugs and explosives) in unregulated borders and at check points.
- *Intervention and neutralisation capabilities*, intended to nullify or disarm dangerous individuals, vehicles or delivery systems.
- *Risk assessment, modelling and impact reduction*, to allow the identification of appropriate and targeted countermeasures; modelling tools to offer aid for decision makers to determine priorities among multiple risk factors and to verify the impact of proposed solutions.
- *Situational awareness*, which involves the capture, fusion, correlation and interpretation of disparate data, and their presentation in a clear manner. It facilitates decision-making and performance in a complex environment.
- *Training and exercise* to improve the effectiveness of all security staff, from crisis managers and first responders to operators and, in some cases, even ordinary citizens.
- *Command and control*[58] is about interoperability and information sharing and the

[58] As stressed by Luis Simón in its *Command and control? Planning for EU military operations* (EUISS occasional paper,

interconnection of different networks.

- *Communication* allows the sharing of data within and between organisations and countries: robust and secured communications are a prerequisite for an efficient chain of command.
- *Doctrine and operations*, the design and construct of the whole leadership chain and crisis management organisation.
- *Incident response*, a cycle of operations that should rapidly neutralise or contain the threats, restore basic services (i.e. energy, water, communications and transports) and allow a temporary rehabilitation of facilities struck by an incident or attack.
- *Information management* is the capability to handle information acquired by different sources (see also situational awareness) and make it available to those with authority.
- *Positioning and localisation* to track and trace people, vehicles, ships and goods inside open or controlled areas.

We can observe the existence of many functions shared by both security and military forces operating in "High-end" security and "Post Cold War" defence missions. These shared functions are:

- Detection; identification and authentication
- Situation awareness (including surveillance)
- Risk assessment, modelling, impact reduction
- Communication
- Information management
- Positioning and localisation.

The fact that these functions are shared by security and military players does not mean, however, that differences in the level of requirements and types of equipment used during the missions do not exist. Today, even when functions are shared between security and defence players, the

January 2010. Available at: http://www.iss.europa.eu/uploads/media/Planning_for_EU_military_operations.pdf) existing deficiencies in the European Command and Control capabilities are a major limit for the successful implementation of EDSP operations, limiting the Union's role as strategic actor.

equipment used remains rather different, with some exceptions especially in the field of communication.

1.3.4.1. Detection, identification and authentication

Detection, identification and authentication are functional requirements used in all security missions and are also required for implementing "Post Cold War" and "High-end" security missions, although in differing degrees according to the intensity of the mission.

In the case of border security, since the military are usually responsible for blue water operations and a number of security forces for brown water, the systems used in these two environments need to be coherent and compatible. Indeed, the Vessel Traffic System (VTS), in use in most large commercial ports, has an interface that guarantees a high level of interoperability with civilian operators, coast guard forces and navy military forces, often fusing data coming from all these sources. An example of such a system is the Vessel Traffic Management System developed for the Italian Coast Guard: the Italian VTS is made of a central control centre and 14 regional control centres, gathering data from 82 local sites, 100 sensor sites and three mobile units. A similar example is the new Integrated Command and Control Centre used in France for the protection of key strategic infrastructure as different as holy places, pipelines, international airports, but also air forces and navy bases. These are examples of interoperability and integration of systems and data between defence and security actors.

Within this category of functions, we can also observe an emerging trend for the procurement of the same systems. The problem of identification and access control for critical civil infrastructure, such as nuclear power plants, or private industrial and service providers, such as banks, chemical industries and IT networks, is by no means different from the problem of access to key military bases. Thus, BOSCH Sicherheitssysteme is not only supplying private customers, such as security systems for Munich Stadium[59], but also public security and military customers. The company sells security systems to the *Bundeswehr* and the Ministry of the Interior to a value in excess of 15 million euros per year.[60]

[59] BOSCH official webpage:
http://www.bosch-presse.de/TBWebDB/en-US/SearchResult.cfm?lb_veroeffentlichung=All&cbx_thema=111
[60] BOSCH Sicherheitssysteme GmbH, Betreibermodelle Von Bosch,

1.3.4.2. Situation Awareness and Surveillance

Situation Awareness and Surveillance is a key element for any operation involving both security and defence forces, as they often share the same environment, particularly in stability missions abroad, but also in border security tasks. Given the high level of uncertainty surrounding the dimension and direction of possible threats, the task of surveillance is particularly complex and multi-dimensional, thus involving a multiplicity of sources in the hands of both military and security players. Reaching a significant level of knowledge of the potential risks and threats depends on the fusion of different sources of surveillance. The demand for dual use assets is increasingly relevant as far as complex systems are concerned, for example observation satellites. They represent an example of the blurring of mission, functions and systems. The development of dual-use space Earth Observation (EO) assets (such as the Italian system Cosmo-SkyMed, the French Pléiades system or the GMES ESA/EC programme) indicates an important blurring trend for this function. The value added by costly space systems is driving the definition and production of common "security and defence" systems.

1.3.4.3. Risk assessment and modelling

Risk assessment and modelling is the next immediate area of common concern for defence and security operations, as any situation awareness given by surveillance systems must contribute to a comprehensive shared risk assessment. IT and security companies offer tailored security risk assessment which includes areas such as IT security and physical security on a particular site. These services can be easily requested by both security and defence actors. In the UK, a risk assessment tool developed for the banking sector is also used by Universities, such as the University of Leeds, and by defence companies such as Thales Underwater Systems. The tool is relevant for both the commercial and military networks of the company, providing health and safety training and risk assessment for the company's three sites. Here again, defence and civilian organisations are potential customers of the same technologies without implying necessarily a

---

http://209.85.229.132/search?q=cache:TOAQUFHu1DIJ:www.bosch-sicherheitssysteme.de/de/service/media/SafetyI2002.pdf+bosch+sicherheitssysteme,+bundeswehr&cd=5&hl=en&ct=clnk&client=safari.

commonality of the missions performed, paving the way for the development of similar equipment to be "customised" according to actors' particular requirements and budget possibilities.

1.3.4.4. Communication

Interoperable communications are considered particularly relevant to enable the use of defence assets in security operations and vice-versa. Interoperable communications are clearly necessary when military forces intervene to restore security in the case of national crisis. This scenario requires a level of coordination with all the other security actors (police, fire brigades, first aid, etc) that can only be achieved on the ground thanks to compatible communications. The same is true for all missions requiring civilian-military close cooperation. For instance, for counter terrorism missions during special events, such as the G8 meetings, close communications are crucial for coordinating the tasks of all the actors involved. Dual assets in the field of communications have therefore been developed. The UK Skynet satellite system provides mobile voice, video, internet and broadcast communications for the UK armed forces, and satcom services to civilian actors, and will supply Cabinet Office crisis management facilities and key crisis management centres across Great Britain. Skynet 5 could soon become an interoperable asset for UK defence and security players. Another relevant example is the radio system installed in the new Mobile Operations Room for the Italian Carabinieri: it guarantees secure communications not only between Carabinieri units but also between Carabinieri and all other security actors (fire brigades, civil security, Red Cross), allowing civil protection to be achieved in a coordinated manner. This demonstrates a strong trend in the security sphere. Due to the fragmented nature of their market, the need for interoperability is clearly expressed by security actors. However, interoperability with defence forces on blurred missions seems to be useful but not a priority for all actors.

The same logic is leading the German BMI to introduce a single software defined radio (SDR) solution for all security actors in Germany, called "BOS". It involves not only the Federal and *Laender* police, disaster relief forces, fire fighters and rescue services, but also customs authorities and domestic intelligence services. Allowing for 500,000 users, BOS will be the largest SDR system

based on the TETRA standard, which is also used in many other European countries.[61] In France, the brand new *Agence Nationale de la Sécurité des Systèmes d'Information* has created a dedicated secure communication system, used by the 300 higher state authorities, called RIMBAUD (*Réseau InterMinistériel de BAse Uniformément Durci*) system. The principal objective of this system is to ensure a secure, higher authority communication network, in case of the collapse of all other networks, with "secret defence" clearance. At the same time, its use is not limited to crisis or defence communication and can equally be used for civilian purposes.

When considering communications, therefore, the need for interoperability between defence and civilian organisations is a growing reality. Again, this need has not yet had much impact on the organisational and operational divisions between the players. Moreover, the level of blurring seems to be somewhat limited by the different technological requirements of armed forces and civilian actors. Civilian crisis management operators require a reliable, resistant and easy to use means of communication. Additional features in communication equipment are often considered redundant. Military users, however, have additional requirements such as anti-jamming devices.

1.3.4.5. Information management

Information management is another important shared function. The complexity and sensitivity of a database holding terrorist information about behaviour, position and capabilities, or containing a catalogue of potential weaknesses in elements of critical infrastructure, are by no means different from the level of sensitivity of databases used by the military in a defence operation. In fact, database structures can be very similar and search mechanisms can be identical. It is hardly relevant if the interrogating operator wears a military uniform or not. However, even though a commonality of requirements is emerging, it should be noted that fragmentation between different security and defence operators is currently producing specific "tailored" requirements.

[61] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsfunktionen, Das Projekt Digitalfunk Bos, http://www.bdbos.bund.de/cln_161/nn_421176/DE/Bundesanstalt/Projekt__Digitalfunk/projekt__digitalfunk__node.html?__nnn=true.

1.3.4.6. Positioning and localisation

Positioning and localisation are critical enablers that are present in virtually all the "Post Cold War" defence and "High-end" security missions analysed. What sometimes differs is the required level of performance. For example, the frequency of updates and precision required for conducting military operations or counter-terrorism are certainly superior to the level necessary for more permissive environments.

The much higher level of precision and availability of the GPS service required by the military (M-code), compared to the open civil service, is a direct consequence of these different environments. The Galileo PRS signal, for use by public security authorities only (including both security and military users), will similarly differ from the open code available to the general public, which will be limited in capability, but based on the same fundamental satellite global positioning and navigation systems. In fact, Galileo is an example of how the same signal can be used for different purposes, particularly the extended concept of "public security authorities", including military users, as defined in Chapter 3. The potential for blurring is therefore evident in the development of positioning and localisation capabilities.

1.4. Conclusions

Our mission-led research shows us contradictory tendencies towards blurring.

At a theoretical and political level, security analysis and perceptions of risk show important commonalities between security and defence. The definitions of missions and functions stemming from the evolving international strategic environment are a clear driver in favour of blurring. We see an increasing number of missions with the participation of both security and defence actors: blurred missions scenarios are a growing reality in a post 9/11 security paradigm. The diminished role of conventional defence missions has brought the military into operations where the application of force is limited, thus lowering the threshold of intervention, and moving into areas such as the restoration of security, reconstruction and law enforcement. Analysis of different specific functions also indicates some overlapping between security and defence.

Nevertheless, if we examine the practical implementation of these scenarios, operational blurring, in terms of responsibilities and equipment used on the ground, is often limited, if not absent. In fact, current civilian-military cooperation appears to be more limited in reality than could be expected from the identified overlap in functions.

For “High-end” security scenarios, the situation seems to be slightly different, as some missions indicate blurring trends also on the equipment side. Due to the emergence of new risks and the growing awareness by European citizens of these risks, the demand for security is increasing and encompassing new roles that were not traditionally foreseen for security organisations. These roles often require the same functions as a defence mission, but necessitate a somehow lower intensity. In this new context, some territorial defence assets developed by national defence organisations during the Cold War period could provide the resilience capabilities useful to address this enlarged security. Still, today the institutional framework of this “new security” is yet to come, and responsibilities are still divided between defence and civilian organisations.

In conclusion, a significant level of overlap between security and defence is evident at the functional level, as missions are increasingly shared by military and non-military players. However, blurring at the level of equipment appears to be concentrated in some key areas only, where a mission requires new technologies. This does not impact on the division of organisations. To what extent these developments are also prevalent with regard to technology will be addressed in the following chapter.

2. Technological aspects of the blurring of dividing lines between security and defence

Based on the literature review and on our engagement with stakeholders, we have pointed to technology as one of the main drivers for the blurring of dividing lines between security and defence. The aim of this chapter will be to substantiate that claim, to identify those technologies that may contribute to the blurring and to discuss the processes and barriers to the transfer of defence-origin technologies to security applications (products and services) and vice versa. This analysis is important for our understanding of the industrial implications of blurring. Where there is a growing blurring of technologies, we might expect this to be a necessary (but not a sufficient) condition for companies to diversify into related markets.

We emphasise here that the focus of this chapter is on technology and that "technology" has a particular meaning, as we will discuss in the first section of this chapter. We define technology as the ensemble of knowledge, skills and artefacts that are used to develop, produce and deliver products and services. Thus, this Chapter focuses on the STACCATO typology of technologies-components.[62]

As a first step, we will define and classify technologies according to their potential for blurring. Then we will locate them, according to their origin (defence or security sector) and to Europe's position vis-à-vis other parts of the world. In this context we will review the activities of Member States with regard to particular technologies. Subsequently, we will discuss the factors that influence the transfer of defence-origin technologies to civil security applications and vice versa. While this chapter focuses on technology's contribution to blurring, it is widely recognised that organisational, societal and human factors greatly impact the security of citizens and communities. Hence, we offer a reflection on societal resilience. A conclusion summarises the main findings and prepares the ground for our recommendations.

[62] As stressed in the introduction, we concentrate on technology as the second of the two main drivers for blurring. This is why we analyse extensively this aspect in this chapter, leaving aside discussions on equipment and subsystems. In fact, although the analysis of equipment and subsystems could also support the evaluation of blurring on the basis of the STACCATO taxonomy, this action would have required a considerable effort of data gathering (often too sensitive to be disclosed or not available at all) which was beyond the remit of our team.

2.1.Technology - definition and classifications

The following assessment of technologies is based on three assumptions: we hold that technology per se is neutral; hence no technology is inherently a dual-use, security or defence technology, only its applications are specific; finally, the location in which it originates in an economy influences the ways and possibilities of its diffusion and use. From these assumptions, we will present our analysis and suggest two classifications for technology.

We define technology as "the ensemble of theoretical and practical knowledge, know-how, skills and artefacts that are used by the firm to develop, produce and deliver its products and services".[63] Defined in this way, technology and its underpinning knowledge is in reality "neutral" and can be applied in a variety of ways. In other words, no technology is inherently a "defence" or "security" technology. Analysts of defence technologies have long argued that technical knowledge – in contrast to physical objects and artefacts – must be presumed to have an inherently dual-use or multiple-use character until and unless analysis shows otherwise. That is, the end products and artefacts for defence customers, civil security customers and private security customers may be very different, but they may well draw upon common or similar knowledge.[64] Following this definition, most technologies at this most basic level are "blurred" since they have multiple applications in civil, security and defence uses. The academic and practitioner literature on dual use technologies has repeatedly made the point over the last two decades. [65]

The neutral character of technology has important implications for how technologies should be classified. For the purposes of this project we will classify them according to two criteria: on the one hand according to their applicability, and on the other according to their origin.

We use the distinction of four security and defence missions developed in the previous chapter to classify the technologies according to their applicability. Consequently, we will attribute the relevant technologies to the categories of "High-end" defence, "Post Cold War" defence, "High-

[63] Burgelman and Rosenbloom *Technology Strategy: An Evolutionary Process Perspective*, JAI Press Inc, 1989.
[64] Alic, John A., Lewis M. Branscomb, Harvey Brooks, Ashton B. Carter, and Gerald Epstein. *Beyond Spinoff: Military and Commercial Technologies in a Changing World*, Harvard Business School Press, Boston, 1992.
[65] For example, see Alic et al ibid; Molas-Gallart, Jordi *Which way to go? Defence technology and the diversity of 'dual-use' technology transfer*, Research Policy, Volume 26, Issue 3, October 1997: 367-385. Cowan, Robin and Foray, Dominique, 'Quandaries in the economics of dual technologies and spillovers from military to civilian research and development'. Research Policy 24, 1995: 851–868.

end" security, and "Low-end" security. This classification according to missions allows us to assess to what extent each technology contributes to a blurring of boundaries between security and defence.

Classifying technologies according to their origin will shape our understanding of the opportunities and mechanisms for the diffusion or transfer of technology between the defence and security sectors. As for the origin of a technology, we can distinguish four possibilities according to where in the economy – what type of company or organisation – and how the technology was developed:

Defence-origin technologies with a growing security application. We define defence-origin technologies as technology investments made with primarily defence mission objectives in mind, which are funded through defence R&D spending and are conducted primarily by government defence research establishments, defence contractors or other research organisations. Stealth technology would be an example.

Civil security-origin technologies with a growing defence application. We define civil security-origin technologies as technology investments made with primarily civil security mission objectives in mind, which may be funded through R&D spending by public sector civil security agencies and/or companies and are conducted primarily by government civil security research establishments, companies or other research organisations: for example biometrical technologies.

Enterprise security-origin technologies with growing security or defence applications. We define enterprise security-origin technologies as technology investments made with primarily enterprise security mission objectives in mind, which are funded primarily by private sector companies and by general public R&D programmes and are conducted largely by private sector companies or other research organisations. Access control applications are but one example of this type.

Generic civil-origin technologies with growing security or defence applications. We define generic civil-origin technologies as technology investments that are not made with defence or security mission objectives in mind but which may be applicable to those missions. Investments in these generic technologies may be funded and conducted by a variety of private and public sector organisations.

Generic technologies include, for example, computer technology; information security technology such as commercial encryption or software protection; telecommunications technology (mobile

phones and their applications); display technologies such as LCD screens; digital imaging; robotics; certain sensors originating in the automobile industry; structural materials such as composite materials; surface treatment materials such as smart textiles; plasma technology; energy generation and storage technology; electronic components; artificial intelligence and decision support technologies; physiology science and medical technologies; biotechnology such as rapid analysis of biological agents and of human susceptibility to diseases and toxicants. All of these have potential defence and security applications.

In the next steps we will use both the categorisation by missions and by origin to identify areas of technology blurring and to indicate the origin of the defence and security technologies.

2.2.National programmes

By way of context, and before identifying areas of technology blurring and considering the origins of those technologies, we now provide a short description of security research programmes in the four Member States that are the focus of this study. We conclude this section with some cross-cutting comments.

However, we wish the Commission to note here that the transparency of these programmes differs between countries. Table 2 (below) provides a summary of the key points for each country.

Germany

The German Federal Government has published a detailed statement of its Security Research Programme with budget information. The Federal Ministry of Education and Research (BMBF) has become an important procurer of research services. Parallel to the EU's security research programme, the BMBF set aside 123 million euros for a four year period starting in 2007 to finance security research activities. Its security research programme pursues two strands.

First, while the programme is announced as promoting "non-military" security research, it aims to enhance the "mutual exchange of research know-how".[66] Stakeholders have indicated, however, that the separation between security and defence persists. Both the Ministry of Defence and the

[66] A. Hoffknecht, *Research for Civil Security, Protection systems for security and emergency services,* Berlin, 2009.

Federal Ministry of Education and Research insist that their budgets are used by the research institutions exclusively for defence research projects with military applications and security research projects with civil applications respectively.

The security research programme unfolds along two major lines:

- "Scenario oriented" research focusing on four topics: (1) protection and rescue of individuals; (2) protection of transportation infrastructures; (3) Protection against failure of supply infrastructures; and (4) security of supply chains.
- "Technology bundles" researching technologies that cut across the different scenarios with a focus on (1) integrated protection systems for rescue forces; (2) multi-sensor systems for CBRNE-risks; (3) pattern recognition; and (4) biometry.

Second, the programme promotes research that investigates technological and societal issues. In each topic emphasis is placed on the assessment of the societal dimension of security. Thus 30% of the funds for the transportation infrastructure scenario are spent on investigating the acceptance of security technologies and measures, on risk assessment and on cost-benefit analysis.

In addition to the security research programme, the Federal Government opened a specific security research programme for information technologies in August 2009, which is part of the "IKT 2020" (information and communication technologies) programme. It addresses new challenges and potential weaknesses in IT systems as well as security in unsafe environments. The Government is providing funding of 30 million euros for the next five years. The programme is targeted at IT and IT-security companies in Germany, universities and other research institutions. It focuses explicitly on those projects that bear a high "scientific-technical risk".

The United Kingdom

In August 2009, the UK government published The United Kingdom's Science and Technology Strategy for Countering International Terrorism. This provides a great deal more information on the UK's strategy and research priorities than was previously available. The document explains that the strategy has three principal objectives:

- To use horizon scanning to understand future scientific and technical threats and opportunities and inform decision making on counter-terrorism.
- To ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority science and technology requirements.
- To enhance international collaboration on counter-terrorism related science and technology.

The strategy also identifies some of the key counter-terrorist challenges that the UK will need to address in the next few years and where science and technology are likely to be vital. The challenges set out in the document are:

- Understanding the causes of radicalisation;
- Protecting the national infrastructure;
- Reducing the vulnerability of crowded places;
- Protecting against cyber terrorism;
- Improving analytical tools;
- Identifying, detecting and countering novel and improvised explosives;
- Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) threats.

Although there is still no publicly available statement of UK central government budgets for security science and technology, the document does reveal that the UK's cross department science and technology programme to strengthen the UK's ability to respond to a CBRNE attack has a budget of around £10 million a year and includes more than 50 projects.

France

The French government does not publish the details of technology funding, but the publicly available information allows us to draw some conclusions on the volume of activities and overall priorities. In total, France devotes 813 million euros to defence and security research (2009

budget). 15% of this budget is dedicated to basic low level readiness technologies. Many of them have dual-use applications benefiting both the defence and security sectors. As a consequence, we can consider that over 130 million euros of R&T technologies could have defence and security applications.

There is no specific security research programme in France. However, the *Délégation Générale pour l'Armement* (DGA) within the French MoD and the *Agence Nationale pour la Recherche* (ANR) are conducting research on national security issues. Both are public administrative institutions and clear links exist between the defence research planning in the DGA and the ANR.

Six programmes of the *Agence Nationale pour la Recherche* are managed in cooperation with the DGA on: new technologies for information and communication (NTIC), nanotechnology, biology and health, security, energy and materials. Another programme "concept, system and tools for global security" is co-financed by those agencies for 2 million euros, while 1.5 million euros are dedicated to the energy storage programme. Last but not least, the Ministry of the Interior devotes credits to equipment procurement, but does not invest in R&T for the security area.

Italy

There is also little transparency to activities in Italy. There is no dedicated national security research programme. In general, national research policies are carried out by an inter-ministerial committee under the guidance of the *Ministero dell'Istruzione, dell'Università e della Ricerca* (MIUR, Ministry for education, universities and research). In 2005, MIUR published a *Programma Nazionale per la Ricerca* 2005-2007 (PNR), which contains research guidelines and a list of strategic areas. The PNR outlines 10 strategic areas, of which only one area is devoted to "environment, transport and security". It includes innovative high-bandwidth satellite based telecommunications systems for surveillance, security and response to natural disasters.

Table 2 provides a summary of the national programmes for our four study countries.

Table 2: National security research programmes

Country	Key statement of programme	Budget (€m)	Focus
Germany	Security Research Programme	123 (for four year period starting 2007)	"Scenario-oriented research": Protection and rescue of individuals; Protection of transportation infrastructures; Protection against failure of critical infrastructures; Security of supply chains; "Technology bundles": Integrated protection systems for rescue forces; Multi-sensor systems for CBRNE-risks; Pattern recognition; Biometry.
United Kingdom	The United Kingdom's Science & Technology Strategy for Countering International Terrorism (2009)	No publicly available statement of budgets but UK cross-departmental CBRNE budget is £10m (€11.33m)	Understanding the causes of radicalisation; Protecting the national infrastructure; Reducing the vulnerability of crowded places; Protecting against cyber terrorism; Improving analytical tools; Identifying, detecting and countering novel and improvised explosives; Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) threats.
France	No specific programme but both DGA & ANR engaged in national security research	813 (defence & security, 2009 budget)	New technologies of information and communication (NTIC); Nanotechnology; Biology and health; Security; Energy; Materials; Concept, system & tools for global security; Energy storage programme.
Italy	No dedicated national security research programme	Little transparency	One of PNR's strategic areas in environment; transport & security

Cross-cutting themes

There are a number of themes that cross-cut some or all of these national programmes, as follows:

- The national security research programmes have all been established relatively recently and represent an important policy innovation at Member State level. The German programme was established with reference to activities at EU level. In the case of the UK, the latest policy statement makes explicit reference to the importance of UK participation in international programmes, including 7th FP.
- There is an increasing recognition on the part of some Member States of the need for greater transparency with respect to their technological priorities for security research. The UK is a good example of this, since its latest policy document contains far more detail than its first publication. In large part, this is because of a recognition that stakeholders in industry and the university sector require greater transparency if they are to engage with the government in this field (although still recognising the security sensitivities of information release).
- There are efforts to create synergies between defence and civil security research activities, although barriers remain (we return to this point and discuss it in more detail later in this chapter).
- Where governments release public domain statements of their technology priorities, we note that those priorities are very similar between national research programmes, in large part because they are also based on similar mission requirements. Thus, the German and the UK programmes have similar concerns about stimulating technologies that contribute to the protection and rescue of individuals, protection of transportation and other critical infrastructures, as well as understanding and countering CBRNE threats. This places an emphasis on sensor technologies, biometry, computing technologies, information security technologies and so forth.

Based on an analysis of these and other documents and our engagement with stakeholders, we have classified the technologies.

2.3.Identifying areas of technology blurring and the origin of technologies

In order to identify areas of technology blurring, and for the purpose of classification, we start with the STACCATO typology of technology-components and present our results in Table 3.[67] For each of the STACCATO technology-component classes, we identify the extent to which that technology has application in defence, civil security and enterprise security. We highlight those technologies that have important applications that cross-cut defence and civil security, i.e. technologies whose application blurs the defence-civil security boundary. We then list the particular technologies that have cross-cutting applications. Here we draw on those technologies identified by ESRAB, as their report provides us with a guide to those technologies that are important to civil security missions.[68]

The applicability of technologies for different missions is assessed on the basis of document analysis. We have supplemented this analysis by consulting a small number of technical experts to validate our findings.

Table 3 summarises our findings regarding both classifications. It contains only those technologies which are applicable with regard to at least two missions.

[67] We re-emphasise here that the focus of this chapter is on technology and that "technology" has a particular meaning as we have discussed in the first section of this chapter. We define technology as the ensemble of knowledge, skills and artefacts that are used to develop, produce and deliver products and services. Thus, this Chapter focuses on the STACCATO typology of technologies-components.

[68] Our findings are in line with the results of another study currently undertaken on a related topic. ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009. Available at: http://ec.europa.eu/enterprise/newsroom/cf/itemshortdetail.cfm?item_id=3931&lang=en&tpa_id=168

Table 3: Origin and applicability of technologies with cross-cutting application[69]

STACCATO Technology-component	Application				Technologies with cross-cutting applications	Origin of techno-logy
	High end defence	Post Cold War defence	High end security	Low end security		
100 Structural materials & technologies & structural effects analysis	✓✓✓	✓✓	✓✓	✓	Composites materials technology Anti blast glasses and concretes	Generic
101 Light and strong materials, surface treatments	✓✓✓	✓✓✓	✓✓		Light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surfaces treatments for improvement of life duration, corrosion reduction	Generic
102 Materials for deterrence	✓✓✓	X	X	X		Defence
103 Stealth materials and Technologies	✓✓✓	X	X	X		Defence
104 Survivability and hardening	✓✓✓	✓✓	✓✓	X	EMC evaluation and hardening, critical buildings specific architectures, blast and shock effects	Defence
105 Energetic materials	✓✓✓	X	X	X		Defence[70]
106 Plasma	✓✓✓	✓✓✓	✓✓✓			Generic

[69] Key: ✓✓✓ - Very highly applicable; ✓✓ - Highly applicable; ✓ - Some applicability; X - Little or no applicability

[70] In our discussions with experts, energetic material was identified as one field where the primary *application* was in war-fighting rather than security. This is not to say that an *understanding* of energetic materials is not needed in counter-terrorism security. Indeed, a detailed understanding is necessary, for example, to design and develop more robust structural materials, anti blast glasses and so forth as well as the development of new bomb detection equipment.

technology						
107 Energy generation storage & distribution	✓✓✓	✓✓✓	✓✓✓	X	Electrical generators, electrical batteries, energy distribution	Generic
108 Photonic/optical materials & device technology	✓✓✓	✓✓	✓✓	✓		Security/ Defence
109 Optoelectronics: laser, optics & related devices	✓✓✓	✓✓✓	✓✓✓	X		Security/ Generic

STACCATO Technology-component	**Application**				**Technologies with cross-cutting applications**	**Origin of techno-logy**
110 Sensor technology & components	✓✓✓	✓✓✓	✓✓✓	✓✓	Hyperspectral/multispectral sensors, hyperspectral/multispectral processing, autonomous small sensors/smart dust technologies, IR sensor technologies, Terahertz sensors, optical sensors technologies, acoustic sensors — passive; active & adaptive optical systems (material, sensors, actuators); radar.	Security
111 Electronic components	✓✓✓	✓✓✓	✓✓✓	✓		Generic
112 Signal processing technologies	✓✓✓	✓✓✓	✓✓✓	✓	Data fusion techniques, data collection/ data classification, image/pattern processing technology, information fusion technology, data and information management technology (DB, etc.)	Security/ Generic

113 Information technologies	✓✓✓	✓✓✓	✓✓✓	✓	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems.	Generic
114 Artificial intelligence & decision support	✓✓✓	✓✓✓	✓✓✓		Text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modelling and simulation, optimisation and decision support technology	Generic
115 Simulation tools & software	✓✓✓	✓✓	✓✓	✓	Virtual and augmented reality, tactical/ crew training systems, command and staff training systems, synthetic environments	Defence/Security/Generic

STACCATO Technology-component	**Application**				**Technologies with cross-cutting applications**	**Origin of techno-logy**
116 Computing technologies	✓✓✓	✓✓✓	✓✓✓	✓✓✓	Protocol technology, software architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering	Generic
117 Information security technologies	✓✓✓	✓✓✓	✓✓✓	✓✓✓	Encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)	Generic
118 Communication technologies	✓✓✓	✓✓✓	✓✓✓	✓	Reconfigurable communications, mobile	Generic

					secured communications, communications network management and control equipment, network supervisor, network and protocol independent secured communications, information security, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment.	
119 Physiology science and medical technologies	✓✓✓	✓✓	✓✓	X	Rapid diagnosis of infectious diseases; Novel antiviral, antibiotics, vaccines & drug development; Chemical & biological knowledge & related databases.	Generic
120 Human sciences	✓✓	✓✓	✓✓✓	✓	Human behaviour analysis and modelling, population behaviour, human factors in the decision process, teams, organisations and cultures	Security/ Generic

STACCATO Technology-component	**Application**				**Technologies with cross-cutting applications**	**Origin of techno-logy**
121 Biotechnology	✓✓✓	✓✓✓	✓✓✓	✓	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control.	Generic

From the table, we can identify three groups of technologies with different degrees of applicability across the four mission types.

First, there are a number of technologies that have applications primarily in "High-end" defence operations and that are hardly likely to be applied for security missions. These are:

- 102 . Materials for deterrence;
- 103. Stealth materials and technologies;
- 105. Energetic materials.

Second, we also identify a number of technologies that have applications in both the defence and civil security sectors. Some of them are eminently applicable only for "High-end" defence operations, "Post Cold War" defence missions and "High-end" security missions, and are less useful for "Low end" security missions. These technologies are:

- 101. Light and strong materials, surface treatments;
- 104. Survivability and hardening;
- 106. Plasma technology[71];
- 107. Energy generation storage & distribution;
- 109. Optoelectronics: laser, optics & related devices;
- 114. Artificial intelligence & decision support;
- 119. Physiology science and medical technologies.

Third, other technologies can be used across the entire spectrum of missions. This latter group of technologies, which has applications in all mission types, is of particular interest for the purpose of this study. These technologies will therefore be outlined in further detail in the next section.[72]

[71] Plasma technology has a number of security and defence applications, including the potential use of gas plasma technology in advanced telecommunications antennas and the potential use of cold plasma for the decontamination of equipment and clothing exposed to chemical and biological hazards.

2.4.Technologies with applications across defence and security missions

In the following paragraphs we will briefly describe the technologies with the largest potential for blurring and qualify our classification.

100. Structural materials/technologies and structural effects analysis. Within this technology component we consider composite materials technology, anti blast glasses/concretes as particularly important for blurring. The concern about designing structures that better withstand explosion is shared by the military, i.e. for military installations and barriers as well as public and private security providers. The latter seek better ways of protecting public buildings. The construction and insurance industries will try to find ways to integrate such technologies in newly erected landmark and vulnerable private buildings.

108. Photonic/optical materials and device technology. These technologies enable the generation, emission, transmission, modulation, signal processing, switching, amplification, detection and sensing of light. Though it is a very generic technology with many applications also outside security and defence, we consider it as a driver, given its significance not only for IR sensors, but also for navigation, search and rescue, mine laying and detection, and command and control, applications.

110. Sensor technology & components. Especially hyperspectral/multispectral and autonomous, IR sensors and optical and acoustic sensor technologies are strong drivers for blurring. They are crucial for the intelligence gathering, surveillance, and reconnaissance functions, which are not only of interest to the military but also to public and private security providers. The latter make increasing use of such technologies as the possibilities for control at borders need to be automated or transformed into a surveillance of territorial space, rather than merely entry points.

[72] BMBF, Sicherheitsforschung - Forschung Für Die Zivile Sicherheit, http://www.bmbf.de/de/6293.php; Bundesministerium für Wirtschaft und Technologie. *Marktpotenzial Von Sicherheitstechnologien Und Sicherheitsdienstleistungen*, Berlin, BMWI, 2009. Hamburgisches WeltWirtschaftsInstitut, Sicherheitsindustrie, 2008. http://www.hwwi.org/fileadmin/hwwi/Publikationen/Partnerpublikationen/Berenberg/Berenberg_Bank_HWWI_Strategie-2030_Sicherheitsindustrie.pdf

The identification of explosive and CBRN substances is a further area of concern to both the security and the defence sector. Here we also include radar sensors which have applications in both defence and security surveillance.

111. Electronic components. These simple electronic elements can be combined together to perform different functions that are the basis for all complex electronic systems, no matter where the latter are applied. They present a generic category with potential applications in many other fields. They may therefore be regarded as an example of blurring although – as a generic technology – the blurring is across many applications both security, defence and civil.

112. Signal processing technologies/113. Information technologies/116. Computing technologies/ 118.Communication technologies. All these technologies are very much akin to each other and play a very important role in blurring. On the one hand, they are deliberately used in order to create interfaces and ensure interoperability among different security and defence providers on common missions. On the other hand, they are critical enabling technologies for modern defence platforms and for Network Enabled Capability (NEC). The resulting rapid increase in dependency on software to provide critical functions, for example, has outstripped the ability of Ministries of Defence cost-effectively to 'own' military software. Because of the particularly difficult problems that MoDs face with high integrity and safety critical software, there is much overlap with civil sector requirements and there is a growing recognition that there is much to be gained by aligning military practices with civil solutions. A good example of the potential for aligning military and security is provided by the case of Software Defined Radio (SDR) which has applications both for military use and use by first responders (police, fire service and so forth). This received funding from the European Commission through its PASR (€3 million) and the 7th FP security theme (€15 million). SDR has also received funding from the European Defence Agency (EDA). Under current arrangements, different funding and management systems were involved between the EDA and the European Commission.

117. Information security technologies. These technologies ensure the secrecy, availability and integrity of data. IT security is a very strong driver for blurring because increased digital connectivity makes the networks of the military and security forces, as well as important economic institutions, more vulnerable to attack. Moreover, hacking is increasingly dominated not only by professionalised crime, but also used by state actors. Increased networking, i.e. through use of NEC, enlarges the scale of hacking effects.[73] While in the past, IT security technologies originated in the defence sector – especially regarding cryptography – most innovation today is achieved in the private security sector.[74]

115. Simulation tools & software. Among these technologies, especially those that are applied in tactical/crew training systems, command and staff training systems, synthetic environments are specifically strong drivers for blurring. Due to the need to prepare for a variety of possible scenarios and given the constraints of public finances, military, police and law enforcement personnel will increasingly use training systems that simulate different missions and are easily adaptable to new requirements. Defence companies like Rheinmetall have built on their expertise in these technologies and successfully entered the security market.

120. Human sciences. Technologies that can be applied for human behaviour analysis and modelling as well as for the examination of population behaviour are strong drivers for blurring. They are, for example, considered to be crucial in the fight against terrorists, as they allow for the identification and filtering of typical patterns of behaviour and the tracing of preparations for attacks. They are also applied for purposes of crowd control and dispersion of demonstrations, which is of equal interest to a military force in a peace keeping operation as to a police force at home.

121. Biotechnology. Here we mean all technologies that allow for the rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water

[73] Hamburgisches WeltWirtschaftsInstitut, 2008.
[74] *Marktpotenzial Von Sicherheitstechnologien Und Sicherheitsdienstleistungen,* 2009.

testing and purification techniques, food testing and control techniques. We consider these technologies to be drivers for blurring as they are essential for military operations in a hostile environment, not only for the protection of forces but also to clear secured territory and resources for the population. Security forces require such technology applications in order to protect domestic resources and react rapidly in case of a crisis be it after an attack or in reaction to a pandemic.

2.5.Specificities of technologies driving the blurring

In the previous section we identified those technologies that have significant applications across defence and security missions. Next we highlight some of the key features of those technologies.

2.5.1. Generic technologies are critical to defence and civil security applications

A first point to make is that generic technologies are increasingly critical to most defence and civil security products and systems. The fact that both defence and civil security products rely heavily on generic and globally available technologies, not least information and communications technologies (ICTs), can be seen as a powerful driver of blurring.

Of course, this is not a new point, but its importance means that it is necessary to repeat it here. The ESRAB Report notes that ICTs in particular are increasingly pervasive and are revolutionising the manner in which organisations (both public and private) are able to address their security needs.[75] Since the 1980s, dual-use and civil origin technologies have assumed growing importance in the defence sector, reflecting the growing size and increasingly technologically sophisticated demand of consumers in the electronics and industrial goods markets.[76]

The defence technology strategies of governments have increasingly sought to find ways of accessing civil origin technologies and spinning-in technologies from these increasingly globalised markets. For example, the *Bundeswehr* tasked a consortium of telecom companies (IBM and

[75] ESRIF, *Meeting the Challenge: the European Security Research Agenda*, 2006.
[76] John A. Alic, et al, *Beyond Spin-Off: Military and Commercial technologies in a Changing World*, 1992.

Deutsche Telekom) to upgrade its communication and information infrastructure. Moreover, German troops serving in Afghanistan have been supplied with communications devices, glasses and protective vests sourced from commercial suppliers. With respect to computing technologies, the defence sector is making increased use of open systems and architectures, and increasingly sees basic computing technologies as commodity items that can be purchased from global markets. However, specific technology solutions are still required in some areas. The most important of these areas is software, particularly for safety critical and other high integrity applications, and information management and information assurance. This is also a key focus of attention for MoDs. At the same time, defence concerns about security of supply and technology integrity have constrained the rate at which such developments have occurred.

In much of the security sector, security of supply and the sourcing of technologies from global markets are much less of an issue, as it is characterised by an "open innovation" approach where companies source technologies in global markets based on their cost and performance. "High-end" security users, however, (not least intelligence agencies) have similar technology sourcing concerns to those of Ministries of Defence, with an emphasis on technology integrity and trusted sources.

2.5.2. European industry has strong capabilities in some technology areas

A detailed analysis of European industrial capabilities for each element of the STACCATO taxonomy is beyond the scope of this study. Individual companies were unwilling to share such information with us, since it is regarded as commercially sensitive and we were unable to find such fine grained data from public sources. Instead, we highlight the point that European industry has a strong position in some of the technologies that we have identified:

Sensor technology and components. Europe has strengths in explosives screening technologies where Smiths Detection is one of the three main competitors in the market (with the U.S. companies GE and L3-Communications). European defence research laboratories, and especially the Porton Down facility of the UK Defence Science and Technology Laboratory, are recognised as leaders in the field of CBRN detection and screening technologies, as are European companies

such as Smiths Detection. Europe also has technological strengths in biometrics technologies, where the French company SAGEM is recognised as a leader in the field of rights management and physical and logical access applications based on biometrics, as well as secure terminals and smart cards. Europe also has a strong technological position in surveillance sensors.

Communication technologies. Europe has world-class strengths in communications technologies including generic communications, wired and wireless communications.[77] Nokia and Ericsson are global leaders in mobile communications technologies and Alcatel and Thales have very strong technological capabilities in networks and secure communications, including secure mobility, wireless technologies and ad-hoc networks. The future competitive strength of the European industry for security communications applications in global markets will depend on the extent to which the European TETRA standard is adopted in third countries rather than the competing P25 standard, which is widely deployed in North America.

Nanotechnologies. European excellence in nanosciences is well recognised, as is the challenge of translating that excellence into commercially viable products and processes.[78] The European aerospace and defence sector is investing heavily in the commercial application of nanotechnologie,s including companies such as Thales and SAFRAN.

Equally, there are a number of technologies where Europe has weaknesses. We identify two here:

Energy storage and distribution. The growing energy demands of both defence and complex "High-end" security systems are placing increasing emphasis on energy storage and distribution technologies. The United States is seen by many of the experts we interviewed as being ahead of Europe in fuel cell technologies, high energy power management and miniaturised energy sources.

[77] Dach, Bernhard, Weber, Matthias and Georg Zahradnik, *Europe's strengths and weaknesses in Information Society Technologies*, 2005. Report of IST -2001-37627 FISTERA - Thematic Network on Foresight in Information Society Technologies in the European Research Area. Available at: http://fistera.jrc.ec.europa.eu/docs/FISTERA%20SW.pdf
[78] European Commission, *Nanosciences and Nanotechnologies: An Action Plan for Europe 2005-2009*, Brussels, 2005.

Computing technologies. Computing technologies is another area of European weakness, with the global computer industry dominated by U.S. and Japanese multinationals. The situation is complex, however, since Europe has a strong software and computer/IT services sector which includes a number of notable large companies such as SAP, CapGemini and Logica. There is also a substantial SME sector that delivers niche products and services in the computer/IT sector.[79] Since we have noted that basic computing is increasingly regarded as a commodity, it is the capacity of these companies (including SMEs) to deliver tailored computing solutions to security and defence users (together with large European defence security firms) that is the most important factor for European technological competitiveness. Thus, Logica is an important actor in the defence and security sector.[80] Equally, there is a substantial number of SMEs, such as the UK company NEXOR which provides information assurance systems to the defence and "High-end" security sectors.[81]

2.6.Emerging technologies

This section focuses on the future and identifies some emerging technologies that may have potentially important applications in both the security and defence fields. Emerging technologies are those distinctive new technologies that will underpin future technical capabilities. The development of emerging technologies is unpredictable, since some technologies may fail to deliver on their early potential, some being superseded by other developments and others successfully transitioning into innovative new products.

Our analysis of key national documents and interviews with experts suggests that the following emerging technologies are likely to have implications for the defence and security sectors.[82] Of course, there are likely to be other emerging technologies that are important, but it is the

[79] This observation is contained in Dach et al, *Europe's strengths and weaknesses in Information Society Technologies,* 2005. However, they do not name specific companies.
[80] For information on Logica's defence and security activities see: http://www.logica.com/defence/350232713
[81] For information on Nexor see: http://www.nexor.com/
[82] In France, the DGA, in coordination with GIFAS and CIDEF, drafted a list of 46 emerging technologies that could potential emerge as having a "breaking" importance for the future (see *Politique et Objectifs Scientifiques*, edition 2008, *Direction Générale de l'Armement*, Ministère de la Défense) and in the UK, the 2006 *Defence Technology Strategy* also identified a number of emerging technologies.

following that are mentioned most frequently and stressed as particularly relevant in the national documents that we have analysed and the interviews that we have undertaken. We focus here on three technologies that have clear potential security and defence applications.[83]

Semantic web technologies. The semantic web will make better use of the World Wide Web as an information source, by providing computational meaning to web documents. Through developments in language technology, computers will be capable of conducting increasingly sophisticated search activities. Semantic web technologies have potential defence and civil security applications. In the defence context, the use of the semantic web will aid decision support by enabling commanders to retrieve relevant information in a timely manner and have it presented in an easily understandable way. In the civil security context, similar applications may aid the work of first responders. Equally, there may be applications in the intelligence community.

Semantic web technology is based on work done by the United States Defence Advanced Research Projects Agency (DARPA) and by international standards bodies such as the World Wide Web Consortium. A number of organisations are developing semantic web technologies to meet U.S. Department of Defence programme requirements, including Lockheed Martin.

Autonomous self-organised networks of smart sensors. The aim of smart sensor networks will be to build a comprehensive picture of an operating environment and these networks may take the form of "intelligent" swarms of unmanned vehicles, as well as fixed networks of sensors. These technologies have applications in both the civil and the defence arena for intelligence gathering, surveillance and border security, and involve innovations in hardware and software used to sense signals, store sensed data, communicate and process information, as well as modules that power sensors for very long periods of time

Wireless sensors are being developed for a growing number of security applications: arrays of wirelessly mesh-networked sensors for detecting improvised explosive devices; GPS-based

[83] Since these are emerging technologies they do not necessarily fit easily within one of the existing STACCATO technology definitions.

radiation detectors; wireless surveillance sensors; and sensors that utilise fusion techniques and allow for identifying and communicating the presence of hazardous materials at major events.[84]

Technology development in smart sensor networks is primarily being undertaken in the United States and funded by the Department of Homeland Security and the Department of Defense. U.S. companies like Ember and RAE Systems are also investing heavily in such technologies for enterprise security as well as civil security applications.[85] Whilst technology development is mainly being conducted in the US, some European SMEs and universities are also working in this field.

Nanomaterials. Nanomaterials and nanostructures have been found to have modified properties associated with their small-scale. Carbon nanotubes (CNTs), nanowires, quantum dot nanostructures, graphene, nanomaterials, coatings and thin films, and nanopowders, are all being investigated for device development. The potential impact of their application will be huge both in the civil and defence sectors, since they offer the potential of protective materials with new properties and small scale devices with novel performance potential. Security and defence applications of nanotechnology potentially include improved CBRNE sensors, blast and ballistic protection devices (energy absorbing nanomaterials/CNT-based bullet proof armours/smart fabrics), nanotechnology-based imaging systems (X-ray, terahertz imaging) as well increased computing performance with applications in high-end intelligence and defence.

Though nanotechnology-based applications are promising for homeland security and defence sectors, commercial products are expected only in the long run. We have already noted that nanotechnology is a potential area of European strength if Europe is able to transfer its scientific excellence into commercial products.[86]

[84] Frost & Sullivan, *Smart Sensors and Sensor Networks: Opportunities for Networked Intelligent Wireless Sensors*, San Antonio, 2006.
[85] U.S. company RAE Systems describes itself as is a leading global provider of rapidly deployable, multi-sensor chemical and radiation detection monitors and networks for industrial applications and homeland security and should not be confused within the UK defence contractor BAE Systems.
[86] Frost & Sullivan, *Nanotechnology in Homeland Security*, San Antonio, 2009.

2.7.The extent of transfer of technology from defence to security

This chapter has identified a number of defence-origin technologies that have potential security applications. In this section we consider the extent of the transfer of technology between defence and security, focusing in particular on the processes (and barriers) of technology transfer from defence to security applications.

One of the puzzles in looking at the defence and security markets is why some defence-origin technologies have been rapidly adopted by security sector users, and why other apparently sophisticated technologies have only been slowly adopted. Another part of this puzzle is why defence companies with apparently similar technological capabilities have entered the security market with different levels of success. We treat this puzzle as a question of technological innovation, and by technological innovation we mean the process from technology development through to commercialisation. We argue that the answer to the puzzle of differing speeds of adoption of defence technologies lies in the interaction of three elements: (1) the nature of the technology itself and the response of potential users; (2) the capacity of defence companies to take technologies and to commercialise them through marketing; (3) the strategies that are open to defence companies.

We illustrate our argument with a discussion of several technologies and we pay particular attention to civilian adoption of UAVs illustrating many of our points. The rate and character of adoption of defence-origin technologies by security customers is likely to be influenced by the following four factors:

Relative advantage. To be adopted by security users, a defence-origin technology must first be perceived to be better than the products and systems that they currently use. Relative advantage is likely to be a complex trade-off between a number of dimensions and the relative advantage may be in terms of performance operating costs. A performance-cost trade-off is one factor which affects the relatively slow rate of adoption of UAVs for civilian use. Thus, UAVs have civilian applications not least in the fields of maritime surveillance and border security, but, in the eyes of

potential civilian operators, there is a trade-off between functional performance i.e. the benefits of long loiter time against perceived operating cost when compared to other solutions, such as conventional fixed wing or rotary aircraft.

Compatibility. A second factor in the rate of adoption of a defence-origin technology is the extent to which the technology is perceived to be consistent with the "world" of the potential adopters: defence-origin technologies are more likely to be adopted where defence companies are able to package those technologies in products, systems and services that are compatible with the existing *skills* and *practices, organisational processes, and the values* of the security user.

Existing skills – Defence products and systems often assume sophisticated and highly trained users with particular levels of physical fitness; they are unlikely to be quickly adopted by security customers if adoption requires significant (and disruptive) re-training of staff and/or the recruitment of staff with different skill levels. This is often an important consideration in the evaluation of new technologies by airports and seaports.

Existing practices - Defence-origin technologies are often combined into products and systems to meet particular operational doctrine or modes of operation. In the security sector, operational doctrine and practice is frequently very different and defence-origin technologies may need to be adapted to fit those particular operational requirements.

Existing organisational processes – In the case of port and airport security, new technologies need to be compatible with existing organisational processes. Thus, technologies are more likely to be adopted if they do not disrupt existing cargo handling processes or passenger throughput. We can also see this as a factor in the rate of civilian adoption of UAVs, since this has given rise to important and difficult to resolve questions about processes for managing civilian airspace. The integration of civil UAVs into the air traffic management environment has become an important constraint on their adoption.

Values and norms of potential adopters – Traditionally, the military operates in a defined battle space and its equipment tends to be used intensely, but for defined periods. In the public security domain, equipment is used in public spaces placing an emphasis on safety. It tends to be used

24/7, requiring "false positives" to be avoided since these can be highly disruptive to daily life, i.e. in the transportation and port security domains. Liability for equipment failure or disruption caused by false positives is also an issue, as well as privacy and data protection. Thus, a factor that has slowed the civilian adoption of UAVs is the need to develop public confidence in their safety and reliability.[87]

Trialability. A defence-origin technology is also more likely to be adopted if the potential security customer is able to experiment with that technology on a limited basis, testing it in the customer's particular operating environment and identifying the strengths and limitations of that technology and the need for adaptation. Where potential customers are unable to trial a technology before committing to its use, we would expect the rate of adoption to be slower, especially if the technology requires costly investment both in the technology itself and also in training and changes to organisational processes. This is one of the reasons why companies have invested in demonstrators as platforms for trialling new technologies to security customers.

Observability. A defence-origin technology is also more likely to be adopted where potential customers can observe its superior performance. Thus, whilst the capabilities of UAVs are recognised from their well reported use in Afghanistan, there is a lack of awareness amongst many civilian users of the readiness, capability and utility of UAV technologies for civilian missions. This reinforces our point about the importance of demonstrators, but it also has other important implications for the adoption of defence-origin technologies. Where technologies are "secret", their observability by others is by definition limited. There may be instances where technologies are used in the defence domain, but civil users may be unaware or only vaguely aware of their use. Thus, we have noted that one of the tasks of the MoD Counter-Terrorism Technology Centre in the UK is to raise awareness of defence-origin technologies that may have applications in the civil security domain. Equally, it emphasises that security customers are more likely to adopt a technology if a supplier can demonstrate a track record of successful use amongst other similar

[87] This point was made to us during several meetings and roundtable events with industry.

customers. For defence companies which are new entrants to the security market, this may present a potential barrier to the rapid adoption of their technologies.

2.8.The extent of transfer of technology from security to defence

A great deal of attention has been paid by policy makers and industry analysts to the challenges of transferring technologies from defence to security applications. This was the subject of the last section. In this section, we consider some of the issues that are arising in the transfer of technology between security and defence. We follow the same approach as in the previous section and focus on the processes (and barriers) of technology transfer from security to defence applications. We argue that the same basic considerations apply and the rate and character of adoption of security technologies by defence customers lies in the interaction of:

- the nature of the technology itself and the response of defence users;
- the capacity of security companies to take their technologies and to bring them to defence customers;
- the strategies available to security customers.

We focus on security technologies and do not consider the reasons for the growth in the use of private security services and private military companies by European Ministries of Defence.

We illustrate our argument with a discussion of several security technologies, and we pay particular attention to information and communication technologies (ICTs). Since ICTs are increasingly important for the military, not least through their role as the back-bone of network enabled capability and the ICT-enabled “transformation” of the military means, the security of those ICT systems is becoming a critical concern for European militaries. Civil-security origin technologies and enterprise security-origin technologies have growing defence applications. These include information security technologies. Companies with a strong position in civil-security origin and enterprise-origin information and communication technologies have entered (or strengthened) their position in the defence market. These companies include Cisco Systems, Sun Microsystems and Fujitsu.

However, there is an important paradox that needs to be explained. Whilst these technologies are clearly of growing importance, it is the case that security companies have rarely established themselves as prime contractors on defence programmes. Commercial technologies may be at the heart of the military network, but established defence companies remain the prime contractors on most communications and network infrastructure programmes. In most cases, security companies – whilst interested in the business opportunities emerging – remain subcontractors and suppliers and this is likely to remain the pattern for the foreseeable future. One example is the UK MOD's Falcon communications infrastructure programme, where BAE Systems acts as prime contractor with technology partners that include CISCO Systems.

Why is this the case? In explaining the challenges of technology transfer from defence to security applications, we placed a considerable emphasis on the factors that influenced the rate and character of adoption, namely: relative advantage of the technology over currently used products; compatibility with the processes of the adopter; the trialability of the technology; and, the potential to observe the technologies in use.

In the case of the transfer of technology from security to defence applications, by and large there is an acceptance by many Ministries of Defence of the considerable advantages in integrating companies from the civil and enterprise security sectors into current and future programmes. This is seen as providing a means of spinning-in their technologies and the systems engineering experience that they have gained from working on large private projects in the financial sector, retail sector and elsewhere.

Balanced against this, however, concerns are emerging about security of supply and technology integrity. Both issues are becoming increasingly important in an environment in which, with respect to computing technologies for example, the defence sector is making increased use of open systems and architectures and increasingly sees basic computing technologies as commodity items that can be purchased from global markets. These technologies are sourced in what are, in

effect, open and global markets from companies who are not under the same controls and scrutiny of Ministries of Defence as are traditional defence contractors.

In any case, specific technology solutions are still required in some areas. By far the most important of these is software, particularly for safety critical and other high integrity applications and information management and information assurance, which is a key focus of the attention for MoDs. Therefore, defence-specific development programmes and suppliers remain in some areas. At the same time, defence concerns about security of supply and technology integrity have constrained the rate at which the transfer of technologies from security to defence applications has occurred.

2.9.Societal resilience

The discussion in this chapter has focused on the technological aspects of the blurring of the dividing lines between security and defence. However, it is widely recognised that technology is not sufficient in itself to enhance the security of the European citizen. This leads us to turn to a discussion of societal resilience. By societal resilience is meant "the capacity of civilian communities to detect and prevent disruptions to a nation's security and, where necessary, to absorb shocks and bounce back into a functioning condition after a crisis as quickly as possible".[88] The societal resilience perspective emphasises that technical measures – enhanced surveillance, intelligence gathering and better equipment for first responders – may have a part to play in the security of the citizen, but our capacity to prevent, protect and respond to security events is strongly related to the resilience of our society.

This growing attention to societal resilience means that the causes of extremism and terrorism, as well as the capacity of societies to respond and recover from security events, have been the subject of increased attention. ESRAB may have been primarily focused on technologies, but it also noted the importance of the dimension of citizens and security and called for research into

[88] Centre of excellence for National Security, S. Rajaratnam School of International Studies, Singapore. http://www3.ntu.edu.sg/rsis/cens/our_work/social_resilience.html

improving the understanding of people's behaviour in crisis situations and also the profiling of terrorist behaviour. This is made more explicit in ESRIF, which has as one of its main themes the importance of societal resilience arguing that "[c]ertain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and must have the ability to recover". ESRIF sustains that a "holistic approach" to European security "must include efforts to ensure that the social, cultural, legal and political aspects of security research and development are taken into account". This should be reflected in research programmes, echoing relevant ESRIF key messages, and thus promoting overall "societal coherence".

Similarly, the recent FORESEC study[89] emphasises the importance of research in the area of societal resilience and recommends that it should focus on questions of cultural and social identity. This emphasis on the societal aspects of security is also reflected in national programmes. We have noted that the *United Kingdom's Science and Technology Strategy for Countering International Terrorism* emphasises that one of its key challenges is understanding the causes of radicalisation. Similarly, the German security research programme funds activities that look at the wider societal aspects of security.

This tendency of putting a growing emphasis on societal resilience has several important implications. First, there is a recognition that technology based responses to security threats are not sufficient in themselves to ensure the security of the European citizen. Indeed, there is a growing concern that the increasing visibility of the physical manifestations of security technology (for instance in the form of more CCTV cameras, more airport screening devices, and so forth) may actually make citizens feel less secure. Equally, there are growing concerns in civil society about the emergence of a "surveillance society" and the threat to individual liberties.

The increasing emphasis on societal resilience may also lead to a change in budget priorities. In the course of our interviews with stakeholders, we have noted that in some countries – the UK is one example – there is a growing question as to the appropriate level of investment in security

[89] FORESEC official web page: http://www.foresec.eu/

technologies. There are some analysts, also in the government, who argue that further investment in security technologies may become increasingly redundant. There may be diminishing marginal returns to ever greater investments in terms of increased security. Indeed, there may be a "tipping point" beyond which ever greater investment in security technologies may actually make citizens feel more vulnerable and less secure, not least because of the consequences for civil liberties.

This means that investments in security technologies may slow. Equally, the growing emphasis on societal resilience may also lead to a change in budget priorities away from further technology investment towards more investment in societal resilience. There is already discussion of such a strategy in the UK, where there have been major security concerns around the threat of so-called "home-grown" terrorists and the root causes of radicalisation. The consequence may be a shift of emphasis to understanding and tackling the causes of extremism.[90]

Another consequence of the emphasis on societal resilience may be a shift in priorities within research programmes. Technology projects will continue to take the overwhelming share of security research programmes in the future, not least because they are much more resource intensive than social science and behavioural science projects. However, if the societal resilience agenda is taken seriously, we might expect social and behavioural sciences to receive an increased share of research budgets. Equally, we might expect technology projects to become more multidisciplinary and include as part of their projects an explicit investigation of the societal, behavioural and/or civil liberties implications of these projects.[91] This is a point that we will pick up again in our recommendations, particularly with respect to the Security Research theme of 7th FP.

[90] Comments suggest that there may be different interpretations of the notion of "societal resilience" as used by the European Commission and by some Member States. It is therefore important that future dialogue on this policy issue is aware of such definitional ambiguities.

[91] 7th FP projects already include a formal analysis of potential ethical issues during the evaluation process. However, we have in mind here something that goes further and builds in active research on societal and ethical issues into each project and through the life of that project. This would likely make projects more multidisciplinary to the extent that social scientists would more commonly work alongside physical and life scientists in such projects.

2.10. Conclusions

This chapter has pointed to technology as one of the main drivers of the blurring of the dividing lines between security and defence. The chapter has emphasised that there is a growing application of some types of technology in both the defence and civil security missions. This increased blurring is particularly evident in ICTs, technologies that underpin UAVs and sensor technology and components.

In a next step, the analysis has shown that European companies have strong capabilities in some technologies, including sensor technology and components, communication technologies, and nanotechnologies. We have identified computing technologies and energy storage and distribution as areas of European weakness. In addition we have pointed to a number of emerging technologies, which are likely to gain larger significance in the future such as nanomaterials, autonomous self-organised networks of smart sensors, or semantic web technologies.

We have surveyed the activities of four Member States: France, Germany, the UK and Italy. Only France and the UK undertake dedicated steps to benefit from synergies between security and defence research efforts and, even here, this is only slowly emerging and in only a few areas. Most countries face institutional challenges to the development of such synergies between security and research programmes.

3. Characteristics of demand in the blurred area between security and defence

This chapter analyses the nature and structure of security and defence customers. It explores how these characteristics impact on the demand for technology and equipment in the blurred area between the defence and security sectors, as identified in Chapter 1.[92]

3.1. Structural differences in demand between the security and defence sectors

Structural differences in demand between the two sectors of defence and security exist both at national and European levels.

At the national level, there is generally only one defence customer, the Ministry of Defence. In contrast, security customers are highly diversified between both public and private entities and are therefore more difficult to identify: i.e. central and local governments, infrastructure operators such as airport companies, rail operators, maritime institutions, telecommunications operators. At national level, security demand therefore remains extremely fragmented.

The same is true at European level. In the defence sector, intergovernmental cooperation has emerged bilaterally and multilaterally and at European level, evidenced by the creation of the EDA. Such cooperation covers research, development and procurement activities. In contrast, security customers have not yet engaged in the same process, despite some initiatives taken at national level by some governments to better coordinate their action. The European Commission is encouraging such pooling in the research area through the European Security Research programme, but no common demand in terms of programmes or equipment procurement is yet emerging.

[92] For a clearer picture of the main defence and security customers involved in blurred missions see Annex 2.

3.1.1. Defence demand in the blurred area between the two sectors

Demand in the defence sector of each country studied in this report comprises one single actor at the national level: the Ministry of Defence (MoD). Defence demand therefore remains extremely centralised, concentrated and structured at the national level, despite the process of cooperation and coordination launched by European MoDs more than a decade ago to face budgetary pressure and to support interoperability between European armed forces.[93] As the sole actor on the demand-side, the MoD strongly influences, either directly or indirectly, all aspects of the industry, including overall management of the definition of requirements, research policy, management of defence programmes, procurement of equipment and industrial policy.[94]

The evolution of the strategic environment, described in Chapter 1, has had a significant impact on the evolution of defence demand. Along with the management of traditional defence missions (i.e. deterrence and defence of territorial and national interests), MoDs have increasingly started to be involved in crisis management, stabilisation, peace-building, peacekeeping and civil protection operations, as well as in "High-end" security missions such as border security, counter-terrorism and maritime security.

In **Crisis Management** operations, it is often the case that military forces support security and stability operations and also perform advisory activities for National Army and/or National Police forces of third countries affected by the crisis. In **Civil Protection** and **Support to Civil Protection** missions, they generally provide logistic support to Civil Protection and conduct transport and restoration of vital functions and tasks.[95] In **Border Security** operations, Navies typically carry out patrol, surveillance and interception activities in blue waters, while in **Critical Infrastructure**

[93] The creation of OCCAR, in 1996, launched the European intergovernmental cooperation in the defence sector. The establishment of the EDA in 2004 provided such cooperative efforts with a well-defined EU institutional framework and, in particular, with a wider range of competencies and tasks.

[94] See: In the UK, *Defence Industrial Strategy* (2005), *Defence White Paper* (2009), *Defence technology strategy* (2006). In France, *Plan prospectif à 30 ans* (2005) and *Politiques et Objectifs Scientifiques* (2008). In Germany, *Gemeinsame Erklärung des Bundesministeriums der verteidigung*" (2007) and *Ausschusses Verteidigungswirtchaft im Bundesverband der Deutschen Industrie* zu Nationalen Wehrteschnischen Kernfähigkeiten. In Italy Segredifesa - Direzione nazionale degli armamenti is responsible for tasks; however, the Ministry for Economic Development is involved as well on a selected number of initiatives.

[95] Typical of this kind of effort is the role of France's Formations Militaires de la Securite Civile (ComForMiSC).

Protection and **Protection against terrorism,** national armed forces are generally marginally involved, rather providing logistic support and infrequent surveillance tasks.

As a result of these new roles, the technological needs and equipment requirements of military forces have also evolved. MoDs increasingly tend to use defence-origin technologies that are used also for "High-end" security purposes (i.e. sensors, satellites and UAVs), defence/security technologies (i.e. helicopters, motors, chips and biometrics) as well as security-origin (civilian) technologies (i.e. access control, bio-technologies and information technologies).[96] We have also noticed, however, that in those missions defined as blurred, the equipment used by military and security actors still tends to remain distinct, determined by their different operational roles. As identified in Chapter 1, this can make interoperability difficult between defence and other end-users involved in the same mission.

MoD demand across Europe for equipment that has both military and security application, such as the Athéna-Fidus French-Italian satellite[97], is increasing in response to the results of national research programmes.[98] The reason for this is twofold. First, MoD planners try to optimise value for money by evaluating whether a military or a civilian product could have a dual defence and security application. The second reason is linked to defence sector budget constraints. Finding commonalities between security and defence equipment can widen the field of those customers involved in a programme, thereby spreading budgetary pressure across more investors. This tendency, at least at the political level, can be observed to differing degrees in each of the countries studied for this report. A review of the security and defence research programmes of EU Member States shows that, in some cases, efforts are being made to leverage synergies between investments in defence and security research programmes.

[96] For instance, security companies such as IBM or Fujitsu are increasingly selling very sophisticated high-end products to MoDs. At the same time, in the CBRN sector, an "High-end" security field in which there is a clear technological blurring between security and defence, the British government is funding with a budget of around £10 million a year a cross department science and technology programme, which includes more than 50 projects aimed at strengthening the UK's ability to respond to a CBRN attack.

[97] See Athéna-Fidus webpage: http://www.asi.it/it/flash/navigazione/athenafidus

[98] See the development trends in security research operated by MS defence research bodies in the Annex 3.

In France, the new White Paper on Defence and National Security emphasises that "value for money in the national research budget will be enhanced by the pooling of defence and security research".[99] To reach this goal, the *Conseil supérieur de la formation et de la recherche stratégique* (CSFRS)[100] was created in November 2009. The CSFRS supervises the activities of the IHEDN (Higher Institute for National Defence) and the CHEAr (Centre for Higher Armament Studies)[101] as well as those of the IERSE (Institute for the Study and Research on Corporate Security) and the INHES (National Institute for Higher Studies in Security)[102]. It promotes interaction between different disciplinary fields or areas relating to security, defence and justice and coordinates research efforts to define new strategic views based on the concept of comprehensive security, integrating national defence, public security, corporate protection and environmental security. In addition, the creation of the *Mission pour la Recherche et l'Innovation Scientifique* (MRIS) within the DGA in 2006 is intended to open the defence market to civilian research and products in order to maximise return in the context of the slowing pace of the defence budget.

As stressed above, in the UK there are increasing efforts to promote synergies between defence and security research in some technology areas, with CBRN leading these developments. The MoD's Science and Technology Counter-Terrorism Centre plays an important role in ensuring MoD investment in a range of research and technologies to assist wider counter-terrorism requirements. In the CBRN field, the MoD and the Home Office (MOI) are engaged in deepening cooperation. This is seen as a means of transferring technological knowledge from the MoD's Defence Science & Technology Laboratory to the civil security sector. Finally, C4ISTAR[103] is considered another clear overlapping area for research programmes in the UK defence technology strategy.

[99] *French White Paper on Defence and National Security*, La Documentation Française, Odile Jacob, June 2008, p. 267, http://lesrapports.ladocumentationfrancaise.fr/BRP/084000341/0000.pdf.
[100] See CSFRS official web page: http://www.csfrs.fr/en/home.
[101] The two bodies are going to be merged to create a single defence research centre.
[102] Also these two institutes are going t be merged in order to create a unique "internal security" research centre.
[103] The acronym C4ISTAR stands for command, control, communications, computers, surveillance, target acquisition, and reconnaissance military functions.

In contrast, in Germany there is greater ambiguity surrounding the research and development of defence/security technology. As analysed in Chapter 2, in 2007 the German government launched the first ever national intra-departmental programme of security research. Rather than exclusively focusing on the development of new technologies, however, the programme is spending equal time promoting research into the social dimensions of security.

At European level, pooling security and defence research is extremely attractive to many actors, especially those in the defence environment, for the budgetary reasons highlighted above. Institutional barriers are more constraining than at national level, however. It is therefore practically impossible to pool research investment between defence (EDA for instance) and civilian actors (European Commission). So far, there has nevertheless been an attempt by different EU Institutions to foster the research, development and diffusion of dual-use technologies. Over the last 2 years, for instance, the EDA has launched a number of common research programmes, which could also have application in the security sector. An example of such efforts is the EDA's SDR (Software Defined Radio) project. The study, aimed at developing a technology for secure communications with important potential applications for civilian and military use, is being developed within an ad hoc joint research project (ESSOR) promoted by Finland, France, Italy, Spain and Sweden, under the EDA umbrella. It is aimed at enhancing the interoperability (in Europe and with the U.S. and NATO) of medium-term national SDR projects.[104] Moreover, the EDA is developing capabilities for the protection of borders and the continuity of supply from the maritime environment. Work in this sphere began in 2006 and three main areas of priority have been established by the participating Member States: Maritime Surveillance Network, Unmanned Vehicles Systems (air, surface and underwater) and the identification of small and non-cooperative targets. Many of the EDA's programmes deal with thematic areas also identified by the European Commission as areas of funding for the 7th FP.[105] Such research programmes could lead to cooperative European actions in the future, affecting the pooling of procurement resources by Member States' MODs and MOIs.

[104] See EDA's Software Defined Radio (SDR) official webpage: http://www.eda.europa.eu/genericitem.aspx?area=Organisation&id=115#Software%20Defined%20Radio

[105] See, for instance, projects AMASS, EULER, OPERAMAR, SECTRONIC, WIMAAS. Specific information on each projects is available at: http://cordis.europa.eu/fp7/security/fp7-project-leaflets_en.html

It is still unclear, however, whether such political efforts to pool security and defence research investment could effectively be translated into concrete market opportunities for industry. Identifying future opportunities in terms of common requirements for equipment, joint procurement, or at least the procurement of "security" equipment by MoDs, will be addressed in Chapter 5. Here, we will identify whether this tendency has in reality already started or not.

The overlap between security and defence demand that we have identified at national and European level remains a limited factor in defence procurement. In general terms, defence demand is more significant in quantitative and qualitative terms than security demand. France is a case in point, as in 2009 the MoD's equipment budget was estimated at 8.2 billion euros[106], while the MOI's equipment budget accounted for roughly 1 billion euros.

Compared to demand in the security market, defence demand continues to be characterised by an emphasis on performance rather than cost, even though budgetary pressures have reduced this tendency. Although it is true that there are already relevant examples of procurement of security equipments by defence actors, military equipment, such as satellites, radar systems and security software, dominates budget spending compared to dual-use products. Indeed, since the end of the Cold War, using COTS components has become increasingly common practice, although it is still not widespread in the culture, structure or processes of most military organisations. The best example of such trends is the IT sector, in which civilian technologies have become more advanced than military ones. This has pushed national MoDs to accept civilian or security technologies and adapt some of them for sensitive and complex military purposes (see the case of the Eurofighter battle management system). In the fields of detection, surveillance, engineering and biotechnologies, more and more COTS technologies are selected by MoDs. In 2006, for example, the French MoD started to procure civilian infra-red detection systems from Sofredir and Ulis, two civilian companies, while considering partnership with Stmicroelectronics, Radial and Soitec, to see how civilian components could be integrated into defence equipment.

[106] *Projet de Loi de Finances 2009 – Budget de la Défense*, p. 42.
Available at: http://www.defense.gouv.fr/defense/content/download/129788/1135476/file/PLF%202009%20-%20Budget%20MINDEF.pdf

Increasing demand of dual-use and COTS equipment from the defence side therefore appears to be a potential driver for blurring.

3.1.2. Security demand in the blurred area between the two sectors

As has been recalled in the introduction to this chapter, the security sector has a far more diverse range of customers than defence, spanning both the public and private spheres. They generally fulfil two kinds of security missions:

- traditional security missions, mostly related to law enforcement and public order;
- new security missions related to the post Cold War and post 9/11 security and strategic context ("High-end" security). These new missions are in the blurred area between defence and security (see Chapter 1).

3.1.2.1. Public security customers

As already highlighted in Chapter 1, several customers and actors are involved in the different missions considered as blurred, largely contributing to the extreme fragmentation which characterises public security demand.[107]

In **Crisis Management** operations abroad, security actors operate alongside military forces to implement stabilisation strategies, in particular acting as first responders or supporting nation building and reconstruction.[108] Gendarmerie-type forces, such as the Italian Carabinieri, the French Gendarmerie Nationale, the Dutch Royal Marechaussee, the Romanian Gendarmerie, the Spanish Guardia Civil and the Portuguese National Republican Guard, all perform military police operations; at the same time, the abovementioned gendarmerie-type forces are deeply involved in training activities, contributing to the establishment of third country national police and security

[107] Due to the scarcity of official information on their operational activities, intelligence agencies and secret services, are not included in the list.
[108] For instance, supporting through advisory and training activities towards National Police forces of third countries affected by the crisis.

forces. Training efforts are carried out also by other security actors such as Customs and Revenues police forces (i.e. the Italian Guardia di Finanza) and National Traffic police agencies.

A significant number of public security customers are also involved in **Civil Protection** and **Support to Civil Protection** missions. Fire brigades, such as the Portuguese Bombeiros, the Belgian Services d'Incendie, Luxembourg's Services de Secours and the Italian Vigili del Fuoco generally carry out Search & Rescue (S&R) activities, while police forces, such as the Spanish Cuerpo Nacional De Policia - Servicio De Medios Aéreos, the Portuguese Policia Maritima and the Italian Polizia della Montagna, intervene in support of S&R activities according to the different situations in which Civil Protection procedures are required. In addition, Coast Guard forces (i.e. Spain's Guardia Civil, Italy's Guardia Costiera and Sweden's Kustbevakningen) provide logistic support in the maritime environment, while Local Police units (Polizia Locale e Provinciale in Italy, Police Municipale in France, Policia Municipal in Spain and Politia Comunitari in Romania among the others) provide basic organisational support in proximity to the theatre of intervention.

Protection against terrorism activities involve a large number of security forces, each performing different roles in the effort to prevent and combat terrorist threats to European security.

- Police special forces, such as the British Serious Organised Crime Agency (SOCA), the Spanish Grupo Especial de Operaciones (GEO), the Italian NOCS, the German GSG 9 der Bundespolizei, the Portoguese Grupo De Operações Especiais and France's National Gendarmerie Intervention Group (GIGN), Police Recherche Assistance Intervention Dissuasion Unit (RAID) and National Police Intervention Group (GIPN), generally carry out special, covert interventions during terrorist attacks, and protect sensitive targets (both people and structures) from terrorist activity.
- Police bomb squads, such as Spain's Grupos Operativos de Desactivación de Explosivos, Italy's Artificieri or Portugal's Centro de Inactivação de Explosivos e Segurança em Subsolo (CIEXSS), manage explosive materials in the case of potential terrorist attack.

- Health and scientific police units, such as Spain's Policia Cientifica and Grupo Operativo NBQ as well as Italy's Servizio Sanitario della Polizia di Stato, provide medical support in the case of bioterrorist attack.
- Investigative police units constantly monitor and evaluate terrorist threats, supported in these tasks by information police units who provide computer-based assistance to their investigative and operational activities.

Alongside national police forces, other relevant security actors operate to prevent, reduce or mitigate terrorist threats: security authorities such as the UK's National Counter Terrorism Security Office (NaCTSO), Sweden's Säkerhetspolisen and Italy's Guardia di Finanza Sezione Anti Terrorismo Pronto Impiego and Unità Cinofila Anti Contrabbando e Antiterrorismo cover a wide range of security operations, including monitoring immigration, investigating financial links to terrorism, counter espionage and surveillance activities in airports, ports and rail stations. Also, Civil Protection and Fire Brigades intervene to counter terrorist threats: the former generally act as first responder in the event of CBRN attack, providing medical support and the detection of dangerous materials; the latter are generally support end-users involved in the event of non-conventional risks, such as terrorist acts involving the use of nuclear, biological radiological and chemical weapons.

The type of security actors involved in **Border Security** operations depends largely on the environment in which tasks are carried out.

- In maritime environments, maritime police forces, such as France's Gendarmerie Maritime, Italy's Polizia del Mare and the UK's Port of Dover and Port of Liverpool Police Forces carry out surveillance, positioning and interception tasks in brown waters, while Coast Guard bodies (German Küstenwache des Bundes, Italian Guardia Costiera, Spanish Guardia Civil and Swedish Kustbevakningen) generally perform patrolling and interception activities in both blue and brown waters, as well as constant monitoring and surveillance of national coastlines.[109]

[109] All these bodies integrate the typical Navies' patrol, surveillance and interception activities in blue waters.

- Custom and Border security forces, such as the French Direction Centrale de la Police aux Frontieres, the UK Border Agency (UKBA), the Rumanian Poliția de Frontieră and the Italian Polizia dell'Immigrazione e delle Frontiere and Guardia di Finanza – Servizio Aeronavale are tasked with combating illegal immigration. These bodies are also, at times, charged with coordinating the different security authorities (i.e. Local Police) involved in such tasks. In their efforts, these agencies are also supported by special units of the National Police forces, such as the Spanish Servicio de Medios Aéreos and the Italian Polizia Reparto Volo.

Critical Infrastructure Protection is a complex category of security tasks that involves a huge number of public security actors.

- National Police forces are deeply involved in maximising the security of critical infrastructure.
- Rail police, such as France's Service National de Police Ferroviaire, Italy's Polizia Ferroviaria, and UK's British Transport Police are in charge of surveillance and monitoring on railways and stations. Also, the Spanish Guardia Civil performs this kind of task.
- Communication and Investigation Police bodies (Italy's Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) and Sweden's Säkerhetspolisen Information and Communication unit) perform information-based intelligence activities, data and info gathering and analysis for prevention purposes thanks to *ad hoc* computer and communications assets.
- Custom and Border security forces (French Direction Centrale de la Police aux Frontieres, the UK Border Agency (UKBA), the Rumanian Poliția de Frontieră and the Italian Polizia dell'Immigrazione e delle Frontiere) are involved in infrastructure protection, focusing in particular on surveillance activity in large ports and international airports.
- Police Marksman units as well as Bomb and Dog Squads are involved in the protection of critical infrastructure during public protest marches or events, while Police Health and Scientific units (Italy's Servizio Sanitario della Polizia di Stato Policia, France's Police Scientifique and Spain's Policia Cientifica and Grupo Operativo NBQ) provide medical and scientific support in the event of biological or chemical attack to critical infrastructure.

Alongside police forces, other actors contribute to the security of critical infrastructure. For instance:

- Port security bodies such as the Port of London Authority, Port of Dover and Port of Liverpool Police forces, Italy's Capitaneria di Porto and single local port authorities are in charge of ensuring surveillance and monitoring of activities within ports and their vicinities.
- Anti-Hacking units, such as the Italian Guardia Di Finanza - Nucleo Speciale Frodi Telematiche and the Spanish Brigada de Investigación Tecnológica, provide the defence of critical information systems against cyber–attacks and information fraud.
- The British National Counter Terrorism Security Office (NaCTSO) offers this kind of information protection to critical and sensitive national infrastructure.
- Finally, Fire Brigades and Civil Protection agencies contribute to the protection of critical infrastructure. Fire Brigades carry out monitoring, inspection and prevention activities against fires and industrial risks, as well as mitigation activities in the event of fire, uncontrolled release of energy and risks deriving from the use of nuclear, biological, radiological and chemical substances. They are also ready to intervene in the event of non-conventional threats, such as terrorist or criminal acts against infrastructure with the use of nuclear, biological radiological and chemical weapons. Civil Protection provides first response aid in case of attack or accident, mainly carrying out medical support and detection of dangerous materials.

The procurement policies of these security forces are managed by both central national institutions and local governments, often without a sufficient degree of institutional coordination. In fact, in the highly fragmented environment described above, bureaucratic politics and inter-departmental rivalries act as a further obstacle to closer cooperation. For this reason, none of these institutions has the same influence over industry as defence institutions in activities such as the definition of requirements, research policy, the management of programmes and the procurement of equipment.

At the national level, MoIs are the major, but not the only, public security customer, driven primarily by the need to provide technological equipment to their security forces. Also local authorities (i.e. Laender, counties, Regioni, Provinces, metropolitan districts) act independently as the customer for their own public security forces, procuring specific technologies and equipment.[110] But the culture of both MoIs and local authorities relies more on manpower than on technology. As a result, when compared to MoDs, they have not set up well defined procurement processes and have not established agencies in charge of managing security programmes. As stressed by an official document of the British Association of Chief Police Officers (ACPO), "police procurement units are not always able to shape effectively business requirements for goods and services. Too often, the involvement of procurement professionals is reactive".[111] The evolution of MoI demand for more technologically sophisticated equipment strongly depends on their growing involvement in missions in the blurred area between defence and security. In fact, as clearly appears from the description of security actors' roles and tasks performed in crisis management, counter-terrorism, border security and critical infrastructure protection missions, they increasingly require sophisticated technologies and equipment.[112]

Demand for security equipment within the blurred area remains fragmented because of the dispersion of demand across different national public administrations. This creates difficulties that can be illustrated by referring to what is happening in the area of maritime surveillance. The examples of France and Germany, who have very different systems of governance (centralised and

[110] In the UK, for instance, the procurement of equipment is undertaken separately by each of the 43 police forces in England and Wales.

[111] British Association of Chief Police Officers (ACPO), *National Procurement Strategy to 2011*. Available at: http://www.nypa.gov.uk/CHttpHandler.ashx?id=2730&p=0

[112] These include technologies and equipment that may be used in all these missions and others that have specific application in one/some of them. The former include data management software and system integration solutions; integrated satellite and radar-based systems; command and control systems; integrated Professional Mobile Radio (PMR) and Software Defined Radio (SDR) systems; bio surveillance systems; heat cameras and further identification equipment. Others, suited for critical infrastructure protection tasks, include advanced technology checkpoint X-ray and CastScope X-ray; biometrics sensors (i.e. retinal scans and fingerprint identification tools); bottled liquid screening systems; Explosive Detection System (EDS) machines; Explosives Trace Detection (ETD); biological, radioactive and nuclear detection system; Personal Radiation Detectors (PRDs) and Fixed Radiation Portal Monitors (RPMs); active and passive Radio Frequency Identification Device (RFID) tags; access control and perimetral systems. Still others specifically fit for border security tasks in maritime environment, include vessel tracking systems such as Automatic Identification System (AIS) and Long-Range Identification and Tracking system (LRIT); scanning equipment for containers (i.e. explosives and nuclear/radiological screening); container tracking equipment; and container seals and identification equipment.

Federal), are particularly revealing. In France, responsibilities for this mission are divided among six different structures and budgets.[113] The case is similar in Germany, where six different structures are also called upon.[114] In both cases coordination between agencies in charge of security continues to be quite poor and no central procurement agency is helping to unify, or at the very least streamline, the demand. Moreover, contacts between public officials and private companies remain limited and there is no real R&D culture, despite the fact that security is a growing challenge for Member States, often requiring increased availability of advanced technology and equipment.

At the local level, some institutions, such as the *Laender* in Germany and local governments in France, Italy and the UK, are also security product customers, particularly for, but not limited to, monitoring, communications and cyber-security equipment. There is a general lack of coordination at this level too, with some exceptions, such as in Germany where we can see emerging coordination among the *Laender*. In other countries, regional security demand is characterised by a higher level of fragmentation. Italian security agencies are highly fragmented between the national, regional, provincial and local levels, with different institutions playing the leading role for different forces.[115]

[113] Ministry of Foreign Affairs (Direction of military and defence cooperation), Ministry of Interior (French Maritime Prefect, National Gendarmerie, Civil Security, National Police), Ministry of Ecology, Energy, Sustainable Development and Sea (Direction of Maritime Affairs, within the General Direction of Infrastructures, Transports and Sea), Ministry of Defence (French Navy), Ministry for the Budget, Public Accounts and the Civil Service (Customs), Prime Ministry Services (General Secretariat of Sea).

[114] In Germany, responsibility for maritime security rests with the Coast Guard, an association of several federal and Laender law enforcement agencies, whose primary missions are border protection, maritime environmental protection, shipping safety, fishery protection and customs enforcement. The Coast Guard association brings together police and military officers as well as civil personnel: Federal Police, responsible for domestic waterways; Ministry of Defence for security beyond the area of 12 nautical miles from German shores; Water protection police, responsible for security up to 12 nautical miles from the country's shores and part of the police of the Bundeslaender such as Bremen, Hamburg, Lower Saxony, Schleswig-Holstein, Mecklenburg-Vorpommern; Maritime Customs Service, Federal Customs Administration, Federal Ministry of Finance; Federal Agency for Agriculture and Nutrition (BLE), Federal Ministry of Consumer Protection, Food, and Agriculture.

[115] In Italy, Polizia Municipale, Polizia Provinciale and Polizia Regionale are three different bodies all concurrently in charge of ensuring security at the local level.

This kind of fragmentation damages the emergence of a coherent security market, thus acting as an obstacle for the convergence of security and defence demand. This limits the blurring of boundaries between the defence and security sectors.

We can, however, identify a few examples of efforts to reduce the fragmentation in the security sector, or at least to centralise procurement. In the UK, the central procurement of "Airwave" (national police radio system) and "Fire Control" (infrastructure for nine regional control centres) brings together previously fragmented approaches to police and emergency services operational requirements and system/equipment procurement. The Home Office is responsible for counter-terrorism policy and the lead for domestic security lies with the civil agencies, particularly with the police. Nevertheless, "there may be plans for a 'single budget' for counter-terrorism and security, but this is likely to be at best the sum of the parts rather than an accountability mechanism".[116] In Germany, the acquisition of a single digital radio system, the BOS, for all Federal and *Laender* police, disaster relief forces, fire fighters, rescue services, customs authorities and the domestic intelligence services is another example. However, these cases represent the exception to the general rule of fragmentation among actors and procurement decision-making.

The European Union is not a customer of security equipment per se, but has responsibility for helping Member States coordinate their needs via the launch of research programmes in the defence and security domains. As analysed above, the EDA manages several R&T projects related to defence research, which may also be applicable to the security sector. The most important role in this area is played, however, by the EU Research Directorate General. The 7th FP, the European Union's main instrument for funding research in Europe, includes a programme on security, whose total allocation is 1.4 billion euros, as well as a programme on space.

At the EU level, "the relationship between defence technologies on the one hand, and security technologies on the other, is particularly noticeable in the field of R&D, with technologies that show potential developments in both areas. At both research and industrial development levels,

[116] UK House of Commons, Defence Committee - Written Evidence: *The Defence contribution to UK national security and resilience*, Memorandum from Fujitsu Defence and Security, 5 May 2009.

synergies are possible and desirable".[117] The 7th FP on security research, by providing co-financed research action between the European Commission and the industry, has considerably stimulated private supply in this area.

Under the Third Pillar there are several initiatives aimed at coordinating European security policy: Eurojust, for the coordination of Member States' national public prosecution services, Europol (European Police Office) which aims to improve cooperation between the states' police and customs authorities and the European Judicial Network, whose goal is to foster mutual judicial assistance. Other European agencies, each with their own legal status, also play a role in coordination: Frontex, dealing with border security, and the European Maritime Safety Agency (EMSA), aimed at enhancing a European maritime safety system.[118] The recent entry into force of the Lisbon Treaty offers a significant opportunity to foster the role of the European Commission and European agencies in driving demand in the security and defence fields and, as a consequence, in the blurred area between the two.

In this context, two Frontex initiatives have to be highlighted. First is the CRATE system (Centralised Records of Available Technical Equipment for control and surveillance of external borders), which shows that the EU Agency already has an important role to play in harmonising the demand of security products. CRATE consists of centralising a database of equipment for the control and surveillance of external borders (aircraft, helicopters, ships and surveillance equipment) that the Member States are willing to put at the disposal of another Member State for a temporary period (on a voluntary basis and upon request from another Member State). It contains "for the moment over a hundred vessels, around 20 aircraft and 25 helicopters and several hundreds of border control equipment, such as mobile radar units, vehicles, thermal cameras and mobile detectors".[119] According to the Brigadier General Ilkka Laitinen, Executive Director of the European border management agency Frontex: "CRATE is only a record that will

[117] European Commission, 7th Research and Development Framework Programme, Security Research Projects, *Towards a more secure society and increased industrial competitiveness*, May 2009. Available at: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf

[118] European Maritime Safety Agency official webpage: http://www.emsa.europa.eu/end173.html

[119] *The Frontex Agency: evaluation and future development*, MEMO/08/84, 2008. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/84&format=DOC&aged=0&language=EN&guiLanguage=en.

help us in better planning Frontex operations. CRATE is like an e-shop, you can watch it on your screen and decide what you need, then order it and pay for it. Frontex doesn't have any vessels itself and cannot afford deployment of a big number of units to a chosen region. These assets belong to the Member States and they are subject to their will to deploy them".[120]

Second, in order to enhance its reaction capacity, the Agency has also launched the SeBoCom project[121], in cooperation with the Sensors, Radar Technologies and Cybersecurity (SERAC) Unit of the Joint Research Center-Institute for the Protection and Security of the Citizen (JRC-IPSC). The project's main goal is to provide European Border Forces with an effective, reliable, interoperable communications system capable of ensuring secure operational transmission of voice and data. At present, SeBoCom partners have carried out a pre-study of relevant end-user operational activity. With respect to its current activities, the Agency, if provided with an adequate budget and consistent powers, could become the catalyst for demand harmonisation in the European border surveillance security segment. Frontex could be charged with setting common procurement standards, which is within its field of competence: however, the role of Frontex as a catalyst for security activities would make it also suitable to this task. The Agency could act by centralising procurement activity, commissioning significant R&D efforts and, potentially, also developing cooperation with defence actors also having responsibility in this area, in particular the surveillance of maritime borders. All these activities, however, would require a political decision to expand Frontex's remit.

In conclusion, public security demand is highly fragmented, both at European and national levels. This is clearly a barrier to the development of blurred security and defence demand. There is, nevertheless, the potential for coordinated European public demand for some security products, in particular for those related to missions that have a continental dimension, such as border control, the protection of critical infrastructures and civil protection.

[120] Frontex official webpage: http://www.FRONTEX.europa.eu/newsroom/news_releases/art26.html
[121] SeBoCom (**Se**cure interoperable **Bo**rder **Com**munications) official webpage, http://sta.jrc.ec.europa.eu/index.php?option=com_content&view=article&id=40:sebocom-project&catid=25:corsa-action-&Itemid=27

3.1.2.2. Private security customers

With "private security customers" we refer to operators and entities involved in strategic sectors (i.e. crisis management missions abroad, infrastructure protection), rather than to the multiplicity of small customers which are very difficult to identify and operate on a scale too small for the scope of our analysis. Private security customers have very different commitments, requirements and therefore procurement logics from national public security authorities.

Although less involved than public security actors in the identified blurred mission, the role of private security actors is increasing.

During **Crisis Management** operations abroad (i.e. Afghanistan and Iraq), Public Security Companies (PSC) or Public Military Companies (PMC) perform personnel and asset protection tasks and bodyguard services. These companies are often tasked with so called "force protection" missions, meaning protecting the security of military bases. This task would normally be performed by the military themselves, but due to the shortage of personnel available for missions abroad, this role is increasingly assigned to private companies. PSCs/PMCs procure their equipment on the free market, the only limit being set by the law. Usually, security equipment procured by a PSC includes nothing more than armoured vehicles (often civilian vehicles modified by local enterprises), small weapons and GPS communications. However, at least within the EU framework, no PSCs/PMCs are involved in either security and stability operations or military police activities.[122]

Other private actors involved in crisis management operations are companies specialised in logistic services for the armed forces, such as catering, food supply and distribution, construction and management of facilities. These actors are not security providers strictly speaking, however, and do not need to acquire security equipment, as the security of their personnel on the ground is guaranteed by the client.

[122] A. J. K. Bailes and C. Holmqvist, *The Increasing Role of Private Military and Security Companies*, Directorate-General for External Policies of the Union, European Parliament, 2007.
Available at: http://www.europarl.europa.eu/activities/expert/eStudies.do?languageEN

The role of private security actors is expanding in **Protection of Critical infrastructure** missions. The security of ports, airports and stations, as well as that of rail and subway systems, oil and gas assets, energy grids and water distribution networks is increasingly dependent on the private market. This model generally leads to two distinct trends. On the one hand, companies owning or managing critical infrastructure or sensitive assets have developed internal Security Divisions in charge of maximising the protection of their property: such Divisions usually control integrated security systems in cooperation with IT providers (i.e. Microsoft, Cisco and IBM). On the other hand, companies owning or managing critical infrastructure or sensitive assets tend to outsource to private security companies the physical protection of their properties: these companies are mainly involved in tasks such as access control, remote CCTV monitoring and visual verification, mobile patrolling and installation surveillance, GPS tracking and the control of vehicles. Private security actors are all very different, some being small, local companies providing exclusively security manpower, while others are large integrated groups (i.e. UK's First Security[123] and Europa[124]) with several millions euros of revenues and thousands of employees, offering a huge portfolio of security-related services, as well as non-security support (i.e. maintenance, reception, site testing). In the first case, security companies generally rely upon technologies made available by infrastructure owners (which thus remain the main equipment customer), while in the second case, large private security companies act directly as customers of security technology and equipment, offering integrated support and protection services to infrastructure owners.

Critical infrastructure stakeholders interviewed for this report acknowledged that the bulk of their security expenses relates to security services (security guards), low technology equipment (mainly CCTVs) and IT security. Equipment in areas such as biometry or other access controls are mostly of interest to operators who do not have direct contact with their clients. For example, travel infrastructure operators (i.e. railways) tend to avoid access control measures, where possible, for fear of damaging their attractiveness. However, an important distinction should also be made between companies owning or managing critical infrastructure who voluntarily invest in security, and those purchasing security equipment and recruiting security staff in order to comply with

[123] See official web page: http://www.first-security.co.uk/home/
[124] See official web page: http://www.europa-services.co.uk/home.aspx

international standards and regulations. By imposing on infrastructure operators both security measures and equipment requirements, regulations (in particular European ones) will help define a consolidated demand for technology and equipment. This is the case, for instance, for airport security, which is regulated by a series of conventions and documents issued by the International Civil Aviation Organization (ICAO). In particular, Annex 17 on "Security Safeguarding International Civil Aviation Against Acts of Unlawful Interference" provides binding organisational procedures that each Member State has to implement in order to deal with aviation security matters. It also requests the definition of National Security Plans. In addition, Annex 17 requires States to identify competent national authorities[125] in charge of adopting and implementing such security procedures and set up measures to: prevent illegal activities; control passengers, crews, baggage, goods and airmail; manage the access, circulation and permanence of people in airport areas; manage emergency situations. The adoption of the provisions of Annex 17 has been recommended in the European Civilian Conference (ECAC) Document 30, which was enforced by the European Parliament and the Council of the European Union in 2002 through the adoption of EC Regulation 2320/2002.[126] Further rules, such as EC Regulation 1546/2006, have been introduced by European lawmakers over recent years in order to respond to emerging security needs.

These rules not only apply to public airport operators, but also to private ones. A case in point is the management of Napoli-Capodichino's airport, which has been acquired by the BAA group, while the GESAC company (a BAA subsidiary) is in charge of the terminal's management.[127] Among other activities, GESAC is totally responsible for airport security and invests part of its 18 million euro budget to standardise its security systems to the levels set up by international, European and national regulations, as well as by agreements signed by the Italian government. In the wake of the failed 25/12 terrorist attack, the Italian government agreed to start a gradual instalment of body scanners in its national airports, forcing GESAC progressively to introduce such devices in its terminal.

[125] Such as the Department of Transport in the UK, the Ente Nazionale per l'Aviazione Civile (ENAC) in Italy
[126] EC Regulation n. 2320/2002 of the European Parliament and of the Council, adopted on 16 December 2002 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:355:0001:0021:EN:PDF
[127] See GESAC official webpage: http://www.portal.gesac.it/portal/page/portal/internet/inGESAC/Profilo

At the same time, the activity of private port security operators (as well as public ones) is regulated both by international and European regulations. The International Ship and Port Facility Security Code (ISPS Code), drawn up in the aftermath of the 9/11 terrorist attacks by the International Maritime Organization (IMO), provides binding security standards as well as procedural recommendations for port facilities and vessels. Also the EU, according to ISPS provisions, has approved ship and port facility security regulations[128] as well as amendments to the Community Customs Code.[129]

The examples of airport and port security shows that in certain segments of infrastructure protection, there is already a fair degree of common regulation, at least at the performance level. In other domains, however, such as rail and subway transport systems, regulatory efforts (both for the definition of operational performance and for the identification of technical standards) remain minimal. Therefore, in the absence of common international or EU-wide solutions, the definition of performance requirements and technical characteristics for security equipment continues to differ between Member States or user groups. This serves to reinforce recurrent problems with interoperability between private security forces operating in the same context, and is further contributing to the fragmentation of private demand, even in sectors in which common capability requirements might emerge and the same equipment could, in fact, be used to fulfil operational requirements.

Moreover, each of these actors has different procurement practices and legal constraints. Private security forces, obviously, do not have to comply with European regulations on public procurement and can freely acquire equipment from whatever source they prefer, within the limits imposed by national laws (clearly, no private entity is allowed to buy weapons bigger than small arms). Public actors, however, do have to comply with national and European regulations for their procurement needs. These differences, which could have an influence on the blurring phenomenon, are analysed in the following paragraph.

[128] Regulation n. 725/2004 on enhancing ship and port facility security, and Directive n. 2005/65/EC on enhancing port security
[129] Through Regulation n.648/2005 and Regulation n. 1875/2006.

3.2. The effect of institutions and regulations

Regulatory frameworks generally affect market structures. Consequently, it is essential to analyse how European and national institutions regulate defence and security markets and investigate how regulation and norms do or could better shape, define and segment the current and future blurred market.

This section of the chapter focuses on the effects of the part of the Defence Package proposed by the European Commission which focuses on procurement[130] and on the role of the standardisation process in the definition and segmentation of the defence and security markets. It also investigates the potential effects of recent institutional developments within the European Union, introduced by the Lisbon Treaty.

3.2.1. Procurement rules in the defence and security sectors

The blurring of demand appears to be limited not only by different procurement approaches across the security and defence sectors, but also within each sector. The defence sector has traditionally procured large, complex systems that are specified in detail by the defence customer and developed in large part through government defence R&D contracts. Historically, in the defence sector, MoDs have been significantly involved in the design and development of new products and decades long development cycles have been the norm.

In contrast, police and security operators tend to prefer off-the-shelf equipment and have a strong demand for the rapid introduction of new equipment. Of course, the increasing involvement of these actors in "High-end" security missions, both abroad and on national soil, represents a stimulus to focus equipment procurement on more sophisticated technologies and goods.

[130] The Defence Package contains three initiatives: the proposal for a Directive on procurement, the proposal for a Directive on intra-community transfers and a Communication on the competitive ness of European defence industries. The latter, in turn, indicated various hurdles which may constrain the strengthening of the European Technological and Industrial Base (EDTIB), and on which the Commission intends to deepen the analysis.

However, from the current security force budgets, it emerges that MoIs invest essentially in low technology products, and even when they purchase tailor-made solutions, which may very well represent cutting-edge technologies, such as wiretapping equipment, surveillance goods and IT products, the overall amount of expenditure is still insignificant.[131] The bulk of security force acquisition remains off-the-shelf equipment, which is both cheaper (since development costs are borne by the producer) and easier to buy (the cost of the product is known and the product already available). As a result of this preference for off-the-shelf products, security actors usually do not have "the culture of the programme and it does not seem that this will be the case in the future", as noted by one stakeholder. This approach has to be taken into account when dealing with procurement regulation. Since purchases are generally made off-the-shelf, regulations tailored to the specific nature of the security sector are even more important than in the defence domain.

Moreover, defence and security force procurement are governed by different regulations at the European level.

3.2.1.1. Defence Procurement

In the past, defence and security products for Armed Forces were generally procured under the terms of article 346 TFEU (former art. 296 TUE, hereby art. 346) which allows a public administration to derogate, in the light of established conditions, from Community public procurement rules based on the principal of open competition at the European level . It states that "no Member State shall be obliged to supply information, the disclosure of which it considers contrary to the essential interests of its security". Moreover, the Article also allows Member States to take such measures as considered necessary to protect its essential security interests, which are connected with the production or trade of arms munitions or war material (here the reference is to a list of armaments drawn up in 1958), as established by art 346 TFEU.

.

[131] Off the record interview.

Defence procurement authorities tended to make extensive use of this derogation by procuring most of their equipment (military and non-military) without using the EC Treaty rules and avoiding, therefore, the basic principles of transparency and competition at EU level. This reinforced defence market fragmentation at EU level. Fragmentation, however, was and remains also driven by the particular capability and performance needs expressed by national armed forces (use of large platforms and complex integrated systems, requirement of high levels of deployability) which lead MoDs to invest heavily in the procurement of military equipment. Such significant investment means that MoDs have high expectations for the quality of the equipment they procure. They tend therefore to define the specifications, supervise and control the output of research and development activities. These circumstances create the conditions for a close demand-supply dialogue on procurement matters between MoDs and defence industries.

The publication of the EC Interpretative Communication on the application of art. 346 in December 2006[132] clarified the legal situation. The Communication recalls that procurement for non-military security purposes is excluded from the field of application of art. 346 1b): the list of arms, munitions and war materiel cannot be interpreted extensively. Therefore, the extent to which defence administrations can circumvent regulation has been drastically limited. In particular, the Communication emphasises that derogation has to be considered only as the final option, when application of the European requirement is incompatible with the demands of protecting fundamental security interests. Consequently, derogation can only be invoked on a case-by-case basis and generic derogation, or derogations generically invoked, are not permitted.

In addition, when a derogation does apply, the 26 EU participating Member States of the EDA should follw the EDA's Code of Conduct on defence procurement, other than in some exceptional cases indicated in the Code. This means that defence authorities are expected to publish their tender in a common electronic portal. Originally, the intention was to foster the opening of the market, even in this sensitive defence segment. In reality, however, it had the reverse effect, since Member States have tended to avoid sharing information about foreseen and realised procurement under derogation. Some have speculated that this has led to a wider application of

[132] European Commission, Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement, 7/12/2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0779:FIN:en:PDF.

the 2004/18 European Directive. However there are no data available on whether Member States have further opened their markets as a result of the adoption of the Interpretative Communication. This may become the case in future, with the implementation of the new Directive on defence procurement that will be addressed later in this Chapter.

3.2.1.2. Public security procurement

Public security forces, such as Police and Fire Brigades, have procured equipment in a number of ways. If the equipment to be acquired was civilian in nature (i.e. vehicles), then procurement followed the regular Community regime on public procurement.[133] If the equipment to be procured was specific security equipment (i.e. bullets for police forces), then the administration had four different choices:

- apply the Community regime on public procurement,
- follow art. 346 1a), stating that supplying information about this particular acquisition would be contrary to its security interests,
- use the exclusion of Article 14,
- make reference to art. 346 1b), stating that the item to be procured could be included in the list of arms, munitions and war materiel only in case of essentially military products which are used during essentially military activities (i.e. international missions).

For public security forces, the situation also changed after publication of the EC Interpretative Communication on the application of the art. 346.[134] In fact, as far as security products are concerned, before the adoption of the Interpretative Communication, art. 346 was widely used for procurement coming from non military forces, such as the police. The situation was therefore similar to that of the defence sector. Now, Member States seem to be more open, perhaps for fear that the Commission might adopt a strict interpretation of the article which could lead to the

[133] However, is largely acknowledged that in the past Member States have considered extensively the List of Products of art 346 TFEU and, therefore, they have not applied systematically the European normative. This is, for instance, the case of the helicopters purchased by Italy for its security forces.

[134] European Commission, Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement, 7/12/2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0779:FIN:en:PDF.

opening of infringement procedures. This type of procurement, therefore, has to be launched in compliance with the applicable European regulation. The need for procurement confidentiality seems to be growing in the face of the terrorist threat, but does not justify a systematic use of art. 346. There is, however, a dilemma between the non application of the 2004/18 European Directive, which will negatively affect costs and efficiencies, and its application, which could lead to sensitive information being disclosed. This is one of the reasons why the new Directive on defence procurement has been enlarged to include sensitive security equipment, as will be explained later.

It should nevertheless be noted that, despite security actors making extensive use of the art. 346 derogation to avoid competition at EU level, close demand-supply cooperation in the development of equipment has not emerged. In fact, due to the characteristics of their operational activities, the equipment requirements of security forces[135] are clearly less demanding than those of military forces. Their equipment budgets are lower than those of MoDs, thus limiting the influence that security authorities have in directing industry's technological and management choices. Even when they waive European regulations on public procurement, therefore, such security forces do not always procure equipment developed according to their bespoke requirements, but tend instead to buy off-the-shelf products.

3.2.1.3. The EC defence package and the process for blurring

The defence package was launched by the European Commission to resolve the problem of fragmentation in the defence market at European level. We have referred to this in the previous section on procurement.[136] For the purpose of this study, we will now focus our attention on Directive 2009/81/EC on defence and sensitive security procurement.[137]

[135] Including Police forces, Fire Brigades as well as those hybrid forces such as Carabinieri, Gendarmerie or Guardia Civil.

[136] The package consists of three elements: 1) a communication on a strategy for a stronger and more competitive European defence industry; 2) a proposal for a Directive on Intra-EU transfers of Defence-related Goods, and 3) a proposal for a Directive on Defence and Security Procurement.

[137] The text of the Directive is available at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:216:0076:0136:EN:PDF

This is the first regulation at EC level that clearly recognises the existence of a blurring between defence and security, by providing common rules for public procurement in both markets. The new directive applies not only to arms munitions or war materials, "*but also to certain particularly sensitive purchases in the field of non-military security" (Rec 9).* This wording covers any equipment for which the safeguarding of classified information is required. The association of the "sensitive" concept with equipment, works and services for security is formulated in art 7: "sensitive equipment, sensitive works or sensitive services means equipment, works or services for security purposes involving, requiring and/or containing classified information". This formulation covers a large proportion of security equipment, considered as classified due to its technology content. In practice, information concerning the purchase of civilian or dual-use equipment can be sensitive in itself, meaning that the even the purchase of relatively common equipment may be considered as classified information: for instance, the number of mobile phones purchased by a national security authority may be considered classified or sensitive information.

With regard to boundaries between defence and security procurement, the text of the new Directive states that: "*These procedures should reflect the Union's overall approach to security, which responds to changes in the strategic environment. The emergence of asymmetrical transnational threats has increasingly blurred the boundary between external and internal and military and non-military security*." (Rec 7).[138] Recital 11 indicates border protection, police activities and crisis management missions as examples of blurred areas.

The previous directive on public procurement (2004/18/ CE), even though in principle applicable to defence and security procurement, did not sufficiently take into account the specificities of those sectors (in particular as regards specific requirements such as security of supply and security of information or defence research and development). The new Directive, on the other hand, provides a set of flexible rules tailor-made for both areas. It allows for the possibility of the negotiated procedure to be generally used ,with publication of a contract notice, and also foresees

[138] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009.
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, and amending Directives 2004/17/EC and 2004/18/EC.

defence specific exclusions, such as gov-to-gov contracts. Member States purchasing defence and security equipment can therefore better protect their security of information and security of supply. With regard to Security of Supply, art. 22 of the Directive allows contracting authorities to request a wide number of particulars, related, for example, to export authorisations and restrictions, information on the supply chain, commitments for additional needs in times of crisis and others. With regard to Security of Information, art. 23 of the Directive acknowledges the requirement for national security clearances, but highlights in Rec 9 the need for an EU wide harmonised security of information regime.

The Directive nevertheless still allows Member States to derogate from these new procurement rules on the basis of article 346 TFEUs. The use of the derogation is, however, limited to the following exceptional cases: "*(…) for contracts in the fields of both defence and security which necessitate such extremely demanding security of supply requirements or which are so confidential and/or important for national sovereignty that even the specific provisions of this Directive are not sufficient to safeguard Member States' essential security interests, the definition of which is the sole responsibility of Member States*" (Rec 16). In addition, by stating in recital 10 that the field of application for defence procurement is based on the list of arms, munitions and war material adopted by the Council with Decision 255/58 of 15 April 1958, which is also the basis for the invocation of art. 346 TFEU, the Directive 2009/81 will also have the effect of limiting recourse to this exclusion.

This Directive will probably have a considerable impact on the defence and security market. The new, flexible procurement procedures and limitation in the use of the derogation should increase competition in both fields. The introduction of transparency and competition in the defence market may act as an incentive for civil/security companies to participate in tenders which were previously not even made known. The market will therefore not only be more open to defence companies, but also to civilian companies.

In conclusion, we consider that the application of this directive should enable the supply of defence and security products to be better managed by Armed Forces and security forces, giving them a specific tool designed for the specificities of each sector. By increasing demand-side competition, the directive may also have an impact on the European defence and security industrial base. More specifically, by including the security sector in this directive, a legal framework has been created for products in the blurred area.

3.2.2. The role of standardisation in shaping the defence and security markets

Standardisation provides common industrial norms aimed at harmonising a sector and improving the regulation of a market. International standards are a guarantee of better interoperability in a context of growing interdependence due to the internationalisation of market economies. There are two ways of looking at the consequences of a regulated market. On the one hand, standardisation increases competition as it puts various actors, from big companies to SMEs, on an equal footing. On the other hand, if standardisation is highly demanding, then it favours the creation of monopoly situations.

Globally, the United States is currently seen as the standard setter in many markets. This situation is visible in defence, as well as in the Standardization Agreements (STANAGs) process within NATO. There would appear to be a significant opportunity for the European Union to take some leadership in the process of setting international standards, to be able to counter the influence of American industry.

3.2.2.1. Standardisation for defence

For defence, standardisation of equipment and technology is already relatively advanced, as there has only been a single customer, the MoD. The internationalisation of defence policies via the creation of international defence alliances, such as NATO, and the creation of a multinational political framework, such as the European Union, combined with the development of multinational military operations, have created a need for harmonised standards, to enable interoperability between different national armed forces. For security, this process of internationalisation remains less significant, as there is no such organisation for security matters. Nevertheless, even MoDs face

challenges in introducing standards that need to be accepted by all services (air, land and naval forces), such as joint Command & Control (C2) technology, and although standardisation practices in the defence domain are more advanced than for security, even this sector still needs further normative efforts to reach the optimal uniformity of standards.

NATO has been managing this issue for 30 years, through the NATO Committee for Standardization (NCS), an authority on overall standardisation matters. NATO's standards are thus defined through STANAGs, providing the member states of the Alliance with a set of common practices for the introduction of military or technical procedures and equipment. For instance, standards are the basis for technical interoperability between a wide variety of communication and information systems that are vital for NATO and Allied military operations. They have also played a role in unifying the market with, for example, the STANAG 4175 and 5516 for the sharing of tactical data between the Allies' Armies, or for different types of ammunition.

The EU's interest in standards is more recent. In 1999, the study "Standardization Systems in Defence Industries of the European Union and the United States", commissioned by the European Commission and carried out by the University of Sussex[139], raised awareness of the requirement for harmonisation at the European level and pointed out the need for action. Since then, the European Committee for Standardisation (CEN) has fought to improve the competitiveness of the European Defence Industry through standardisation.[140]

In 2004, along with the creation of the EDA, the "Western European Armaments Group (WEAG) Standardisation Team" evolved into the "Materiel Standardisation Harmonisation Team" (MSHT), an independent body working in liaison with the EDA. For the EDA, standardisation facilitates, in particular, collaboration and common solutions to capability gaps. The MSHT is a body composed

[139] The report, know as the "Sussex-Study", is not available but some of its finding are presented in the EDA European Defence Standardization Journal, Issue 2, 2009: http://www.eda.europa.eu/webutils/downloadfile.aspx?FileID=491

[140] Cf. the creation in January 2001 of the BT Working Group 125 (BT/WG 125), who endorsed the setting up of CEN Workshop 10 in charge of developing a European Handbook for Defence Procurement. The European Handbook for Defence Procurement (EHDP) contains references to standards and standard-like specifications commonly used to support defence procurement contracts, as well as guidance on the selection of standards and standard-like specifications to optimise effectiveness, efficiency and interoperability. The second version was published in 2008.

of defence standardisation management experts, working in liaison with the EDA and providing guidance to other organisations on defence standardisation management, such as CEN, the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). Alongside this structured institutional framework, European defence industries have significant experience in the application of standards (both civil and defence) for defence purposes and, therefore, the role they play in the development and application of standards is critical to defence procurement.[141]

As clearly stressed by the Council of the European Union, standardisation of defence equipment is considered an important basis for the "building of a strong European defence industry".[142] At the same time, interoperability and standardisation are seen by the EDA as key elements of capability development for the ESDP.

At present, the main types of standards used by European countries are[143]:

- International standards (ISO, IUT etc.)
- NATO Standards (STANAGs)
- European standards (CEN, CENELEC, ETSI, AECMA, ASD, IMO etc.)
- US Standards (ANSI, ASTM, API, MIL-STD, NSA).

Although all these standards are currently in use, many stakeholders interviewed pointed out that besides national standards, much of the defence industry is adopting United States MIL standards. This appears to be an obvious point of convergence for most, if not all, the suppliers engaged.

3.2.2.2. Standardisation for security

While a standardisation process for defence equipment is already well developed and European armaments cooperation has enabled the rise of common performance and technical standards,

[141] The Study into the Role of European Industry in the Development and Application of Standards, EDA, ref: 08/ARM/003 study performed by ASD/STAN for the European Defence Agency, October 2008.
[142] Council of the European Union, Council Resolution on standardisation in the field of armaments n. 6953/03. Available online at: http://register.consilium.europa.eu/pdf/en/03/st06/st06953.en03.pdf
[143] From the *European Handbook For Defence Procurement*: National procurement structures and procedures, http://www.defense-handbook.org/procedures.php

standardisation (in particular, technical standardisation) for security equipment is still under-developed. States often offer only performance regulatory frameworks for security equipment, without providing specific technical standards, slowing down the harmonisation of technologies and equipment among private operators, as well as among public security forces (local forces in particular). Moreover, when a State's agencies purchase security components and equipment, they generally procure off-the-shelf products, unlike defence sector products that are specifically developed for Armed Forces, with technical specifications usually defined by the customers (Armed Forced and MoD).

As a result, the process of standardisation is less evolved in the security sector, although we should distinguish here between the types of missions considered as being part of the security sector. Private or traditional security operators operate in a relatively unstandardised market, but "High-end" security missions operate under similar standards to those found in the defence sector.

In past years, however, public authorities at the international, European and national levels have started progressively to establish standards in the safety and security sector. This evolution is mainly a response to specific and dramatic events. The fact that rules and standards have been established to avoid the repetition of a difficult or dramatic situation implies that these rules are set with specific performance targets in mind. The intention seems to be to achieve a particular outcome, and technical standards are a way of obtaining this result.

In 1976, a small chemical plant close to the small town of Seveso, Italy, leaked around 6 tonnes of dangerous chemical material, like dioxins, into the surrounding area. Several hundreds of people suffered injuries from skin lesions due to chloracne. The Seveso accident played a major role in the improvement of safety standards in sensitive chemical plants, since it was following this disaster that the European Union approved new industrial safety regulations.[144] The same can be said for civil aviation security.[145] New standards in the field of security have emerged since 9/11 and, as

[144] Council Directive 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances (Seveso II Directive).

[145] Regulation (EC) 2320/2002 of the European Parliament and the Council of 16 December 2002 establishing common rules in the field of civil aviation security.
Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:355:0001:0021:EN:PDF; Regulation (EC) 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security.

counter-terrorism requires a real level of international cooperation, more and more international legislation is being introduced for transportation in general (air, train, sea) and for the control of goods and individuals.

It is in this context that a number of security standards were established in different sectors under the authority of the European Union, including airport security and air transport of goods[146], identification of goods or persons[147] and maritime transport.[148] In addition, the CEN started various activities that could usefully contribute to setting standards in sectors perceived as priorities by European policy-makers, such as Eurocodes (see CEN/TC 250), the transport of dangerous goods (see CEN/TC 296), urban design against crime (see CEN/TC 325), co-operation with NSA (expertise in radiological and nuclear detectors, decontamination and modelling, interoperable communications), civil protection (ISO/TC 223, see CEN/TC 239), network and information security (joint CEN/ISSS and ETSI Focus Group and ISO/IEC JTC 1 'Information technology'), biometrics (ISO/IEC JTC 1/ SC 37), the certification of equipment and personnel (see CEN/CENELEC JTC 1, ISO CASCO), designing crime out of products and the marking of small arms. CEN's BT/WG 161 "Protection and Security of the Citizen"[149], operational until the end of December 2008, identified some areas where standards are particularly required. These areas largely coincide with the "High-end" security missions identified in our study:

- Identification and reduction of crime risk in products and services
- CBRN incidents (Chemical, Biological, Radiological and Nuclear)

Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:089:0009:0010:EN:PDF

[146] Commission Regulation (EC) 820/2008 of 8 August 2008 laying down measures for the implementation of the common basic standards on aviation security and Directive (EC) 300/2008 on common regulations in the field of civil aviation security.

[147] Council Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States and Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. As regards biometric standards, the US is leading the field.

[148] 1) A proposal for a Directive on common rules and standards for ship inspection and survey organisations and for the relevant activities of maritime administrations (recast) (5912/06); 2) a proposal for a Directive amending Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system (5171/06); 3) a proposal for a Directive establishing the fundamental principles governing the investigation of accidents in the maritime transport sector and amending Directives 1999/35/EC and 2002/59/EC (6436/06); 4) a proposal on state port control (5632/06); 5) a proposal for a regulation on the liability of carriers of passengers by sea and inland waterways in the event of accidents (6827/06).

[149] The CEN's BT/WG (Bureau Technique/Working Group) 161 operates in the "Security of the citizen" sub-sector, which is part of the broad "Security and Defence" sector. This sector also deals with "Defence procurement" and "Humanitarian mina action" issues.

- Critical infrastructure - Energy supply
- Critical infrastructure - Building and Civil Engineering works
- Supply chain security
- Integrated Border Management
- Emergency services
- Defence against terrorism
- Security of water supply.

Notwithstanding CEN's remarkable efforts, in the security sector no common system of certification for security equipment exists at the European level. We can add that, even where the EU has established recommendations for the creation of common European security sector standards, differences in the application of these recommendations by Member States makes harmonisation far from perfect.

As shown above, maritime transport security is a sub-sector in which the need for standardisation is extremely significant, since almost 90% of world trade containers are transported by sea and worldwide maritime trade has more than quadrupled in the last 40 years.[150] The abovementioned ISPS Code and the following European regulations provide a comprehensive set of standards intended to enhance the security of ships and port facilities. Although developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks, it currently has relevant application also for operations against terrorism and organised crime, as well as for border control missions. Moreover, the Maritime Security Committee (MSC) of the IMO has adopted new regulations for Long Range Identification Tracking (LRIT), along with associated performance standards and functional requirements. The LRIT information that ships will be required to transmit include the ship's identity, location and date and time of their position. The MSC has also adopted performance standards and functional requirements for LRIT. It is clear that the US is very sensitive to the risk of terrorism and is therefore pushing all its partners and allies to adopt very

[150] Keith Michel and Peter Noble, *Technological Advances in Maritime Transportation*, The Bridge, Volume 38, 2008. http://www.nae.edu/Publications/TheBridge/Archives/TransportationInfrastructure/TechnologicalAdvancesinMaritimeTransportation.aspx

high security standards. The US has already imposed a national standard through its Customs Containers Security Initiative. Seaports that have an agreement with US Customs are required to scan sensitive containers and are, in fact, supposed to use containers with specific sensors, identifying the cargo being carried by a ship at least 24 hours before it leaves port. Twenty-four European seaports have already signed up to the US Customs Containers Security Initiative, but there is no common overall position at the European level.

3.2.2.3. Standardisation for the blurred market?

As highlighted by a series of interviews with stakeholders carried out during a study undertaken by ASD-STAN[151] on the role of European industry in the development and application of standards, a significant number of the existing civilian standards could in fact be used in the defence sector. According to the study, up to 90% of standards in the civilian naval sector could be used in the defence sector, as well as 75% of those used in the aeronautic and 70% in the land sectors. These findings show that the convergence of civilian and military standards in the security sector is possible and could potentially be a favourable factor in blurring between the sectors.

However, this technical convergence still remains potential at the political level and no significant steps have been taken to move closer to common military-civilian standards. As stressed above, in some of the missions considered as blurred, the level of technology and equipment standardisation remains limited. This seems to be due to two concurrent elements:

- on the one hand, the will of MoDs and Armed Forces to maintain their own exclusive control over military standards. Although they increasingly operate together/side-by-side with civilian security forces, they are still extremely reluctant to consider the idea of standardised, common civil-military technology and equipment.
- on the other hand, the high number of security actors involved in "blurred" missions who have not yet been able to or interested in acting as a unique security voice, therefore slowing down any common efforts towards standardisation in the security sector.

[151] The study is available at the ADS-STAN official webpage: http://aecma-stan.org/Study%20EDA%20008-ARM-003%20%20Final%20Report%20Executive%20Summary.pdf

A further aspect to consider is the case of companies themselves defining standards. An example of this practice is the creation of the NCOIC (Network Centric Operations Industry Consortium).[152] In 2004, a number of American enterprises, including Boeing, Northrop Grumman, Raytheon and others, created such a consortium of companies working on network centric warfare. The goal was to promote the standards they have developed internally to a wider audience. More than 100 companies are currently part of this consortium, essentially in the defence sector, but also including telecom companies. In order to extend its standardisation activities, NCOIC started working together with the Emergency Interoperability Consortium (EIC) on services and data interoperability standards to be applied to technologies and equipment used by emergency actors and first responders during complex humanitarian disasters.

In addition, ESRIF has also made a significant effort to promote an extended standardisation process across Europe. THE ESRIF "EU Security Label" proposal is designed to encourage standardisation and certification, with the intent of harmonising practices as a market entry criterion for security products and services. Moreover, the Security Label is also meant to reassure European citizens that the security measures provided by public and private organisations respects specified European criteria. The Label, therefore, also address the societal dimension of security by responding to citizens' requests for an adequate and measurable level of security. Other ESRIF recommendations include increasing interoperability in order to reinforce harmonisation in the fragmented security market. The aim is to improve European security, because "the multitude of Europe's problems with territorial, organisational and cultural non-interoperability along its Member States' borders enables criminal and terrorist organisations to exploit the patchwork's inherent weaknesses".[153]

These emerging trends, within the realms of both business and institutions, could represent an important start point for the development of coherent standardisation thinking, which is still so lacking in the security sector. Although, at present, these two approaches are only in their initial phase and are not definitely channelled into a common course, the increasing relevance of

[152] NCOIC official webpage: https://www.ncoic.org/home
[153] ESRIF Final Report, September 2009, http://www.esrif.eu/documents/esrif_final_report_part_i.pdf

security missions involving different actors (industrial and political), and their need to operate jointly, could finally foster a structured approach to effective standardisation.

3.2.3. Impact of the Lisbon Treaty

Although not providing specific provisions on the blurring of lines between external and internal security, the Lisbon Treaty (for a detailed analysis see Annex 3) offers some interesting food for thought over the possibility of increasing the EU's role across the two sectors.

The most relevant change introduced by the Treaty is represented by the new role of the High Representative of the Union for Foreign Affairs and Security Policy, who covers crucial positions in the two main institutional promoters of the EU R&T activities in the security domain. Since the High Representative is concurrently the Head of the European Defence Agency and Chief of the EDA's Steering Board, and the Vice-President of the Commission with competencies in the management of the Union's external actions, she might have a pivotal role in the setting of the EU's external agenda, including the definition of a broader (simultaneously military and civilian) approach towards European security and its reference market. As shown above, both the EDA and the EC are increasingly active in promoting research programmes in what we have identified as an emerging blurred area between security and defence. The new institutional framework created by the Lisbon Treaty could lead to a synchronised EDA-EC funding of defence and security research, which would in turn reinforce the blurring between defence and security market demand at European level.

A second relevant element introduced by Lisbon's provisions is the extension of the Petersberg tasks (humanitarian and rescue tasks; peace-keeping tasks; tasks of combat forces in crisis management, including peacemaking), which will be integrated by new joint disarmament operations, military advice and assistance missions, and conflict prevention tasks. Of course, as we stressed in Chapter 1, these provisions are not enough to foster a real operational blurring between defence and security actors. However, if accompanied by a clear will inside the European Member States to proceed in this direction, the extension of the Petersberg tasks might contribute to the development of an EU comprehensive approach between civil and military operations.

The enlargement of missions in the blurred area is not limited to crisis management. It also covers counter-terrorism, which is emerging as a key threat to be addressed by the EU in its internal domain, as well as in its external efforts. The Treaty's provisions on the fight against terrorism are included both in the part which deals with the CFSP/CSDP and in the part which deals with the area of Freedom, Security and Justice (FSJ).[154] According to the Treaty, defence forces and internal security actors, such as the police, could be increasingly involved in common efforts against the terrorist threat. This twofold approach is a clear sign of the EU's intention to address in a "comprehensive" way threats in the blurred area.[155] This is what emerges, finally, when analysing the provisions of the solidarity clause (art. 222 of the Treaty), which prefigures the possibility for both the EU and Member States to intervene, even with military resources, in the territory of the Member State who requests assistance. What seems particularly relevant is that the article introduces the possibility of using military resources, the typical tool to guarantee a State's external security, in the internal security domain (to prevent the internal terrorist threat; to protect democratic institutions and the civilian population; to assist a Member State in its territory), sensibly extending, at least theoretically, the use of military force in the internal sphere at the EU level.

At the institutional level, the Lisbon Treaty might affect the way the EU currently runs its internal security policies. The creation of the Area of Freedom, Security and Justice should bring together currently dispersed Justice and Home Affairs policies. An expansion of the Communitarian rather than intergovernmental method, and the improvement of decision-making mechanisms, are also foreseen. The standard decision-making procedure will be co-decision. This method will apply to areas such as police and judicial cooperation in criminal matters and migration and integration of third countries' nationals. Thus, we can hope to see the existing agencies, Europol, Eurojust and the European judicial network, working together more closely, with the practice of co-decision leading to a more integrated policy. Experience shows that this type of process would help harmonise security requirements at the European level.

[154] Terrorism, in fact, is mentioned both in the provisions which discipline the Common Foreign and Security Policy (Art. 43 TEU) and the area of Freedom, Security and Justice (Art. 88 TFEU).

[155] The possibility of enhancing a joint approach between military and security forces does not mean, however, that it would automatically lead to a convergence of technical and operational requirements and thus use of common equipment.

Moreover, the Treaty establishes that a permanent structured cooperation (PSC) within the EU framework could be set up by "those Member States whose military capabilities fulfil higher criteria and which have made more binding commitments to one another in this area with a view to the most demanding missions". The first PSC's objective is "to proceed more intensively to develop its defence capacities through the development of its national contributions and participation, where appropriate, in multinational forces, in the main European equipment programmes, and in the activity of the [EDA]". Given the EDA's interest in developing civil-military synergies in the "new security" domain[156], the Agency could exploit its institutional prerogatives to promote the launch of European equipment programmes in the blurred area between security and defence in coordination with the European Commission.[157] .

3.3.Conclusions

This chapter has enabled us to point out the characteristics of demand in the defence and security sectors and in the blurred area between the two sectors. It places an emphasis on how a common demand in the defence and security area is slowly growing, but shows where its limits exist. The chapter also takes into account the impact of regulation on demand in our target sectors.

Our basic assumption is that the defence and security markets remain very different. The embryonic emergence of a European demand in the defence sector, fostered by the EDA's Capability Development Plan and common R&T projects, is a positive driver for the strengthening of the European DTIB.

On the security side, the emergence of any coordinated demand across Europe is still largely missing, as demand remains fragmented within single Member States. Data on national security budgets show (see Table 5, p. 176) that it is still difficult to define exactly what security demand is and what the security market includes. This helps explain the difficulty in clearly defining any blurring of the borders between security and defence. The security market is far less structured than defence and its dimensions are almost undetermined.

The current framework for the management of R&D and procurement does not support the

[156] See EDA's fifth Annual Conference dedicated to « bridging efforts : connecting civilian security and military capability development », 9 February 2010, www.eda.europa.eu

[157] As already done in the Software Defined Radio (SDR) sector: http://www.eda.europa.eu/newsitem.aspx?id=51

growth of the blurred area between defence and security. The 7th FP in the security field helps private and public organisations invest in security technologies that could potentially operate in both the defence and security sectors. In order to obtain this result, though, the European Commission must be able to transform the technological findings of the 7th FP into equipment programmes. Thinking over pre-commercial procurement is a step in the right direction, but more decisive actions could be undertaken to shape truly coordinated European demand, an aspect that we will develop in our recommendations.

The European Commission could therefore have a real role in shaping future demand for blurred security/defence products, acting as a major player in the definition of standards and as a catalyst in the development of a world-leading security market. Standardisation does not appear as a generic solution for all market problems, however. There are further opportunities that we will develop in our two last chapters.

4. Characteristics of supply in the blurred area between the defence and security sectors

In Chapter 1, we have seen that missions related to "Post Cold War" defence and "High-end" security[158] are driving the blurring of dividing lines between the defence and security sectors. This remains primarily a conceptual blurring, however, currently less evident at operational level. In Chapter 2, we have shown that technology is another main driver of this blurring of dividing lines, due to the growing application of some types of technology in both defence and civil security missions. Finally, we have demonstrated in Chapter 3 that defence and, to a lesser extent, security customers are beginning to embrace efforts towards national and European cooperation and coordination. Attempts to engage in dialogue and to coordinate a number of initiatives between the two sectors are also being made, despite the numerous obstacles that still exist at institutional level.

This chapter builds on these findings to identify the industrial players operating in the emerging blurred segment and, in particular, to verify whether the blurring has an influence on the structure, organisation and strategy of suppliers providing equipment and services in this segment.

4.1.A fragmented supply base

In the past, industrial security and defence players concentrated largely, if not exclusively, on their own specific market. A number of factors reinforced the difference between the two sectors, such as their procurement patterns, levels of interaction with companies in their own sectors and the extent of interference and oversight exercised by public authorities over their activities.[159]

The defence industry was specialised in developing individual solutions for an exclusive customer, the Ministry of Defence, who specified, financed, oversaw and owned the output of research and development work, thereby controlling the sale of products. Public security providers would, on

[158] For more details on the definitions see Chapter 1, pp 20-21.
[159] W. Walker and P. Gummett, *Nationalism, Internationalism and the European Defence Market*, Chaillot Paper 9, 1993.

the contrary, mostly use products and technologies developed for and tested in commercial markets and available to private customers, such as physical access control, intrusion and fire detection, CCTV and video-surveillance, Private Mobile Radios. In some cases, however, specialised equipment, not available for sale to private customers, has also been provided to security forces for particular tasks: for example, the Canadair water bomber, an aircraft specifically designed for aerial fire-fighting, or small naval vessels for coastal patrol duties have been used by national civil protection forces to respond to public security emergencies. This is still the case today. Even in these particular cases, however, the equipment was seldom developed in cooperation with, and upon request from, a particular end-user with specific requirements: rather, it would be designed with a specific function in mind and then sold off-the-shelf to public security customers. Direct demand-supply dialogue and cooperation were mostly limited to the customisation of existing, off-the-shelf equipment, for example, the armour-plating of vehicles for special police tasks such as VIP protection.

It is therefore not surprising that the supply structure of the security and defence sectors has shown a significant degree of difference. Both industries have remained largely separate, differing in terms of their technological bases, size and political weight. The defence industry has developed specific military technologies in a very close relationship with Ministries of Defence, often under the veil of secrecy to maintain a military edge and for exclusive use by national and allied armed forces. Large, upfront R&D investments and economies of scale have given an incentive for consolidation, leading to a concentrated market structure with large firms. This development was fostered by occasional collaboration on the demand side in large armaments projects. Intellectual property remained with the customer, or at least under his control. Long-range planning cycles allowed the systematic innovation and improvement of high end products, with an emphasis on performance and reliability, rather than time and cost. Commercial, off-the-shelf technologies were used, but often adapted and "hardened" to perform reliably under tough military conditions.[160]

On the other hand, security companies have operated in a more competitive market and adapted their products to far shorter product life cycles, driven by market research rather than closed-door

[160] A. Markusen and J. Yudken. *Dismantling the Cold War Economy*, New York, Basic Books, 1992.

negotiations. Intellectual property remained with the producing firm and could subsequently be used freely for other applications. The test of success was in the market, with its numerous possible customers, not on the battle field. There was therefore no need to produce equipment durable enough for battle scenarios, except for some specialised items mentioned above, which could be either produced for use by public security customers or customised from off-the-shelf equipment.

At present, our findings show that the blurring we have identified at mission level has had only very little practical consequence for procurement decisions and, therefore, for the expansion of a specific industrial base which might provide equipment and services for these missions. Today there is no single and structured industrial base which would serve both defence and "High-end" security customers. Interviews with stakeholders confirm this: those working on defence matters (in a broad sense) consider that the "industrial base" operating in these market segments is mainly composed of big defence companies and big security firms. Those who work on security matters (in the sense of internal security) tend, on the contrary, to emphasise the role of small and medium sized security companies. As a result, it is difficult to identify companies which clearly dominate the market segment. The industrial landscape is, rather, characterised by extreme complexity and fragmentation, with numerous industrial players coming from various industrial areas and providing different types of solutions according to the specific requirements of their military or security customers.

For military crisis management operations abroad ("Post Cold War" defence missions), for example, it is the traditional defence industrial base which produces and delivers military equipment for the armed forces deployed on the ground. Security and civil equipment and services used by military and non-military forces and staff on the ground, by contrast, are provided by civilian companies, often SMEs.[161] This is not surprising, since these products are often less technologically sophisticated and/or bought in a rather limited number, which makes these

[161] For example, air surveillance provided by a civil aviation company from Luxembourg for operation ATALANTA, transport for the operation in Chad provided by the Ukrainian company Salis and various framework contracts established with private companies for civil operations (for supply of fuel, armoured vehicles, etc).

procurements less interesting for big companies. Hence, both the equipment and the industrial supplier base for civil-military missions remain often different.

The situation for “High-end” security missions is even more complex, since these missions (i.e. organised crime, border control, the fight against terrorism) are very different. Consequently, different types of equipment, systems and sub-systems are used, depending on the customer and the purpose of the mission.[162] Therefore, suppliers for this market segment differ greatly in size and nature and come from a broad range of industrial fields (big defence players, big civilian players, SME niche producers, IT, etc). In other words, “High-end” security can neither be considered as one security market, nor does it seem appropriate to talk about a “High-end” security industry serving this market.

There may be some blurring at the technological level, but far less when it comes to equipment. Sometimes the technology used for "High-end” security applications can be similar to defence technology (sensor equipment, identification equipment, biotechnology, detection of explosives, biometric equipment, etc.), but still significant differences in terms of requirements can persist at the equipment level. European customers demanding comprehensive and tailored solutions incorporating defence/security technologies are still, at best, the exception, and there is very little indication that this will change in the future. Any instance of European countries procuring complex systems is extremely rare, and we are not aware of large homeland security programmes being developed or requested at the national level for the moment. The Italian Finmeccanica group, for example, has signed different contracts for vessel traffic control and border monitoring systems. Most of these were, however, with non-European countries (Libya, Yemen, Algeria, Australia)[163], while only one was concluded with a European country (Italy).

So, the principal characteristics of the supply base in the blurred area are heterogeneity and fragmentation. Since industrial players operating in these segments differ greatly, it does not

[162] Some examples from the STACCATO taxonomy on equipments, sub systems and platforms: sensors equipments, signal protection, CBRN, munitions devices and energetic content, explosives removal, biometric.

[163] Some interviews from large defence and security companies referred to an emerging export market for defence/security integrated systems, mainly in countries where post 9/11 scenarios create new needs to enhance protection against “terrorist like” threats.

come as a surprise that they have developed very different approaches to address these segments.

4.2. The approach of defence origin companies in the blurred area

4.2.1. General structure of defence origin companies

The European defence supply sector has a total turnover of 137 billion euros, of which 71.1 billion euros represent purely defence customers, and employs around 676,000 employees[164]. The strength of the European defence sector is demonstrated by the fact that of the largest ten defence companies at global level four are European, namely BAE Systems (2°), EADS (7°), Finmeccanica (9°) and Thales (10°).[165].

The structure of the defence supply base can be represented by a pyramid, with system integrators at the top, which are often – but not exclusively - subsidiaries or joint ventures of big groups (EADS, Thales, BAE Systems, Finmeccanica). A second tier is composed of specialised sub-system producers (i.e. Safran), and a third tier includes hundreds of SMEs that are suppliers of components and services for the two tiers above.

If we look at general turnover, according to the ASD 2007 data, overall military sales in Europe are estimated at around 70 billion euros, divided into:

- military aeronautical sales, including avionics and electronics for air platforms and services, which account for around 40 billion euros (of which 13 billion euros of exports);
- space turnover of 5.2 billion euros, of which 3.2 billion come from the institutional market and only 1 billion euros is for military systems, although this shows a consistently upward trend since 2001;
- the defence naval sector, which accounts for almost 15 billion euros;
- the land military sector, exceeding 14 billion euros.

[164] Data from ASD: http://www.asd-europe.org/site/index.php?id=2.
[165] SIPRI Yeabook 2009.

These data, once export figures are excluded, are not far, although not entirely consistent, from the European demand-side aggregate data provided by the EDA. These show that, for the year 2007, expenditure on defence equipment and R&D was in the range of 40 billion euros.[166]

4.2.2. Different approaches towards the blurred area between the sectors

It is generally argued in public debates that, since the end of the Cold War and even more since the terrorist attacks of 9/11, defence companies have been moving into the security market by acquiring primarily civilian supplier businesses, generating a blurring between the defence and security sectors. Certainly, since 9/11, security has become a greater political priority in Europe, leading defence-origin suppliers, in particular, to consider it almost certain that there will be future public investments and procurement in this area. This is why some companies have reorganised themselves, adding a security dimension to former defence units and creating common "security and defence" divisions. Nevertheless, these expectations do not seem to have been driven by any massive growth in this new security market, able to generate profits for large scale companies. A closer look shows that the reality is less clear, in terms of both corporate positioning and turnover related to this market segment.

Large system integrators and defence firms of the pyramid's second and third tiers have very different interests in, approach to and success in the security market. What most of them have in common is a difficulty in establishing a comprehensive business strategy for entry into the security market. According to industry sources, most companies were – at least initially - driven by the belief that there would be a new market with significant business opportunities. This belief, however, had immediately to face the particular difficulties which characterise the security segment. According to our sources, the main difficulties are clearly linked to the characteristics of demand in the security market: the fragmentation of customers, the lack of harmonisation of requirements, non-existent capability planning to address complex threats and limited budget and investments. Security customers indeed require rapid reaction from their supplier base and prefer already existing and rapidly available off-the-shelf solutions at affordable prices. Defence

[166] European Defence Agency (EDA), *Defence Data of EDA Participating Member State 2007*, 2007, http://www.eda.europa.eu/defencefacts/.

companies, in contrast, are used to a completely different way of operating with Ministries of Defence, where long term planning is the rule and product development typically lasts 10 or 15 years. Relationships with "security" customers require very different marketing strategies, based on competitiveness and price for off-the-shelf products.

After 9/11, defence system integrator companies expected the emergence of a security market comparable in size to the defence market. This has not been the case. Available figures[167] often provide data aggregating the already existing "traditional security" segment and the emerging "new security" one. This leads to increasing the size and the importance of the new "High-end" security market. The same is true for investment in research. We cannot identify a massive shift of investment in security technology at MS or EU levels. The EC security research programme certainly represents a considerable effort which has attracted many companies, but has not led so far to important procurement programmes. Consequently, some defence companies who have tried to enter the market have encountered only limited success, while others have remained more prudent and have decided to maintain their strong position in the defence area.

We will now consider the business conditions that are necessary for a defence company successfully to enter the security sector. We will focus here on companies who are privately (not government) owned and/or who behave like private value-maximising companies and discuss three business conditions necessary for successful diversification[168]:

Possession of valuable and distinctive technologies. The first necessary condition is that a defence company possesses valuable and distinctive technologies.

By valuable we mean that those technologies must be valued by customers because they can contribute to the execution of particular security missions. This helps explain why some companies (for instance, MBDA) are unlikely to enter the security market; simply put, they have strong technologies for defence applications, but those technologies are not valuable to security customers.

[167] For instance, those provided by the ECORYS' *Study on the Competitiveness of the EU security industry*, 2009.

[168] Of course, companies may either not recognise these pre-conditions and/or ignore them. In our judgement this can be observed in the strategies of some European defence companies. The ultimate outcome of such a situation is likely to be either poor performance of their security businesses or potentially outright failure.

The technologies possessed by a defence company have to be not only valuable to a customer, but also distinctive. To diversify successfully, a defence company must possess distinctive technologies that provide the basis for some form of commercial advantage over other competitors. There is the potential for miscalculation of the true distinctiveness of technologies which is likely to be exacerbated where a defence company has limited knowledge of the market. For example, defence companies see systems engineering as a distinctive competence, but systems engineering capabilities are also strong in telecommunications companies and there are examples of defence companies losing out to telecommunications companies in head-to-head competitions for security programmes. One example of a defence company losing out to a telecommunications company is provided by the 2005 procurement competition in the UK to supply a UK national radio system for first responders. The programme was won by O2 Airwave – a consortium led by the telecommunications company BT – at the expense of a consortium led by EADS Defence and Security. Equally, however, examples of the reverse can also be identified. For example, a consortium led by defence contractor Raytheon Systems Limited won the UK eBorders programme against competition from a BT led consortium.

Access to the necessary complementary capabilities. Analysts of the innovation process of taking technologies and converting them into commercially successful products emphasise the importance of what they call *complementary capabilities*. These may be capabilities in marketing, brand exploitation, distribution or manufacturing. What makes them crucial to successful innovation is that they are necessary to bring a company's technologies to the customer. Most important of all is access to marketing capabilities. In Chapter 3, we note that the character of customers in the security market is often very different to that of the defence industry's traditional MoD customer: in some segments of the security market, there is a large number of customers who are often relatively technically unsophisticated and have limited capability to specify their technical requirements. The buyer values of those customers are also very different from the values of defence buyers.

To diversify successfully into the security market, defence companies have two main choices: either they seek out security customers who have similar characteristics to defence customers (i.e. coastguards, who are large institutional buyers with a demand for large and complex systems), or they obtain new marketing capabilities (through organic growth or by acquiring a company already

established in the security market). The acquisition of Detica by BAE Systems can be seen to be an example of the latter approach.

Viable business model. The third pre-condition for successful diversification is that the defence company is able to develop a viable business model i.e. to generate a return on investment. Three considerations deserve attention in this context:

Investment expectations – Defence investments in R&D and production facilities traditionally assume that the government customer will fund R&D and then guarantee a minimum level of production. Practice in the security market is normally different. Although defence companies do spend "private venture" funds on new product development for the defence market, their willingness to shoulder the risk of speculative own R&D funded projects for security markets is limited.

Expectations of market size and rate of return – The nature of the defence market means that defence companies have particular expectations of market size and are likely to evaluate security business opportunities against defence market criteria, especially in terms of the ability to plan returns long-term. The character of many security markets (i.e. large numbers of customers each procuring relatively small values of products and services) has, for example, implications for the overheads and general cost of defence companies diversifying their business.

Regulation – The regulatory environment shapes the possibilities for developing a viable business model from defence technologies. Again, civilian use of UAVs is a good example, where the rates at which defence companies are taking their UAV technologies and moving into the civilian security sector is being driven in part by regulatory issues and the development of sense and avoidance technologies to ensure traffic safety.

Having discussed the conditions which are necessary for a defence company to move into the security market, we can now try to identify the strategies which industries can develop to fulfil those conditions. Defence companies have a number of potential routes available for entry into the security market. We have identified three broad diversification strategies, which are not mutually exclusive, and companies frequently use more than one strategy simultaneously.

Organic diversification. A defence company may diversify organically by drawing primarily on its own resources and capabilities to exploit its already existing defence technologies in the security market. This organic diversification is likely to rely heavily on the company's capacity to find its own channels to market and to develop the necessary marketing capabilities through trial-and-error learning, gaining a gradual understanding of the security market. This was the case, for example, for Finmeccanica, which transformed itself into a "security and defence" company by reallocating internal resources for the security market.

Diversification through acquisition. A defence company may seek to gain the marketing capabilities necessary for entry into the security market by acquiring other companies that already have an established market position and brand image amongst security customers. Finmeccanica, for example, took control of the IT company, Datamat. The evolution of Thales also illustrates how this type of diversification strategy works, with, for example, the takeover of Racal, a UK electronics firm with strong defence business lines but also active in areas such as civilian telecommunications.

Partnering or teaming. A defence company may seek to exploit its technologies in the security market through partnering or teaming. In this way, a defence company's technological capabilities can be complemented with the knowledge of the security customer possessed by other companies. Equally, since defence companies perceive themselves to have strong systems engineering capabilities, we observe teaming between defence companies (as systems integrators) and other (non-defence) suppliers of systems and sub-systems. For example, the successful bidding consortium for the UK eBorders programme was led by the defence contractor Raytheon Systems Limited and other members of the consortium include Serco (a services company), Accenture (IT and consulting), Detica (a company focused on the security and intelligence sectors recently acquired by BAE Systems), QinetiQ (the privatised UK government defence research agency), Capgemini (the IT services and consultancy company) and Steria (an IT services provider).

In the following paragraphs, we identify several examples of how defence companies have adopted and combined the above mentioned strategies. We also attempt to measure their degree

of success in entering the security market. It should be noted, however, that this quantitative analysis should be treated with caution, since there is no common definition between companies for "security products". There are, in fact, no European or national guidelines for the identification of security goods. The result is that companies often cannot provide specific data for their security activities portfolio, which is often mixed up with dual or civilian products. However, it is still possible to compare data which, although they are not completely precise, are indicative of current trends.

Examples of the difficulties found by defence companies in entering the security market are provided by the experiences of Finmeccanica, BAE and DIEHL.

FINMECCANICA is a good example of the combination of different strategies for entry into the security market. Finmeccanica is an Italian defence group which has developed several business lines in the security sector through the acquisition of companies operating in different market segments. These include businesses producing systems for homeland protection, systems and radar for air defence, battlefield management, air traffic control, coastal and maritime surveillance (Selex Sistemi Integrati, Selex Galileo), IT and logistic (Elsag, Datamat) and, more recently, the American DRS, involved mainly in electronics for defence but also producing dual-use goods.

The approach chosen by Finmeccanica is not limited to acquisition, but is also focused on using its system integrator capability to provide security solutions. The Strategic Situation Centre,[169] unveiled by Finmeccanica at the 2009 Le Bourget exhibition, merges data and C4[170] capabilities for all the defence and security functions identified in this study.

The Italy-based group is also deeply involved in all political activities shaping the security market at European level, such as high level groups in ESRAB and ESRIF, the Preparatory Action for Security Research and 7th FP projects (SENTRE, STACCATO), the promotion and expansion of industrial associations in the security sector (EOS, security role of ASD). Finmeccanica's investment in 7th FP for security research is done in the perspective of future development of EU security programmes. This choice is based on their national experience with research and development programmes that

[169] For details see: http://www.dedalonews.it/it/wp-print.php?p=19471
[170] The acronym C4 stand for: command, control, communication and computer.

often end up with a procurement process.

However, if we compare the turnover of Finmeccanica's security divisions to that of the defence division, security business appears to be limited. The group's "security champion", Selex Sistemi Integrati, has declared 646 million euros of revenue for 2008, while Selex Communications has revenues of 754.7 million. In addition, Finmeccanica's space subsidiaries (Telespazio and ThalesAleniaSpace) are involved in a dual-use market and explore the opportunities of blurring between defence and security. Including Finmeccanica's space activities, total security revenues for the company are about 2.4 billion euros. This represents only 17% of total Finmeccanica turnover, which is about 13.6 billion euros. We should also take into account that an important share of these 2.4 billion euros, which is difficult to quantify, is related to products which are neither security nor defence, but purely civilian (for example, Selex S.I. also produces air traffic management systems for airports).

Therefore, despite significant investment in the security sector, the company remains strongly "defence oriented". In Finmeccanica's published budget, there is no sign of a "security" business division. Finmeccanica's managers indicate SELEX SI as the "security champion", highlighting the "integration of systems" approach to security, yet it is also defined as a "security and defence electronics" company.

Finmeccanica illustrates the experience of those system integrator companies which expected the post 9/11 development of a new security market in Europe, fostered by the European security research programme. Yet the impossibility of retrieving pure security data from Finmeccanica clearly indicates the uncertain size of this business for the company. In other words, security is considered as a potentially emerging market, but it is still to be developed and sustained by clear demand. Exports in the sector, particularly border security projects, appear to present a reasonable opportunity for growth. The company has won some large export security contracts abroad: Libya recently acquired from Selex Sistemi Integrati a 300 million euro border security system[171], while Yemen is using a Selex SI Vessel Tracking Monitoring System[172] to improve the security of its territorial waters threatened by piracy. Other European companies, too, are

[171] See Defense Industry Daily, 12 October 2009, http://www.defenseindustrydaily.com/Libya-Buys-Border-Control-System-from-SELEX-05846/.
[172] See Finmeccanica press release, http://www.finmeccanica.it/IT/Common/files/Holding/Corporate/Sala_stampa/Comunicati_stampa/Anno_2009/ComFin_VTMSYemen_25_06_09_ITA.pdf.

increasingly exploiting the opportunities presented by the export market: EADS, for example, has already supplied Qatar with a border security system and was recently awarded a contract by Saudi Arabia for the construction of a security system for the entire territorial border of the kingdom, a contract reportedly worth billions of dollars.[173] However, the development of a domestic European security market is yet to crystallise. Such a European market would have sufficient size to provide business opportunities for a global system integrator, such as Finmeccanica.

BAE also remains extremely defence-oriented. The company's largest division is the "Land & Armaments group", whose revenues amounted to £ 6.4 billion in 2008[174] (+38% on 2007). The Electronic, Intelligence & Support group (£ 4.5 billion) and the International group (£ 3.3 billion) are also mainly defence-oriented, although they comprise some purely civilian activities.[175]

However, BAE, in common with Finmeccanica, has attempted to enter the security market. The company's approach combines the acquisition of security and civilian companies with the exploitation of defence products and technology that can be used in the security sector, such as civilian use of UAVs already provided for the operation in Afghanistan. In 2008, BAE acquired the UK government commercial software business of Petards Ltd's Universal Video Management System (UVMS), which gave it a small opening into the national security and resilience sector. The £ 530 million acquisition of Detica is also consistent with BAE Systems' objective to establish security businesses in its home markets. The choice to invest in Detica proved to be right, as its own 2008 revenues increased by 20% on 2007 (reflecting higher sales to the UK government), notwithstanding the overall contraction of revenues within BAE's Programmes & Support operating group, to which Detica belongs, from £ 5.3 billion in 2007 to £ 4.6 billion in 2008. At the EU level, however, BAE is not following the same strategy as other companies that have tried to use EU research funding, such as for instance Finmeccanica and DIEHL. BAE has limited its investment in the European security sector and has not participated in the Framework Programme's activities,

[173] Grace Jean, *Saudi Arabia Securing its borders with Sensors and Software*, National Defense, December 2009, http://www.nationaldefensemagazine.org/archive/2009/December/Pages/SaudiArabiaSecuringitsBorderswithSensorsandSoftware.aspx.

[174] 34% of BAE's total revenues for the year, according to the company's Annual Report 2008, http://bae-systems-investor-relations-2009.production.investis.com/en/~/media/Files/B/BAE-Systems-Investor-Relations-2009/PDFs/results-and-reports/reports/2009/Annual_Report_2008.pdf

[175] The Electronics, Intelligence & Support operating group designs, develops, produces services systems and subsystems also for commercial applications. The International group own shares in civilian Air Astana of Kazakhstan.

rather waiting for concrete opportunities to emerge. It is active at the political level in various debates and it is involved in networks and associations such as EOS. Even though BAE's position differs from that of Finmeccanica, their analysis of the security market is the same: BAE's response is simply more cautious than Finmeccanica**.**

The **DIEHL** corporation comprises more than 40 different companies and is active in the automotive, electronics, defence and security and aeronautics sectors. DIEHL started to have an interest in the security market following the launch of the EU's initiatives on security, particularly the establishment of the ESRAB process. Therefore, as with the previous two examples, the company's investment in the sector was not the result of a strategy developed from specific market analysis showing concrete potential for growth. It was rather the result of a feeling or a belief that there could be market opportunities coming from the political interest in security shown by EU institutions. Hence their political involvement in all EU activities related to security. In response, DIEHL has developed a "technology-driven" approach to security, by identifying the technological knowledge they have in the defence sector which could be applicable to products in the security sector.[176] They have naturally identified the "High-end" security segment as the market with greatest potential.

This approach has, however, proved to be unsuccessful for a variety of reasons, leading the company to step back from the security market at EU level. Among the difficulties they faced was the fact that EU initiatives are mainly focused on research and technology, particularly the European research framework programme. As a medium sized, family-run business, DIEHL was unable to invest in research, without a guarantee of winning a contract and being able to develop equipment, as is the case in the defence sector where research and development is financed by the customer.

At national level, the main difficulty they faced was fragmented demand, with different requirements and limited budgets. This was particularly true for DIEHL in Germany[177], where they tried to sell existing products and technology already developed for the armed forces to security

[176] Such as: image processing analysis - technology from sensors missile applicable to sensors for transport security, critical infrastructure and border surveillance, search and track sensors used to protect camps applicable for airports protection or border security, bio-sensors developed to sense bio and chemical war

[177] Being a Federal State, Germany is probably a more relevant example than other countries for the argument of fragmentation.

customers (local police and buyers of crisis management products). Critical mass, and therefore return on investment, could not be achieved, since demand was not high enough to reduce costs and allow the products to reach an affordable price. This issue is not specific to DIEHL, and is a serious problem faced by many defence firms, except a small number of very large companies, when entering the security market, where the structure and level of production costs is totally different from the defence market. As a consequence, DIEHL has decided to concentrate on its market of origin – defence – and to remain partially present in the German security market, where they can use or adapt defence technology or products. Its annual sales in 2008 illustrate this trend. Of the 2.1 billion euros annual sales, 608 million come from defence and security, security representing no more than 1% of this amount.

These experiences do not mean, however, that defence firms have altogether failed in penetrating the security market. A closer look shows that success stories do not come from defence companies, but rather from business units of big defence groups which have already been operating in the security market for a long time and are therefore used to the specificities of this sector. According to industry sources, these business units normally operate completely separately from the defence businesses of the same groups, with very few – if any – synergies, even in research.

Good examples of this different approach are Thales and EADS, two large companies which both have dedicated security business units, and Safran.

Thales is a global leader in detection, information, communication and combat systems for the armed forces. It is a major world player in three markets: defence, aerospace and security. Consolidated turnover in 2008 was 12.7 billion euros (+8% on 2007). Revenues for the defence sector indicated a 9% growth, up to 5.47 billion euros, while the security sector accounted for 3.175 billion euros (25% of the total). This is a very important aspect, as Thales is the only large European corporation operating in the sector which explicitly refers to the security segment in its official financial documents.[178]

[178] Thales annual report 2008. http://cms.thalesgroup.com/group/Investors/documents/doc_annual_report_2008

Thales has chosen to increase its positioning in the security market for surveillance and intelligence systems, identity systems, security of large scale critical infrastructure, via the acquisition of civil/security companies in the sector of communications, crypto and surveillance.[179] Indeed, Thales is seeking inroads into the US ISR (Intelligence, Surveillance and Reconnaissance) market[180], demonstrated by the establishment of Thales USA Defence & Security Inc. and their attempt to buy the US defence technology group DRS Technologies in 2008 (finally purchased by Finmeccanica for $ 5.2 billion). This choice is based on the conviction that the action of public authorities and critical infrastructure operators in the civil sector requires the use of dual technology and expertise resulting from massive investment in the military sector, subsequently transposed and tailored to meet civil requirements.[181]

Since 9/11, Thales has strengthened its focus on the most technology-intensive segments of the defence market, particularly network-centric warfare and force interoperability. These are the segments where synergies with security applications are more common. In 2004 it also reorganised its divisions into 6 branches corresponding to their respective markets, to facilitate implementation of common technologies: Aerospace, Air Systems, Naval, Land and Joint Systems, Security and Services.

Thales has two major security goals:

- respond to state demands for developing surveillance and intelligence systems, urban security and identity systems,
- contribute to the safety of critical infrastructure functioning and security, such as the railway and energy networks, trouble spots, banks' information systems.[182]

In its strategy for 2010, four crucial sectors were identified: land transport, critical infrastructures, administrations, industry and finance. For investment, the major effort focuses on the

[179] Systems to ensure safety of critical infrastructure network, monitoring, observation and control in order to prevent security attacks/satellite observation, internet surveillance, airspace control, equipment of civil and military forces with communication, command, protection and threat detection solutions.

[180] K. Wagstaff-Smith, *Thales still "aggressively" seeking inroads to US ISR market*, Jane's.

[181] Technology designed to detect and identify threats; integration of complex systems, real-time information processing gathering, secure communication systems.

[182] *Thalès solution de sécurité et de services*, Press report, Mexico, March 2009. Available at : http://www.thalesgroup.com/assets/0/249/250/d5bca324-7d32-4a2b-a23d-66ad28747d51.pdf?LangType=2057

"*development of their position in railway signaling*[183]*, the strengthening of systems integration capabilities to offer comprehensive urban security solutions, the building on key technologies and commonality with defence".*[184] An example of the last goal is ThalesAleniaSpace, the space subsidiary of Thales and Finmeccanica, which is developing dual-use systems contributing to a specific evolution of the space industry. This subsidiary is clearly targeting the blurred area between defence and security.

The Thales posture towards the security sector is pretty clear: the company believes in commercial exploitation of the opportunities provided by the growing concerns for the security environment. Indeed, the company is oriented to exploit its twofold presence in both the defence and security segments to address "*the emergence of new types of threats - from terrorism and organised crime to drug trafficking, mass immigration and cyber attacks – [which] defence organisations alone are not fully equipped to contend with the changing risks*"[185], and which therefore require a convergence (political as well as technical) between security and defence approaches.

EADS is a global leader in the field of aerospace, defence and related services. It reported revenues of more than 43 billion euros in 2008. The company is structured into four divisions: Airbus, Eurocopter, Astrium, and an integrated Defence and Security division. EADS Defence & Security realised a turnover of EUR 5.7 billion euros in 2008, which represents about 13% of the total turnover of the company. However, only 3% of the revenues of the division come from non-defence market areas.[186] The largest share of EADS's industrial activity, thus, is still oriented towards its two classic markets of reference: civilian[187] and defence[188].

---

[183] Thales, in the frame of the consortium Transtec Gotthard, will deliver, set up and test a railway signalling system for the Saint-Gothard tunnel. It will comprise electronic engaging systems, an ETCS system of 2nd level and a centred check system for the traffic. This contract costs around EUR 72 million.
http://www.thalesgroup.com/Press_Releases/Markets/Security/2009/091215_D3S_Thales_equips_the_world%E2%80%99s_longest_tunnel_with_complete_signalling_solution/

[184] Official presentation of Luc Vigneron, *Towards a stronger Thales*, December 2009. Available at: http://www.thalesgroup.com/Workarea/DownloadAsset.aspx?id=11101&LangType=2057

[185] Thales' Security Division webpage: http://www.thalesgroup.com/Markets/Security/What_we_do/

[186] EADS Annual Review 2008,
http://www.reports.eads.com/2008/en/s/downloads/files/annual_review_eads_ar08.pdf

[187] In 2008 Airbus revenues accounted for 27.4 billion euros (61% of the total share). Eurocopter largely operates in the civilian market, and also Astrium portfolio include some civilian activities such as telecommunication, observation, scientific and navigation satellites.

Defence and Communication Systems (DCS), a business unit of the Defence and Security Division, aims at developing systems capable of interconnecting a large range of platforms under a unique network (LSI – Large System Integration). This should provide solutions to reduce risks in border surveillance, coastal and maritime surveillance, crisis and emergency management, protection of population and critical industries and identity management (all these solutions are part of the so called "global security vision"). It proposes solutions for critical mission communications, under TETRAPOL, TETRA and P25 standards, that are dedicated to public security, civilian protection, transport and industry. At the same time, the Network Centric Operations Simulations Centre (NetCOS) provides the systems design framework and core competencies for system-of-systems concept development. This federated net-centric simulation environment creates a tool to be prepared for accidents, civil incidents, military missions and natural disasters.[189] However, it is interesting to note that only 3% or 168 million euros of total sales went to the European civil market[190], showing how, at present, defence institutions (MoDs) are the most relevant potential customers for such high-technology integrated systems.

The strategic priority of EADS is indeed to develop its security activities worldwide, trying to develop markets abroad as they are considered more profitable. EADS radio devices are used in more than 65 countries, including China and Brazil, and the company is developing its security businesses in the United States through the acquisition of the California-based PlantCML (provider of communications and response technologies for public safety, business continuity and homeland defence). The company supplied a maritime surveillance system to the State of Qatar in 2007, and provided equipment for border security and protection of critical infrastructure to Romania and Bulgaria. As already mentioned, EADS recently secured a contract with Saudi Arabia worth billions of dollars for a border security system. Similar to Finmeccanica, for the time being EADS considers "High-end" security mainly an as export market because it sees more procurement opportunities from public and private authorities abroad than in Europe. The recent creation of a Middle East

[188] In 2008 the Military Transport Aircraft Division revenues accounted for 2.8 billion euros (6.2% of the total share). The other defence revenues come from Eurocopter's and Astrium's military activities, and from four of the five branches of the Defence&Security Division.
[189] EADS Defence & Security, official webpage: http://www.eads.com/1024/en/businet/defence/defence.html
[190] EADS, *We Have What It Takes. EADS Annual Review*, 2008. Available at: http://www.eads.net/xml/content/OF00000000400004/4/94/42517944.pdf

and North Africa business unit is a good illustration of this trend.[191] However, EADS remains also positioned at EU level, particularly through its participation in the EC 7th FP research programmes, which could shape any future EU security market.

EADS illustrates the paradigm of a European security and defence system integrator which has a double vision of the security market: export for today and prepare for EU development in the future (the same strategy pursued by Finmeccanica). Like the Italian company, EADS is prepared for potential growth in the "High-end" security market, developing some dual-use platforms that respond today, or could respond tomorrow, to emerging needs coming from both the security and defence sectors. This trend is currently evident within the EADS space division, as well as in those of Finmeccanica and Thales, which works both on the satellite and services sides, developing a large number of dual-use space based UAVs aimed at addressing the presumed converging security and defence markets.

The **Safran** Group, which can be classified as a sub-system and technology provider, is a company we have identified as having a successful business strategy in both the defence and the security areas. It has achieved these results through a strategy of acquisition and technology development. Safran's 2008 turnover is 10.3 billion euros, with 16% of the business in the "defence and security" area. According to the figures available for 2009, Safran's turnover is 7.5 billion euros for the first 9 months of 2009, with 485 million (6.5%) for security.[192] The availability of specific security data indicates two trends. First, the emergence of a security market has justified for Safran the separation of its security division from other businesses. Second, it shows Safran's particular interest in separating the security business from defence, in order to pursue targeted growth in the security sector. Here again, the development of the security business in itself seems to be a pre-condition for further synergies and growth within the blurred area between security and defence.

In December 2009, French media speculated on a large deal between Safran and Thales. Safran

[191] Christopher Foss, *EADS to refocus Middle East business strategy*, Jane's, February 2009, http://www.janes.com/events/exhibitions/idex2009/sections/daily/day3/eads-to-refocus-middle-ea.shtml.

[192] Safran, *Safran reports nine-month revenue 2009*, Press release available at the official webpage: http://www.safran-group.com/site-safran/presse-et-medias/communiques-de-presse/2009/article/safran-publie-son-chiffre-d

would acquire the security activities of Thales, in exchange for its defence activities. If this deal were to be realised, France would have a very large defence player in the shape of Thales, while Safran would became the larger national security player. It would also be fair to assume from this potential development that neither company has found particular benefit from a mixed defence and security business model.

Sagem Sécurité, part of Safran, is a world leader in biometric technologies for fingerprint, iris and face recognition, and a major player in smart cards, identity management solutions, access management and transaction security, with solutions that meet emerging needs for the safety and security of people, companies and countries.[193] It offers a wide range of tools targeting police enforcement, among which we can distinguish APFIS (Automatic Palm and Fingerprint Identification System), identification solutions, border control systems[194], road safety[195] and access control systems. Safran companies include also Sagem Identification, Sagem Orga and Sagem Trak.

Operating via Sagem Sécurité, Safran has a long-standing experience in the security market, even more than Thales and EADS. It did not, therefore, face the difficulties encountered by newcomers, especially at that level, such as Diehl. Sagem Sécurité recently decided to continue expanding in the security market via the acquisition of 80% of another security company - GE Homeland Protection, worldwide leader in airport scanners. Alongside its development efforts in the security sector, Safran remains also well positioned in the defence market and uses its defence technology for security applications (this is the case for tactical UAV, where they also have a position of leadership). For instance, Greece is currently using the Sperwer UAV for border surveillance. Safran estimates that the small (less than 1.2 tonnes) Medium Altitude Long Endurance (MALE) drone is a promising market, that could have both defence and security applications. The problem at this level is the lack of a clear specification of defence needs. Safran is, however, developing a demonstrator in this field and intends to pursue investments.

---

[193] Safran Security Division official webpage: http://www.safran-group.com/site-safran-en/security/?331

[194] Safran has won the 2009 Frost & Sullivan European Border Security Product Innovation Award for its automated biometric border control solutions). See Sagem Sécurité Press release, http://www.safran-group.com/site-safran-en/press-media/press-releases/2009-447/article/sagem-securite-announces-that-its-10172

[195] *"Sagem Sécurité (Safran group) has signed a contract with United Telecom, a Russian company specialised in the integration of intelligent transport systems, to supply and install 110 MESTA automatic speed control radars in Belarus, along with an automated ticket processing centre."* SAGEM Sécurité Press release, 2010. Available at: http://www.safran-group.com/site-safran-en/press-media/press-releases/2010-698/article/sagem-securite-s-automatic-speed

Within the second-tier of the industrial pyramid, there are companies firmly and successfully positioned in the defence market. The best examples are operators in the space sector, where a limited number of companies (subsidiaries of the first tier, such as TAS and EADS Astrium, or niche players, such as Cobham[196]) are providing key solutions for the defence segment. Yet, they are also playing a growing role in the security sector. This relevance of the space industry as a participant in the blurring of the defence and security sectors is a key aspect. It corresponds to an evolution of the mission/demand side (see Chapter 1) for space technologies, linked also to the need for new sensors for monitoring (see Chapter 2). As space industries traditionally provide technologies for defence and civilian markets[197], civilian and military satcoms or civilian and military EO satellites have strong commonalities and are developed in parallel. From an industrial and technological point of view, space is historically a sector of convergence between defence and civilian missions. Since the 1990s, the evolution of space missions has brought some EU countries to develop new types of capabilities in order to fulfil flexible evolving needs (see Chapter 1). Dual-use programmes have been developed in Italy and France. The development of a dual use policy is largely supported by space industries who wish to increase or maintain their market, also developing European systems. Furthermore, EU flagship space programmes such as GALILEO and GMES, also "blurred" by themselves, represent an important development opportunity for European space industries (see Recommendations).

To summarise, space companies in Europe have always relied on strong public demand, coming from either the civilian or defence side. The evolution of space missions has created opportunities in the blurred area for all EU space industrial players (EADS Astrium, ThalesAleniaSpace, Telespazio, Fuchs Group). Space companies represent a mix of technical dual use developments (sensors, already mentioned in Chapter 2), blurring of missions and also of demand (with Italian and French dual-use systems), a trend that could be fostered by further EU policies to strengthen the space sector.

[196] Cobham management structure is based around four divisions: Defence Systems; Mission Systems; Aviation Services; Avionic and Surveillance. Within the Avionic and Surveillance division, the Surveillance sub-unit is a World-leader in the field, providing products and integrated surveillance solutions (audio, visual, tracking, locating, cellular, sensor, covert surveillance and search and rescue solutions) to law enforcement, military, national security and border patrol, and civil agencies.

[197] This has been emphasised with regard to EADS Astrium, footnote 26.

The third tier includes a significant number of companies, more than 80 in Italy[198] and an unclear but certainly greater number in France[199], providing parts and niche capabilities. They include specialised defence contractors, linked with second and first tier defence producers (for example the Italian company Aerea, specialised in military aero structure, such as missile rails) and SMEs operating across different markets, therefore already present directly (thanks to niche products) or indirectly (providing parts for joint security and defence solutions) in the "blurred" area of the market.

The main findings of our research about the strategic approach of defence companies to the "blurred" market segment (crisis management and "High-end" security) can be summarised as follows. In general, many companies encounter difficulties in trying to access a market that is complex and presents many obstacles, as discussed in Chapter 3. Only dedicated security units or controlled companies prove to be successful, in particular those who have significant experience and understand the culture and demands of both military and non-military security actors. Companies have developed various approaches and attempts. Some have tried to influence the behaviour of demand in order to recreate the same market conditions found in the defence sector in security, for example special relations between customers and suppliers, and high technology equipment. Others have tried to make use of their defence technology for security application, exploiting their technological knowledge to offer interoperable solutions to different customers. Finally, some have made direct acquisitions of players already operating in the security market to optimise complementarities. Despite such attempts, we cannot identify a significant entry of defence companies into the security market or, furthermore, into the blurred area. In terms of activity, positioning and turnover, the security sector remains significantly smaller than defence. For those "security and defence" companies, security is still a business awaiting development based on a potential for the emergence of new EU public demand and driven by the funding of European security research programmes.

[198] Aziende Italiane per l'Aerospazio, la Difesa e la Sicurezza (AIAD*), Relazione Esercizio 2007*. Available at: http://www.aiad.it/documenti/RelazioneAnnuale2008.pdf.

[199] There is no precise data about the number of French third tier of subcontractors. The GIFAS (Groupement des Industries Françaises Aéronautiques et Spatiales) only mention 268 firms without detailing the number of SMEs: http://www.gifas.org/en/pages.php?tab=gifas&sub=1

4.3.The approach of security companies in the blurred area

4.3.1. Overview of security suppliers

According to our findings, a comprehensive mapping of European companies operating in the field of security does not exist. This is also the case for the defence industrial base, but the security supplier base is even more difficult to identify, categorise and structure. It is dynamic, since it can cross all sectors of the economy. In addition, no systems of classification, with legal requirements to subscribe to specific registers, exist in the security field, while this is the case for defence companies. It is therefore extremely difficult to identify who is actually present in the security field and how strategies are developed. Any analysis of the security sector is limited by the amorphism of the sector. Estimates of the size of the security sector are also extremely variable. One of the most recent studies on the competitiveness of the European security industry[200] estimates the range of the market to be between 26 to 36 billions euros. The wide gap between the low and high estimate testifies to the uncertainty that exists regarding the actual size of the market and its players.

The only way to obtain an overview of the industrial players in the security area is to go through all the existing lists of associations and networks operating in the field, especially those that have emerged over the last two years: in particular the European Organisation for Security (EOS), the European Security Directory (ESD) or the European Security Research and Innovation Forum (ESRIF).

The membership of EOS, ESD and ESRIF confirms that the industrial landscape in this segment is extremely heterogeneous and difficult to structure, even if system integrators are systematically present.

- EOS was created in 2007 by European private sector suppliers and users from all domains of security solutions and services in order to help European security stakeholders to develop comprehensive security strategies at national, European and international levels. Members are composed of around 29 major European defence and security stakeholders, representing around 20% of the global security market. Members range from security

[200] ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009, pag. vi.

solutions and service providers to technology producers. They represent many sectors of the economy (ICT, defence, civil security, energy, transport, finance, services and research)[201] and are mainly positioned in the blurred area of the market ("crisis management" and "High-end" security). According to EOS estimates, 2 million people are estimated to be employed in the worldwide security industry with a yearly turnover of some 100 billion euros in 2008.[202]

- ESD was created as a tool for building contacts between suppliers and potential customers. The 2009 Buyer's Guide identifies 84 actors including companies, groups, research centres and university labs. They are listed by country and alphabetical order, but also by technologies, equipment and platforms based on the STACCATO taxonomy. As underlined in the document, however, it does not cover all the European players; the majority comes from France, Germany and the United Kingdom. The listing is still at an early stage, though, and not only includes industrial players, but also institutions and consultancies. The guide cannot be considered, either, as providing a comprehensive mapping of the security industrial base. It in fact shows how the borders of the security sector are sufficiently porous that industrial blurring (twofold, according to EDS, because it would include also the civilian market) seems to be emerging.
- ESRIF is a voluntary strategy group which aims to bring together the demand and the supply side of security research (industry, public and private end-users, research institutions, NGOs), with a total of 645 members from 31 European and other countries.[203] It was created in 2007 with the intention of developing a mid and long term Joint Security Research and Innovation Agenda that would link security research with security policy making. The ESRIF process relies on 11 Working Groups, each dealing with a particular aspect of security; this division emphasised the holistic approach to security adopted by ESRIF. Only two of these Working Groups are chaired by industry representatives. Regarding the involvement of industry in the ESRIF process, we notice

[201] EOS Members : Altran, Amper, ASD, CORTE, Atos Origin, Avio, BAE Systems, Bumar, CEA, Cotecna Inspection, D'Appolonia, Diehl, EADS, Edisoft, Engineering, G4S, Hellenic Aerospace Industry, Kemea, IBM, Indra, Iveco, Sagem Sécurité, Selex Sistemi Integrati/Finmeccanica, Siemens, Smiths Detection, Teletron Euroricerche, Thales, TNO. Sectors of common interest are border surveillance, critical infrastructure protection, and civil protection. http://www.eos-eu.com/AboutEOS/QuestionsAnswers/tabid/151/Default.aspx.

[202] This figure was published on EOS homepage (http://www.eos-eu.com/Home/tabid/36/Default.aspx), accessed July 2009.

[203] As of November 2009.

the presence of the big defence corporations analysed above, i.e. EADS, Finmeccanica, and Thales, together with SAGEM, a Safran Group company, Petards Ltd. belonging to the BAE Group, and Saab. Other firms participating in ESRIF are the big security companies, Smiths Detection and FREQUENTIS. Representatives of national industry communities[204], of research establishments[205] and of academia are also involved in the ESRIF processes.

These findings allow us to draw two main conclusions. First, the security market is definitely less mature than defence, since the only two specific security companies involved in the ESRIF framework are much smaller than their defence fellows.[206] Secondly, the large European defence companies are still largely involved in the security sector.

We have tried to compare these sources and classify the listed companies, excluding consultancies, research institutes and other organisations. Table 4 provides the main results of this comparison, extracted from a comprehensive table attached in Annex 4. Companies have been clustered by size and type. We have used the formal EU categorisation[207] which considers a "small company" as an enterprise with less than 50 employees and up to 10 million euros in turnover, while a "medium company" employs fewer than 250 and has a turnover of 50 million euros. Companies are categorised as:

- **CIV**. Produces goods for the civilian market excluding security functions (i.e. air traffic management systems)
- **SEC**. Produces goods specifically designed for security use.
- **DEF**. Produces goods designed for defence use.

However, most of the companies are active in two or more of these fields.

[204] For instance: Security & Resilience Industry & Suppliers Council (RISC),
[205] For instance, TNO- Netherlands Organisation for Applied Scietific Research.
[206] Smiths detection 2009 total revenues amounted for £ 501million; FREQUENTIS 2008 total revenues amounted for 141 million euro.
[207] On 6 May 2003 the Commission adopted Recommendation 2003/361/EC regarding the SME definition. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

Table 4: List of European security companies

	EOS (23 companies)		ESD (28 comp.)		ESRIF (10 comp.)	
Mainly **SEC**	6	**26%**	17	**60,7%**	3	**30%**
Mainly **DEF**	9	**39%**	6	**21,4%**	3	**30%**
Mainly **CIV**	6	**26%**	5	**17,8%**	4	**40%**
Large	20/23	**87%**	17	**60,7%**	9	**90%**
Medium	1/23	**4,3%**	6	**21,4%**	1	**10%**
Small	2/23	**8,6%**	4	**14,2%**	0	**0%**

Source: EOS, ESD, ESRIF. Data elaborated by IAI.

We can observe that large companies represent the clear majority of EOS and ESRIF industry members (87% and 90% respectively). In ESD their presence is less predominant (60%), and we can observe higher involvement of medium and small enterprises.

Another interesting point relates to the involvement of security companies. Around 61% of the companies listed in the ESD are involved mainly in the security field, while the ratio of defence and civilian companies is much higher in EOS and ESRIF (respectively 39 and 26% in EOS and 30 and 40% in ESRIF).

In addition to the lists we have compared, the European Commission services have also created their own database, especially for the sectors of activity of DG JLS (corresponding to our “High-end” security area), based on their own network and contacts. We can also identify many industrial players by looking at the list of participants in the European research framework programme. In order to complete the overview, it is also possible to find information about the

main industrial players in sector studies dedicated to the various segments of the "High-end" security market.[208] None of these approaches, though, is systematic or exhaustive.

In conclusion, any attempt to classify the security sector and its industrial composition is extremely difficult since no comprehensive mapping and taxonomy exist in this market segment. Defence corporations, civilian companies and security firms are all, in certain cases, included in a broad definition of the European security sector. These findings show that:

- The industrial security sector, post Cold War and the 9/11 terrorist attacks, is less known than expected. Companies operating in the market are heterogeneous. Pure security corporations are still a minority, while there is a large number of security SMEs.
- The defence industry has a significant interest in the security segment. Large European defence corporations are actively participating in the definition of the security sector through their presence in both EOS and ESRIF. Since these corporations are mature and well-organised, in particular when compared with those operating in the security sector, they have the skills and resources to shape supply in the security sector.

4.3.2. Security suppliers' approaches towards the blurred area

Here we are looking at whether "non-defence" companies, therefore the rest of the security sector, have also detected opportunities in the segments currently being analysed ("Post Cold War" defence and "High-end" security) over the last two decades.

First, we can point out that the defence segment of the potential blurred market has also appeared to be attractive for security companies in general. There is indeed a tendency by security suppliers to try and approach the defence market by selling civilian or security products to MoDs (logistic, IT, communication, sensors) or components and spare-parts for the military.[209] In limited

[208] For example, the main industrial players for x-ray equipment for the protection of critical infrastructure (air transport in particular) are Smiths Detection (EU) GE Homeland Protection (US), L3 Security and Detection System (US), Rapiscan Systems part of OSI Group (US). Medium sized companies are Reveal Imaging (US), American Science and Engineering (US) and Gilardoni (EU). See ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009, pag. 109-113.

[209] For example, the ATR 42 civilian plane has been transformed by Alenia Aeronautica into a "surveillance plane" in order to tackle the monitoring need linked to "Post Cold War" defence and "High-end" security missions. This is a

cases, we can identify examples of upgrading technology to meet military requirements. However, this trend is difficult to quantify, both in terms of the number of companies following this approach and in terms of turnover, for the reasons indicated in the previous paragraphs.

As emphasised in previous chapters, the budgetary pressure on MoDs and the need to make use of civilian equipment for the new military missions, such as crisis management, are certainly amongst the main reasons for security companies considering the defence market as a new opportunity. There are many theoretical advantages from entry into the defence market: higher margins thanks to limited competition, a reduction of risk for the company, a possibility for economies of scale based on common technologies and more generous R&D funding from MoDs and MoIs.

The limited size of many security companies and their capacity to offer solutions to a large number of customers, both public and private, based on off-the-shelf components, make their products in theory much cheaper than the tailored systems offered by defence companies. There is therefore the possibility to compete on price. This is the case for products or equipment that are civilian in nature, such as IT and communication products. Many small companies find opportunities in the "crisis management" market, as we have seen in Chapter 1 (i.e. providers of civilian planes for surveillance, vehicles, and ballistic jackets, etc). In addition, more and more civilian companies are also trying to access the growing market of services (for surveillance and logistics in particular) and maintenance for military forces.[210]

As defence companies entering the security market have problems, also security companies trying to enter the defence market face difficulties and barriers. Their knowledge of defence customers and procurement rules often remains limited. Moreover, the traditionally close relations developed between established defence companies and MoDs represent an entry barrier for newcomers to the market. Some security companies have therefore tried to hire former military

clear example of how a civilian origin product is customised and transformed to respond to a potentially blurred market.

[210] See the list of companies registered in the TPLS web site of EDA (platform for logistic support for crisis management).

high-ranking personnel[211] in order to increase knowledge of the defence customer culture, imitating defence companies which traditionally rely on former officers for their contact with military customers. Others have established joint ventures with a traditional defence supplier.[212] However, such alliances, often unbalanced, generally do not last.

The fragmentation of the market in closed national markets is also a complicating issue, especially for medium and small size security companies. Finally, many also face high costs to comply with defence customer procurement requirements that are either not possible to reach, in terms of standards, or too tailored, therefore requiring modification to the basic product, which changes the whole cost structure. MoDs also tend to limit the use of civilian technology incorporated in military solutions and to impose strict rules for re-exporting.

If we now look at the "High-end" security market, we can also identify a growing participation of security companies in response to the changing international environment and to the introduction of security related regulations made after 9/11. For instance, the introduction of mandatory Automatic Identification Systems (AIS) for large vessels by international regulation has increased the production of such equipment during recent years. The number of companies producing these systems has been growing. The same is true for security systems for air cargo protection, a sector where after 9/11 we can observe a shift to mandatory ones, including 100% screening of carry-on and hold luggage. These requirements are more demanding than the basic x-ray baggage screening adopted in the 70s, and have progressively led to the development of more sophisticated technologies for detection. Also, the market for CBRNE detection equipment has expanded, because of the protection of critical infrastructure, but also the needs of private operators such as banks and supermarket chains, providing new opportunities for industry. We can make the same observation for the biometric market as well.

[211] One relevant example is the former Italian Chief of the Defence Staff, Gen Mario Arpino, who is currently President of the Vitrociset Group, an high-technology corporation operating in the informatics, electronics and integrated logistics sectors. Vitrociset designs, produces, integrates and manages computer and electronic systems both in the security and defence domain.

[212] This is the case of the two joint ventures between the French group Alcatel and the Italian Finmeccanica, Alcatel Alenia Space e Telespazio. After one year from the creation of the two companies, Alcatel sold its share to Thales.

So, the increase of demand in the "High-end" security area has had an impact on industry. This impact remains difficult to quantify, though, without many specific market sector analyses which are not yet available – although some efforts have recently been undertaken, as seen in the recent Commission study on the competitiveness of the security industry performed by ECORYS. However, even the ECORYS study reports the impossibility of scoping the security industry from available sources of industrial statistics, and the general lack of statistical data available from the industry itself. Therefore, the ECORYS study presents approximate estimates, and only for some key market segments[213].

The above general trends can, however, be illustrated with some examples.

- The Italian medium-sized company Vitrociset, a specialised security company in the air control sector (Air Transport Movement, ATM), has recently moved into the space sector and into defence related applications, such as mission planning. The approach chosen by a former Chief of Defence Staff experienced in procurement and aeronautics, responsible for this area, is focused on the identification of common integrated solutions for both security and defence customers in areas such as VTS. At the same time, the company has raised the interest of the main Italian defence player, Finmeccanica, which holds a stake in the company.

- The French company Cegelec provides several MoDs in Europe and worldwide with solutions and services in multi-technical engineering (access control equipment, telecommunication systems, supervisory control and data acquisition) and logistics. It is one of the eight largest suppliers to the French Defence Procurement Agency. Cegelec safeguards sites that are classified as the most high security defence installations, such as the Parisian facilities and those of the Army and Marine Forces Rapid Reaction Command Posts (citadelle of Lille).

- Many IT and electronics companies, such as Smith Detection, IBM, Fujitsu or Siemens are also involved in this process. The same or slightly modified product is often proposed with

[213] As in ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009, Executive Summary, page v.

success in response to security and defence needs. Smiths Detection, one of the five divisions of Smiths Group, is strongly connected to the defence sector. It is a global leader in the provision of threat detection (including CBRNE) and screening technologies for military, transportation, homeland security and resilience applications. It has also developed its activity in the "High-end" security area (air transport protection) after 9/11 by acquiring Heimann Systems GmbH in 2002 (market leader in x-ray security products). Other companies such as SAM Electronics (DE) or COMAR Systems and SATAMATICS (UK) have expanded their activity and production of Automatic Identification System (AIS) in response to the need to increase control of vessel traffic. A Siemens and IBM consortium have won the German MoD Hercules contract to provide and manage non military ICT. IBM is providing ICT support services to European MoDs, such as an Italian contract for C41 data elaboration support.[214]

Another interesting approach to better qualify the evolution of the industrial sector towards the blurred area deals with the evolution of technology.

4.4.Technology-driven industry consolidation

The maturing of some "new" technologies is beginning to drive consolidation in some industry sectors, a consolidation which may well happen across the security-defence continuum. Biometric technologies provide a good example. They include hardware (sensors and devices) and hardware-dependent software algorithms. Increasingly, even if there are some specialised sensors being produced for "High-end" security applications, most sensors are mass produced and this is causing a fall in the relative price of hardware. It is the sophistication of the algorithms that differentiates products in the eyes of users, as does the ability of companies to tailor their products to solve particular user problems. In these conditions, it is the case that systems integrators such as EDS

[214] During our interviews, IBM representatives confirmed that in the IT domain there is continuous technological development which is not linked to the defence or civilian nature of the market. Some customers are very demanding and push for new technological solutions. For example banking activities requires a high level of security for their data solutions. On the other hand, the Israeli MoD is pushing for the development of innovative data processing for security.

and IBM, as well as security-focused companies, are forming strategic alliances with biometric suppliers, as biometrics becomes an integrated enabling technology.[215]

There is also an expectation that defence contractors may make acquisitions, as biometric technology companies prove the strength of their technologies and defence contractors integrate such technologies into complex security systems. For example, in April 2009, Safran completed the acquisition of Motorola's biometrics business and this will now be integrated into Safran's SAGEM Securité business. This is one example of how the technology strategies of defence companies may also drive consolidation.

We have noted that many technologies of growing importance to both the defence and civil security sectors are not necessarily the ones traditionally and successfully developed by defence companies. Increasingly, defence contractors are pursuing more "open" innovation strategies, seeking to access such technologies through their supply chain, through alliances with other companies, and sometimes through the acquisition of companies with valuable technologies, as we have already mentioned in this chapter. This is a strategy that has been actively pursued by some U.S. defence companies, such as Northrop Grumman, Lockheed Martin and Raytheon.

Some defence companies possess distinctive strengths in some technologies with security applications. These defence companies tend to have technological strengths in these sectors: high performance, high integrity and system critical technologies including photonic/optical materials and device technologies; sensor technology and components; information technologies; artificial intelligence and decision support; simulation tools and software; information security technologies; and communication technologies.

Those distinctive strengths also tend to focus on the integration of a range of (sometimes generic) technologies into complex systems, as systems engineering is another area where the aerospace and defence sector has traditionally been strong. Defence industry capabilities in systems engineering are highly applicable to complex civil security systems.

For example, Finmeccanica's SELEX Communications has well-developed capabilities in secure communications technologies that are applicable in both defence and security applications. BAE Systems has strong capabilities in secure computer systems, information and networks

[215] Frost & Sullivan, *European Homeland Security: A Market Opportunity Analysis,* San Antonio, 2005.

technologies and systems integration. Significantly, after attempting to grow these capacities organically, it made the decision in 2009 to acquire DETICA (a specialist “High-end” security company), in part as a way of strengthening its marketing capabilities in the security field

This technology-driven industry consolidation may help strengthen European industrial competitiveness where it allows strong large and competitive companies to emerge and where it increases economies of scale and scope. Equally, however, consolidation may have consequences for innovation in Europe with an eventual impact on the quality of the product and systems available to users, and may also have a consequence for wider European innovative performance. This kind of vertical integration through the acquisition of technology suppliers by large systems integrators may reduce innovation, as large systems integrators choose to source from their own internal technological capabilities, even when these may be inferior to those available through the external supply chain. Consolidation may also reduce the number of high technology SMEs in some sectors, with potential consequences for European economic performance and innovativeness.

4.5.Conclusions

Our analysis shows that blurring between the defence and supply sectors does affect the supply side of the market, but its effects differ by company type.

System integrators (large companies) have developed strategies for security business, based on the assumption of significant, post 9/11 growth in the market. In their perception, the development of the security market would generate attractive returns, largely by translating defence capabilities into security products and services. The growth of the security market would, under these conditions, foster a positive blurring between security and defence. In reality, though, the development of this “High-end” security market has been slow, as security tends to be a fragmented market with different cost structures. Nevertheless, we have identified a reshaping of the supply side, with the emergence of dedicated security subsidiaries, able to act autonomously and adapt to this new market. For these system integrators, the development of a large scale security market is the principal requirement for gaining synergies from the blurring. The

development of a European public security market is perceived by these companies as a necessary condition for the achievement of profitable business. The space sector represents the first step towards the development of dual-use security and defence systems. As we will analyse in our recommendations, the space sector can be considered as a model for the development of common European capabilities for dual-use. Space is a key part of an “awareness and communication” chain of systems and technologies, but other technologies and platforms are involved. Thinking in terms of platforms a set of satellite, UAV's and ground based services could contribute to this dual use trend, translated into programmes able to shape demand.

For SMEs, the situation is different. There are two types of SME business to consider. First, they may act as a sub-contractor of a system integrator, in which case their growth will depend on the success of the large company. For this reason, there cannot be an “absolute” division between SMEs and large companies. Second, they may operate autonomously, thus it is likely that their activities will be on a smaller scale and they would benefit from an expanded blurred market by being able to supply both the security and defence sectors with their technologies. The security market, at both the public and private levels, is characterised by SMEs competing among themselves on price and services. After 9/11, the “High-end” security segment was expected to grow remarkably, and to offer further market opportunity for these companies, though not all these expectations proved to be well-founded.

Furthermore, we have indicated how technology-driven industry consolidation may help strengthen European industrial competitiveness. We have shown that some defence companies possess distinctive strengths in some technologies with security applications and identified processes and barriers to the transfer of defence-origin technologies to security applications.
We have emphasised that the possession by a defence company of a valuable defence-origin technology is a necessary, but not a sufficient, condition for its transfer to the security market. This has led us to emphasise the business conditions that are necessary for a defence company to successfully transfer a defence-origin technology into the security sector. These include the possession of the necessary complementary capabilities, including a detailed understanding of the distinctive features of the security customer, and the development of a viable business model.

5. Opportunities and challenges for industry

5.1.Introduction

In the following chapter, we will try to identify the opportunities and challenges that arise for industry from blurring between the defence and security sectors. To achieve this, we will first review the complexity of this "blurring" and illustrate, based on findings from previous chapters, that there are limits to the effects of blurring, which are likely to endure. Understanding these limits is important for identifying which challenges may be turned into opportunities, possibly by public intervention, and which conditions will require industry to adapt its strategy and secure success.

Since the outlook for research investment has already been addressed in chapters 2 and 3, we will concentrate here on current and future procurement trends and what they could imply for industry. Our analysis will be based on defence and security capability needs in the blurred areas of crisis management and "High-end" security. We will verify whether these needs can lead to concrete and substantial market opportunities. In so doing, we will also try to distinguish which industry (defence, security) is facing which opportunities and challenges in which market segments (defence, public security and private security).

5.1.1. The Limits of blurring

The previous chapters have shown that blurring between security and defence takes different forms, reaches different levels and even has different meanings in the areas "missions", "technology", "demand" and "supply".

It is generally recognised that the main security threats today are not large-scale military conflicts, but regional crises and threats from non-governmental actors, in particular terrorism and organised crime. The latter often operates globally, in transnational networks, blurring the dividing line between internal and external security. Facing such threats, governments in the EU and worldwide have redefined their security and defence policies and started to develop a

comprehensive approach, combining a broad spectrum of military and non-military instruments. Hence, blurring has already become a reality at the political and conceptual level, and this process is likely to continue as long as there are no fundamental changes to be expected in the strategic environment.

As a consequence, the borderline between defence and security missions has blurred as well (see Chapter 1). Traditional missions continue to exist on both sides, but missions related to post Cold War and post 9/11 threats are to a large degree shared (crisis management, the fight against terrorism and organised crime, protection of borders and critical infrastructures). This comprehensive security approach, developed at the political and conceptual levels, means that the blurring of the dividing line between defence and security missions is likely to continue, including new areas such as cyber-security and the security of energy supplies.

On the basis of shared missions, armed forces and security services have also developed, at least in part, similar capability needs. As we have demonstrated in paragraph 1.3.4., capability and functional needs overlap, in particular in the areas of protection, communication, command and control and information gathering and in functions related to these areas, such as detection, identification & authentication; situation awareness; risk assessment, modelling, impact reduction; communication; information management; positioning and localisation. What is more, the technology base for these capabilities is in many cases the same. As we have seen in chapter 2, blurring at this level is particularly evident in ICTs, technologies underpinning UAVs, sensor technologies and components.

Armed forces and security forces may, however, share the same missions and capability requirements, although most of the time their roles and tasks differ. The fight against terrorism, for example, is a completely different challenge for armed forces and police forces. Each of them contributes to tackling the same threat and fulfils, therefore, the same mission, but their respective tasks and roles remain specific and (normally) separate. Such differences are absolutely compatible with a comprehensive security approach. The most effective way to fight today's

security threats is precisely to draw on a broad variety of means and combine them into a coherent strategy. To achieve this objective, a high degree of cooperation and information sharing at the political and strategic level is necessary. Ideally, this should be complemented at the operation level with common planning. However, improved coordination does not mean that defence and security actors would lose their specificities when they share the same missions (and even when they participate in the same operations). Each of them will still make his specific contribution in his own field of action to fight the same threat from different angles.

This is the case also when actors take over new roles. In some crisis management operations, for example, armed forces perform policing, reconstruction and even medical support, as long as the operational environment is too unstable and insecure for the deployment or autonomous action of non-military actors. Armed forces also go beyond their traditional role when they support security forces for the protection of critical infrastructures and maritime borders. In these cases, however, armed forces intervene precisely because they have specific equipment which allows them to do what non-military actors are not able to do (alone).

Differences in roles will persist in the future, even when blurring leads to a redefinition or redistribution of tasks. Control of air space, for example, has been traditionally a military task closely related to air defence against military attacks from abroad. In the current threat environment, air defence increasingly becomes air policing against possible terrorist attacks. Today, this task is performed mainly by traditional military aircraft. In the future, new technologies may enable security services to take over this task, for example the ground control of hijacked civil aircraft. In this case, again, roles and responsibilities change, but equipment needs remain specific to the respective service and its tasks.

All this has important consequences for the market structure of the blurred area. Different services need different equipment, even when they are involved in the same missions. When common capability needs are translated into concrete equipment requirements, commonality often ends, because applications and/or technical requirements are different for the fulfilment of

specific tasks and roles. Fragmentation of the demand side between defence and security, and between the various security actors, is thus to a considerable degree a logical consequence of role specialisation.

This neither means that there would be no common requirements, nor that the respective equipment would always differ completely. In areas where security and defence actors cooperate together on the ground, there is a clear need for interoperability, in particular of communication means and information management systems. In other areas, different services have the same capability needs for which the technology base is the same and the respective application very similar (i.e. for detection or identification).

It does not mean, either, that current fragmentation of security and defence demand in Europe will always follow rational lines, and that there will be no room for improvement. In the field of defence, harmonisation of military requirements between European armed forces has been recognised for a long time as a necessity for improving interoperability and reaching the production volumes necessary to achieve competitive costs. In the field of security, decentralised procurement systems often lead to fragmentation of demand, even when services have the same needs. This inevitably creates unnecessary duplication, lack of interoperability and extra costs. Resolving such shortcomings would make procurement mechanisms more efficient and help to save scare resources. However, it is unlikely fundamentally to change the market situation in the "High-end" security area.

To conclude, the blurring of concepts, missions and even capability requirements does by no means automatically lead to a blurring of demand. It is true that security and – even more so - defence customers increasingly try to identify common capability requirements. However, differences in roles and tasks persist and set natural limits to the possibility – and the need – of translating common capability requirements into common equipment needs across different services. Consequently, the blurred market along the defence and security dividing line will probably remain complex and fragmented. For companies from both the security and the defence

sectors, this offers challenges and opportunities in equal measure, but makes it almost impossible to draw clear-cut conclusions for “industry” in general.

5.2. Opportunities and challenges in defence markets

5.2.1. The defence capability development processes

The shift from traditional defence missions to post Cold War missions has not only created new defence capability needs, but has also changed the way in which these capability needs are defined. During the Cold War, defence planning followed an equipment-based approach, which focused on developing the entire range of air, naval and land equipment for territorial defence against a military enemy; the aim was to define the number of units, tanks, ships and aircraft needed for a clearly defined large scale military conflict. This approach is ill suited to today's security environment, where threats are asymmetric, interrelated, transnational and more or less unpredictable. Consequently, defence planners have started to move away from the traditional equipment-based approach towards a new capability-based approach, which is more flexible and aims at bridging the gap between the general objective of a mission and the set of tools which are necessary to achieve it. On the basis of threats and challenges, it defines capability needs, trends and shortfalls, and translates this into categories of solutions in terms of equipment needs. Therefore, as stated in the EDA’s Long Term Vision, “it is not just equipment, but more comprehensively strategic concepts, doctrine, training and organisation that will, in their combination, yield the desired effect”. [216]

[216] EDA's “Long Term Vision for European Defence Capability and Capacity needs”, endorsed by the Steering Board on 3 October 2006 gives a perfect illustration of this new approach: "The key future force and capability identified are: 1) synergy (going beyond combined-arms warfare to coordination of effects with non-military actors, 2) agility (implying speed of reaction, deployability and mobility at the tactical level); 3) selectivity (meaning a wide range of capabilities and the means to ensure an informed and appropriate choice at each stage of the operation), 4) sustainability (suggesting the right logistic support, but also theatre access). These characteristics are translated into a Future Capability Profile for each of the main capability domains of Command, Inform, Engage, Protect, Deploy and Sustain. In working towards this capability profile defence planners will need to concentrate on some key issues, including: a) knowledge exploitation (improving intelligence, information and analysis at all levels and developing appropriate forms of network-enabled capability); b) Interoperability (through greater commonality of equipment and systems, and shared or pooled capabilities), c) manpower balance (finding ways to enable greater investment by cutting manpower numbers and costs) and d) Rapid acquisition (in particular quicker exploitation of new technology). See www.eda.europa.eu

The capability-based approach is most advanced in France and the UK. The EDA was already established as a “capability driven” Agency and continues to work along these lines. NATO has also started to transform its defence and armaments planning in the same direction. Both the EDA and NATO will contribute to familiarising Members with this new capability culture and will drive reforms to national planning processes. Budgetary constraints act as an additional catalyst for this shift. The capability-approach is therefore likely to become the general basis for the way military needs are formulated and translated into business opportunities for industry.

A comparison of the EDA Capability Development Plan and NATO Defence Planning Process reveals the principal capability needs and gives an idea of the procurements and business opportunities to which they could lead:

- Deployability, i.e. the capability to transport troops and equipment to distant places. This creates procurement requirements in the areas of airlift (i.e. A400M) and sealift (i.e. Fast ships).
- Engagement, i.e. the capacity to engage military forces effectively in hostile environments. This requires a broad range of military hardware, such as precision-guided weapons and offensive electronic warfare.
- Mobility, i.e. the capability to move rapidly on the ground during an operation. This creates new needs for logistical support (i.e. helicopters).
- Protection, i.e. the capability to protect forces during an operation. This necessitates an appropriate surveillance capability (i.e. UAVs) as a prerequisite for effective operations, as well as an ability to detect and then counter weapons which are not available to forces (such as CBRN weapons, IEDs and MANPADS).
- Information and communication, i.e. the capability to rapidly gather, treat and transmit information necessitates a broad range of C4ISR tools, including space-based earth surveillance and Software Defined Radio (SDR).

If, and to what extent, these capability needs actually create concrete business opportunities for industry depends first and foremost on budgetary constraints. Without appropriate funding, the most evident capability need may not lead to an acquisition, even when the technology is easily available. Given historic rather low levels of defence spending in Europe, and the general situation of public budgets at present, there is very little hope that defence spending will increase in any significant way anytime soon. Moreover, in many Member States, a considerable proportion of defence procurement budgets is currently still absorbed by major programmes which were launched a long time ago. This reduces further the money available for investments in new equipment to meet current and future capability needs.

In any case, the new capability-based approach is at least partly conceived as an answer to financial constraints. Pooling and sharing of resources, for example, are concepts closely related to the new capability approach and are likely to become more frequent in the future as means to cope with scarce financial resources.[217]

Another important aspect to this new approach is the definition of capabilities, not only in terms of equipment, but also including concepts, training, support, interoperability etc. Equipment is therefore only one parameter amongst others which defence planners take into account in their decisions. This is important, since it shifts the focus away from sheer numbers (and production volumes) and emphasises the importance of related services.[218]

Moreover, defence planners are increasingly open vis-à-vis new, non-traditional solutions for their capability needs. There is in particular a growing interest among defence establishments in satisfying military needs with civil equipment.[219] Already, armed forces are using commercial

[217] See Nordic cooperation or NATO Strategic Airlift Capability SAC, where 12 nations share a pool of three C-17s.

[218] A good illustration of this is the so-called helicopter gap. European armed forces have 1,700 helicopters in service, but most of them cannot be used in crisis management operations, because the crews are not trained to fly in the relevant environment (such as deserts or mountains) or because the helicopters are not equipped for such environments. See "Improving capabilities for ESDP's future needs", by Alexander Weis in *What ambitions for European defence in 2020*, Institute for Security Studies, edited by Alvaro de Vasconcelos, p.100, July 2009.

[219] See speeches of Catherine Ashton and Hakan Syren (chairman of the EUMC) at the EDA conference on "Bridging efforts", 9 February 2010.

equipment and services in (low-intensity) military crisis management operations, and this will probably be true even more for new missions, such as countering piracy and cyber-security.

Finally, several defence capabilities needs overlap with civilian capability needs for crisis management (protection, mobility, communications, information and logistics). Non-military forces operating in crisis management situations need transport helicopters, for example, in regions where road transport is too difficult or dangerous. They also need efficient logistic support, capacities for medical evacuation, interoperable and secure communication means and timely and reliable information and intelligence.

This overlap of capability needs for crisis management operations led, in 2009, to the establishment of the Third Party Logistic Support Platform (TPLS), operated by EDA. The TPLS provides a forum for interaction between Contracting Authorities (EU institutions and EU Member States) and Industry to facilitate and support the identification of commercial solutions for mission and operation-related logistics. It consists of a catalogue of services covering the whole spectrum of logistic support, alongside a list of specialised industries. What is interesting here is that TPLS acts as a platform for both military and civil missions and is open to both defence and civil companies. This is clearly an example of blurring in the area of crisis management and illustrates the attempts of defence planners to make the logistic support of operations more cost-efficient.

The TPLS is "only" a common platform for the procurement of logistical support, i.e. an instrument downstream in the acquisition process. The EU's new *Crisis Management and Planning Directorate* (CMPD) aims at going one step further, to coordinate civil and military planning processes upstream in order to achieve more and greater synergies. In the future, this could lead to a common planning process with truly common capability and equipment needs.

Particularly in the areas of networking, communication and situation awareness, this approach could lead to new system-of-system solutions across the defence – security dividing line. For instance, Europe has a strong industrial base for secure telecommunications and space-based

earth observation, but deployed capabilities are all national. Ideally, these capabilities could be interconnected and upgraded fully to match future operational requirements and evolve into a global awareness system for security and defence. The same is true for radar-based applications, where existing civil and military capabilities would have to be linked into an overarching maritime surveillance network to allow the sharing of information on the Recognised Maritime Picture. Such integrated systems of systems for civilian and defence actors could be enablers for cost-effective, sustainable and competitive solutions in the future.

Common planning could also lead to the development and acquisition of multi-mission oriented equipment. Systems which could be useful for both military and civil missions, such as UAVs, could be pooled and used for different purposes and operations, for example to monitor movement on the ground in civil and/or military operations abroad, or spot illegal immigrants at Europe's external borders. Logistic support, including air transport, and communication networks are further areas where only marginal adjustments would be necessary to make equipment suitable for multiple purposes.

Common planning is therefore a must for fostering blurring at the operational level and for finding common solutions across the defence – security divide. Defence planners seem to be particularly open to this approach. To exploit potential synergies fully, however, and translate them into concrete business opportunities for industry, would probably also require new investment models involving security, defence (and space) customers together. Unfortunately, such models are still a long way off. Currently, the different actors can at best invest separately with their own budgets in areas of common interest (see cooperation / coordination between EDA, ESA and the Commission on SDR, or Unmanned Aerial Systems (UAS). Despite the calls for avoiding duplication of effort, common funding for research or joint procurement across the security – defence dividing line is still not possible.

5.2.2. Impact on industry

These developments illustrate that the situation for industry in defence markets has become more complicated than in the past. The blurring of missions creates new business opportunities, but these opportunities are not easy to exploit, because financial conditions are all but favourable and planning processes have become complex.

The shift from an equipment-based to a capability-based approach brings a number of challenges for industry. First, it changes considerably the traditional defence customer-supplier relationship: Industry is required to become involved in the planning process, develop pro-active proposals for possible solutions, and focus less on the development of new platforms and more on services and network enabled capabilities. Second, it makes the environment in which industry operates less predictable and stable than in the past. Defence capability development is in fact guided by generic threat assessments, which are then translated into generic operational scenarios. This inevitably makes previsions for new equipment needs more difficult and capability planning in defence, ironically, more similar to capability planning in security. Whether this situation will improve depends a lot on whether planning processes will be further developed and strengthened at the EU level (as the only point of intersection for bringing small Member State, large Member State, defence and security capability planning together).

Opportunities and challenges are not the same for all companies, however. The situation seems particularly challenging for established defence suppliers, which have lived for decades in the traditional defence customer-supplier relationship and built their business model on the traditional equipment-based approach. They still benefit from some ongoing big "traditional" defence programmes (i.e. Eurofighter, Tiger, A 400 M and Rafale), but the future is – for all the above-mentioned reasons – rather unclear.

What seems clear, however, is that new programmes, if any, will rarely reach the same production volumes as during the Cold War – not only because of budget constraints, but also because of structural changes in the organisation of armed forces, particularly considerable downsizing in all

Member States. The reduction in the numbers of platforms is a direct consequence of the shift from territorial defence to crisis management; "leaner but meaner" has become the leitmotiv, and this will not go away as long as the threat environment does not change dramatically.

This constitutes an enormous challenge for defence suppliers, since the reduction of production volumes makes it extremely difficult to bear the high R&D costs incurred for complex weapon systems. One way to cope with this is to use, wherever possible, civil technologies to reduce R&D costs per unit. In this respect, blurring at the technology level and the flow of technology from the civil to the military domain offers an opportunity for defence companies to offset the higher unit costs of smaller production volumes.

At the same time, the increasing use of civil components for defence equipment and commercial technologies for the development of defence applications means that defence markets become accessible for producers which normally operate only in civil and security markets. This creates business opportunities in particular for ITC suppliers. For established defence players, these newcomers represent an opportunity (rather than a challenge) as well, since the latter enable the former to reduce costs, but do not normally bring into question their leading role as system integrators and prime contractors.

This is also the case in ITC, where commercial technologies may be at the heart of the military network, but established defence companies remain the prime contractors on most communications and network infrastructure programmes. In most cases, security companies – whilst interested in emerging business opportunities – remain subcontractors and suppliers and this is likely to remain the pattern for the foreseeable future. One example is the UK MOD's Falcon communications infrastructure programme, where BAE Systems acts as prime contractor with technology partners that include CISCO Systems. Security companies have therefore mainly entered large defence programmes as ("black-box") sub-system suppliers, with established large defence contractors playing a crucial role as intermediaries, integrating technologies developed in the civil and enterprise security sectors and translating them into military applications. Given the

cultural barriers between the defence and the civil world, this division of labour is unlikely to change.

Another entrance point for civil companies into the blurred defence market is the vast field of defence related services. In certain areas, in particular logistics, this can imply huge business opportunities, in particular since European armed forces lack the capabilities to support deployed troops over long distances. In these cases, it can often be easier and cheaper to use commercial service providers, rather than building up own capabilities. In particular in low-intensity military operations, this approach can even go so far as to outsource core defence tasks, such as surveillance, to civil companies. Such commercial solutions are particularly tempting to save costs, but they are also a challenge for established defence players, since they replace the potential acquisition of "real" defence equipment.

Further business opportunities for non-defence companies may arise in the area of maintenance. These opportunities, however, are limited to rather simple equipment and/or day-to-day maintenance. More complex tasks (in service support, repair, modernisation) for sophisticated equipment normally remain with the producer, since the latter holds the system authority and is the only one who has the necessary know-how to maintain and support the system as a whole.

In general, it can therefore be said that the shift from territorial defence to crisis operations – and the implication this has in qualitative and quantitative terms on defence capability needs – has opened new opportunities for civil companies in the defence market. The main driver for this development is cost saving.

The application of the new procurement directive will certainly reinforce this development, since it will increase competition and cost pressures. In addition, by introducing EU procurement rules into the defence market, the directive should also make defence procurement processes more transparent and more accessible to companies who, up until now, have operated only in non-military markets. Technical, cultural and financial entrance barriers remain high, however, which

also means that established defence players are likely to remain dominant in the market, being able to exploit civil input to reduce their own costs.

Moreover, defence ministries are aware of the economic and financial pressures which budget constraints and procurement reductions put on defence industries. They will therefore foster the use of commercial technologies and use civil suppliers wherever possible to reduce costs, as explained before – but only as long as this does not reduce the workload of the key defence industrial players to a point at which core industrial capabilities could be lost. Again, blurring at the industrial level therefore has its limits.

5.3.Opportunities and challenges in security markets

As we have seen in the previous chapters, demand in the security market has been driven mainly by two major developments. First, security actors (who traditionally have been limited to internal security tasks) are increasingly involved in operations abroad, be it as first responders or to support nation building and reconstruction. Second, security actors (who have traditionally been faced with rather low-scale and low-intensity security threats) are now facing new adversaries who act globally and, although non-military and non-governmental in nature, are so dangerous that they can even threaten the essential security interests of States. As a consequence, new, much more demanding security missions have emerged, which, in turn, have created new and more demanding capability requirements. At the same time, "High-end" security threats could affect all sectors of society, which necessitates in particular the protection of those infrastructures which are critical for the functioning of society.

It is these dimensions – facing a globally acting, extremely dangerous adversary at home and abroad – which drive blurring on the security side of the dividing line. The more that security forces and services are affected by (one of) these two dimensions, the more their missions and capability needs become similar to those of the armed forces. The second dimension ("going abroad") was discussed in the previous section, together with defence. The following section will therefore focus on the "Homeland" dimension of the "High-end" security area:

- The fight against terrorism and organised crime by detecting, preventing and prosecuting terrorist and organised criminal activities.
- Protection of critical infrastructures from being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, accidents, computer hacking or criminal activity.
- Protection of borders by identifying and preventing illegal movement of persons, weapons, illicit substances, tracing and securing product supply chains and logistics.

In Chapter 3, we reviewed the broad range of security actors involved in these missions. In order to determine the size of the blurred security market and the opportunities that this blurring bring to industry, one would also have to identify which equipment they need to fulfil tasks relating to these "High-end" security missions, and how much financial resource is allocated to the procurement of this equipment. For a variety of reasons, however, these questions are particularly difficult to answer: 1) the "High-end" security customer base is highly fragmented at different levels (public–private; national–regional–local; different services), which makes it almost impossible to draw a comprehensive picture of what is procured; 2) important parts of the "High-end" security market lack transparency, because information on procurement is too sensitive to be disclosed. In particular purchases for the fight against terrorism and organised crime are normally neither advertised nor specified in budgets. Consequently, it is impossible to get a clear picture of procurement decisions or planning in these areas; 3) most security customers do not follow a systematic, long-term oriented approach to identify their equipment needs. This is the case in particular for services in charge of less sensitive tasks, but also for private security customers. This makes it very difficult (to say the least) to identify future business opportunities for industry.

5.3.1. Security market estimates

Given these difficulties, it is extremely difficult to estimate the overall size of the security market. According to a Frost & Sullivan (F&S) study[220], the European homeland security market forecast for 2007 was about 300 million euros, with an expected increase of 100 million euros per year in the following 6 years, reaching a plateau of 900 million euros per year from 2013. The market share identified by the F&S report per technology in the ten year period 2005-2014 would be: biometric 42%, UAVs 28%, radio-frequency identification (RFID) 19% and screening 11%. Given a total turnover forecast of about 5.2 billion euros for the period 2005-2014 (about the same size as the annual market for space products alone), the potential 10 year markets are respectively 2.2 billion euros for biometric products, 1.5 billion for UAVs, 1 billion for RFID and 500 million for screening. According to a study by Civitas Group, published in November 2006[221], the level of procurement in the EU security market for security would be for 64 billion euros over the following 5 years. Thus the average would be at 13 billion euros per year, quite different from the results of the F&S study.[222] A recent ECORYS report[223], finally, estimates the value of the EU security market in 2008 at between 26 and 36.5 billion euros, which is significantly higher than the two previous studies. The huge differences between the findings of the three reports confirm that all market estimates should be considered with caution. Depending on the definition of security, which data is collected and how it is categorised, the results can vary significantly.

In the absence of reliable figures and commonly agreed definitions, it is even more difficult to identify the "High-end" security market (vis-à-vis the traditional security market). According to the ECORYS study, physical security protection based on general security applications such as CCTV, access control, fire detection, etc. counts for nearly 40% of the total European market share. The authors estimate that this traditional security sector presents the largest market share today, but expect it to have a relatively slow rate of growth in the future. New "High-end" security markets, such as critical infrastructure protection, counter-terror intelligence and aviation security, by

[220] Frost & Sullivan, 2005.
[221] Figures published on EOS homepage (http://www.eos-eu.com/Home/tabid/36/Default.aspx), accessed in July 2009.
[222] Frost & Sullivan, 2005.
[223] ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009.

contrast, are expected to be the fastest growing market sectors. The authors consider them still in relative infancy, as demand would mainly come from national governments and administrations. However, arguing that security issues would remain high on the political agenda, they also expect these sectors to have sustainable growth rates and to increase their market share vis-à-vis traditional security market sectors.

The high degree of uncertainty about the size of the (future) security market is in itself an enormous challenge for industry, because it makes it extremely difficult to take investment decisions. In the security market, this problem is further exacerbated by the diversity of customers.

5.3.2. Public versus private security markets

In this context, the main distinction is between the public and the private segment of the "High-end" security market. The main difference between the two lies in the role which public authorities play for demand: when public authorities are customers, they determine demand directly via their own procurement decisions. When private operators buy security equipment, they may do this on their own initiative, because their specific activities require them to do so (i.e. physical security protection in banks or warehouses). Generally speaking, this represents the traditional private security market. When it comes to "High-end" security, however, the investment decisions of economic operators are often determined by regulation set by public authorities to ensure a certain level of protection. This is the case in particular for critical infrastructures, which are a crucial element of the "High-end" security market. In these sectors, the demand for security supplies and services is private, but defined and driven by public intervention.

The ECORYS study identifies the heavy involvement of the public sector as one of the main feature of the European "High-end" security market. According to the authors, public authorities would be by far the main purchasers of "High-end" security equipment and services, accounting for around

80% of the market and a total spending of €13bn to €17bn. The private sector, by contrast, would account for only 20% of the market with a value between €3bn and €4.5bn.

This assessment, however, stands in contrast to our findings on public expenditure for security procurement. According to official ministerial figures, the four biggest Member States together spend (at the central level) less than two billion euros for security procurement and R&D (FR: € 0.53 bn, DE: € 0.55 bn, IT: € 0.15 bn, UK: € 0.7 bn).[224] Even when one takes into account public security spending at regional and local levels and in the other EU Member States, it seems unlikely that the level of €13 to 17 bn, indicated in the ECORYS report, will be reached. This is true in particular since the official ministerial figures mentioned above include expenditure for both traditional and "High-end" security. How much of these total security budgets is specifically dedicated to "High-end" security is again difficult to identify and may vary between Member States, depending on their respective organisation. The French Ministry of Interior, for example, has an investment budget of 508 million euros (210.8 million euros for the National Police and 297.2 for the Gendarmerie). These investments essentially concern low technology products. Moreover, the budget is parcelled out into hundreds of micro procurement projects, with the modernisation of the communication system for the national police (ACROPOL), for 37 million euros, being the largest.[225] In Germany, the police is mainly the responsibility of the *Laender*, which means that the federal government focuses its missions and expenditures on "High-end" security. However, total spending at the central level is roughly the same as in France. The procurement budget of the federal MoI doubled from 2001 to 2007 to € 546 bn, which still represents only about 15% of the defence procurement budget. The main spending items were services (36%) – mainly for airport security – telecommunication technology (25%), vehicles (15%) and information technology (12%) of the overall budget.

[224] See Annex 4 for more details.

[225] Annex of the Loi de finance on « Sécurité ». This sector is responsible for activities centred on equipment and infrastructure, amongst others. This includes management of both the operational and investment budgets for the national police force, as well as equipping the departments. http://www.performance-publique.gouv.fr/farandole/2009/pap/pdf/PLF2009_BG_SECURITE.pdf , p.13

These are only examples, but they illustrate that public spending on security procurement is still limited and remains much lower than investment in defence procurement. This is true for security in general and, even more so, for "High-end" security.

Table 5: Defence and public security budgets at the central level (procurement + R&D)

COUNTRY	DEFENCE	SECURITY
France	9.5*	0.53*
Germany	6.5*	0.55***
Italy	3.2*	0.15**
United Kingdom	10.9*	0.7**

*Figures are expressed in billion euros. * 2008; ** Estimated, 2009; *** 2007.*

These findings are confirmed by other studies, which estimate the investment part of budgets (expenditures for procurement, in-service support, maintenance, modernisation, etc.) as much higher in defence (up to 50% of total spending) than in security (7%), where the bulk of expenditure remains focused on personnel and operational costs.[226]

5.3.3. Impact on industry

The different studies mentioned above and the analysis of various public security budgets confirm that, in terms of market opportunities, the blurred capability areas identified in chapter 1.3.4 seem currently most promising: detection, identification & authentication; situation awareness; risk assessment, modelling, impact reduction; communication; information management; positioning and localisation. These capabilities are indeed common to the three main "High-end" security missions, i.e. the fight against terrorism and organised crime, as well as protection of borders and critical infrastructures. In terms of equipment, the ECORYS study estimates IT and Secure Communications[227] as the most important markets in the years to come (€ 6bn), followed

[226] Yves Bélanger, Directeur du Groupe de recherche sur l'industrie militaire et la sécurité GRIMS, *Le marché de la protection, de la sécurité et de la défense : perspectives d'ici 2015*.
[227] Secure mobile ad-hoc communication systems for operations in case of incidents, crisis, disaster or event.

by screening and scanning equipment[228], tracking and tracing devices[229] (€ 3.5bn to € 4.5bn respectively), CBRNE detection[230] (€ 1 to € 2bn), protective clothing (€ 1.5bn to € 2.5bn) and biometrics[231] (€1 to € 1.5bn).

In most of these capability areas, business opportunities are likely to emerge in both the private and the public security sector. Due to their specificities, however, the two sectors will probably also have different equipment needs in many areas, even when they share the same capability needs. First, when public security forces procure surveillance or safe communication equipment suited for crisis management operations or maritime border control, for example, interoperability with military equipment will be an important requirement – which is probably not the case when operators of critical infrastructures purchase surveillance or communication means. Second, private "High-end" security customers focus their efforts exclusively on the protection of potential targets against possible attack, whereas public security actors play a proactive role, aiming at preventing attacks and prosecuting potential malefactors. This by itself creates different procurement priorities. Third, for private operators, security is not an end in itself, but a "necessary evil" which must remain compatible with their normal business activities. Whereas public security customers will have to strike a balance between costs and performance, private security customers will have to take into account a third element, which is compatibility with normal business processes. Last but not least, those public security actors which are specialised in the fight against terrorism and organised crime are certainly customers of the most sophisticated security equipment. In many cases, these services need tailor-made solutions, which are technologically very complex and produced in very small numbers. Such procurements are probably more sensitive and confidential than most defence procurements.

This confirms again that fragmentation of security markets in Europe is to a considerable degree structurally determined. Hence, the situation will probably continue to vary considerably between

[228] For the detection and identification of dangerous or hazardous goods and materials for secure air transport.
[229] Tracking and tracing of goods (and ships) for secure maritime transports.
[230] Detection of chemical, biological, radiological, nuclear and explosive substances (other than air transport of goods).
[231] Biometric solutions for entrance/barrier control of protected areas, buildings or events.

the different market segments. This makes market access, in particular for newcomers, by definition challenging.

The (technologically) most demanding requirements are likely to come primarily from public "High-end" security customers. At first glance, one could expect this to give a comparative advantage to defence companies vis-à-vis traditional security or civil firms. However, reality is probably more complex. The need for technologically very sophisticated equipment is probably limited to certain very specific security services (which are unlikely to buy large numbers of products). Moreover, public security customers in general are very different to defence customers, and their buyer values are not necessarily receptive to product offerings from defence companies. Police forces tend to be relatively conservative with respect to their use of new technology. Equally, new technologies may require changes in operating procedures and training and civilian security agencies may prefer manpower intensive solutions over complex, costly and untried technological approaches. A challenge for defence companies remains to develop business models (like pay-as-you-use) to encourage adoption of some technologies that may be regarded by many civilian agencies as too expensive and complex to operate. At the same time, defence companies are facing competition in "High-end" security markets from incumbent security companies with niche capabilities and strong reputations amongst security customers.

All this means that public "High-end" security remains a challenging market for defence companies, even when market conditions are similar to defence (single customer, huge procurement programme and complex technological requirements). This is the case in particular for ITC programs, where new entrants from the civilian sector are drawing on civil origin technologies and applications drawn from the dynamic retail, banking and telecommunications sectors. The situation may be somewhat easier for defence companies, where security applications can be developed on the basis of defence specific technologies, such as MALE UAVs for surveillance purposes.

At the same time, one should not forget that in some capability areas national procurement programs are already on their way. This is the case in particular for secure communication and data exchange equipment. In Germany, for example, the MoI is currently introducing a single software defined radio (SDR) solution for all security actors, called "BOS". It not only involves the Federal and *Laender* police, disaster relief forces, fire fighters and rescue services, but also customs authorities and the domestic intelligence services. Allowing for 500,000 users, BOS will be the largest SDR system based on the TETRA standard, which is also used in many other European countries. Further examples for big (public) investment programmes which are already on their way are the AirWave programme in the UK for a first responder communication system (£2.5 billion over 19 years) and the eBorders border control information technology programme (£650 million).

Such large scale programmes are relatively rare and last a very long time. In other words, once the contract is awarded, new business opportunities in the respective area will probably not re-emerge for some considerable time. Moreover, follow-on (service) contracts, for example, for maintenance, will probably be awarded to the initial supplier for IPR and/or confidentiality reasons, which limits business opportunities for newcomers still further.

In the medium term, major new business opportunities may come for security applications for Galileo and GMES, once these systems become operational. Further opportunities may arise with the growing requirement to create "systems of systems" in order to ensure integration, interconnectivity and interoperability of security systems, such as:[232]

- A European-wide integrated border control system, able to deliver a comprehensive and integrated border management system capable of providing concentric layers of protection from control measure to cooperation within, and between, Member States.

[232] Opportunities identified in the ESRAB Report, *Meeting the Challenges: the European Security Research Agenda*, 2006.

- A logistic and supply chain security system, able to deliver an efficient, secure network of supply chains that guarantees the security of goods transported, while having minimal impact in terms of cost and time on commercial operators and enterprises.
- A mass transportation security system, able to deliver a consistent and integrated suite of mass transportation security systems, taking into account the cross-border dimension of mass transport.
- A CBRNE system of counter-measures, able to cover the phases from prevention to response and recovery.

In many cases, these systems of systems would go beyond the national level. Whether they become real opportunities for industry, therefore, depends largely on how cooperation at the EU level evolves and which role European institutions are allowed to play. As we have seen, the EU already acts as a sponsor for security-related research activities. It has also co-funded security related procurement in the new Member States via the PHARE programme. Thanks to Galileo and GMES, it will also operate security related infrastructures. The question is whether the EU will in the foreseeable future develop these activities further, i.e. (co-)fund transnational systems of systems (as those mentioned above), become itself a customer of security supplies and services (for example for a pool of EU-owned equipment for civil crisis management operations or border surveillance), contribute to harmonising national security demand (at least in certain areas, such as border control via FRONTEX), or develop its security research activities (for example, closer to defence research). All this will have a considerable impact on the "High-end" security market in Europe in general, and the evolution of the public demand side in particular.

The situation – and therefore also the EU's potential role – is different for the private "High-end" security market. Here, market opportunities are determined mainly by regulation, which sets the framework for investment. Regulation defines which security measures economic operators have to take and which kind of equipment has to be used. At a lower regulatory level, standards define the performance and the operation of equipment. At this level, the current situation is far from satisfactory. First, in the absence of common EU-wide solutions, performance standards for

security equipment differ between Member States or user groups and / or are often not clearly defined. This is a major challenge for industry: It makes it difficult for equipment providers to know what performance potential customers expect. This, in turn, makes it hard to determine investments in technology and / or product development. Second, technical standards differ as well. At this level, the absence of common standards results in potential problems of interoperability and further contributes to market fragmentation, even when common capability requirements exist and the same equipment is used to fulfil these requirements. Here, the EU clearly has a role to play to drive standardisation, in order both to ensure throughout the Union the same level of security and to enhance the openness of security markets in all Member States and across the different market segments.

Last but not least, Directive 2009/81 will bring both new challenges and opportunities for industry. As we have seen in Chapter 3, the new Directive is highly innovative, since it is the first piece of legislation which covers the whole blurred market area, applying to procurement contracts awarded by defence customers, public security customers and (many) operators of critical infrastructures. The new Directive will certainly change considerably the way in which procurement in defence and security markets is organised. Change may even be bigger in the security sector, where the debate on opening-up national markets to EU-wide competition is much less advanced than in defence. Private operators of critical infrastructures often themselves face competition in their own markets and may therefore be ready anyway to choose the economically most advantageous security solution, no matter whether it comes from a national or non-national supplier. For public security customers, the situation is probably different, at least in the "High-end" security segment. The more sensitive their tasks are, the more reluctant they often are to buy equipment from non-national suppliers. It remains to be seen to what extent (or how fast) the Directive will be able to change this attitude. In any case, it constitutes – across the blurred defence-security dividing line – an opportunity for competitive companies (which may find it easier to win contracts abroad), but also a challenge for awarding authorities (which will have to change their traditional way of procuring) and less competitive firms (which may find it harder to survive in a more competitive environment).

5.4.Conclusions

The market situation in the blurred area is complex and fragmented. As we have seen, this complexity and fragmentation is at least in part structurally determined. This means that there are natural limits to harmonisation and simplification, which have to be taken into account in any attempt to make markets more efficient.

Complexity offers both opportunities and challenges for all companies operating in the blurred area. Defence companies (may) find new opportunities in the security market, security and civil companies (may) find access to the defence market. This applies to big companies as well as for SMEs. Actors from each side will face challenges when trying to penetrate the other side, simply because the two worlds remain very different (customer habits, cultural apects, different requirements). The great variety of company strategies (and success rates) in penetrating the other side of the blurred market illustrates the uncertainty and chaos which governs this market segment. At the same time, it proves also that market access across the dividing line is possible – it may be difficult, but there are companies which are able to overcome all challenges and exploit new opportunities.

In general, the defence market seems to offer – in spite of all difficulties – more opportunities for newcomers from the non-military world than the security market for defence companies. There are a variety of reasons for this. First, defence budgets remain much bigger than security budgets, and the volume of individual contracts is bigger. This makes it easier to find business opportunities in the defence market which are sufficiently worthwhile to "make an effort". Second, the budget pressure on defence establishments is enormous and is driving the opening-up of the market to commercial components, technologies and services. In security markets, by contrast, budget constraints will certainly not be an incentive for customers to consider defence solutions. Third, the new capability-based approach of defence planning shifts the focus from platforms to network-enabled capabilities and ITC, i.e. domains where technological innovation often comes from commercial industries rather than from defence firms. Moreover, the capability approach is by definition built on flexibility and openness vis-à-vis non-traditional solutions. In security

markets, by contrast, procurement decisions are still not based on systematic planning processes (be they equipment- or capability-driven). This makes it particularly difficult for defence industries to operate on these markets. In certain areas, capability requirements may have become so demanding that only defence suppliers are able to provide solutions, but these areas seem rather rare.

All this would also explain why defence groups who have succeeded in penetrating the security market have done so via dedicated business units with long and successful experience in these markets. At the same time, there are limits to the possibilities for non-defence companies in defence markets. In core capability areas, established defence players have a specific know-how which cannot be simply replaced and which governments are not willing to lose. The challenge for the future will be clearly to identify these areas and evaluate how these key capabilities can be maintained.

Given the high degree of complexity and uncertainty in the blurred area, any market intervention should be considered with care. Rationalising demand will certainly be both necessary and useful. With respect to regulatory initiatives to foster industry's innovation, however, care needs to be taken not to interfere with competition, but rather to foster competition - between defence, security and civil companies across the blurred dividing line and across national borders. The following chapter presents our recommendations for possible EU action to achieve this objective.

6. Recommendations

This study has found the extent of blurring between the defence and security sectors to be more limited than expected. In the previous chapter, however, we have also noted that blurring could provide opportunities for industry in the future. Many obstacles remain to be overcome if industry is to be able to benefit from these opportunities. Our analysis demonstrates in particular that structural differences between the defence and security markets are the main factors impeding the development of a blurred defence and security segment. Specifically, the heterogeneity and fragmentation of demand in the security sector emerges as a major obstacle to the maturation of the market and, thereby, to the still limited convergence between security and defence.

This is the reason why we have designed a series of recommendations to develop and reinforce the security side of the market. We consider this issue as a pre-condition to fostering any further blurring between the two sectors in terms of governance (better coordination between security and defence players), industry (facilitating access of security and defence players in the blurred market segment), and technology (supporting technological blurring thought research activities).

We strongly believe that the European Commission should play a pivotal role in the development of the security sector within the European Union. This view has been reinforced by stakeholders interviewed for this study, who stress how technology research projects sponsored by the EU in the security domain will be a critical starting point for nurturing the blurred market segment. Follow-up Commission activity will also be necessary to sustain this initial initiative.

Recommendation 1: The European Commission should establish European Technology Platforms (ETPs) in the security domain in order to structure further the development of mission-oriented technologies. Since a single Technology Platform for security would be too complex to be feasible, we propose that these ETPs should focus on the specific missions which have emerged as particularly sensitive within this report, such as Border Security.

Recommendation 2: Having identified that a high level of fragmentation has affected the development and maturation of the security market, we recommend that the European Commission establish a clear set of European standards in the security domain. Common European standards would significantly reduce the fragmentation of the security market, by defining levels of interoperability required between security products. Both large companies and SMEs proved to be particularly supportive of this issue.

Recommendation 3: Additional research programmes should be launched by the Commission through Joint Calls between security and other 7th FP cooperation themes, ensuring the development of key technologies and the deepening of sensitive security-related issues. Health, nanotechnology and new production technologies, socio-economic and social science research appear to be fields where the Commission's efforts could enhance a more comprehensive understanding of security, to be translated into new industrial activity. This could further lead to an expanded 8th FP Security Research Theme, able to build upon this comprehensive approach to security.

Recommendation 4: At the Member State level, we have noted an emerging effort in the development of national threat and risk analysis capabilities. We believe that these efforts should be raised to EU level, in order to achieve a common approach to risk analysis. Such a combined approach could then be at the heart of common security policy-making and common security-related investment decisions. We therefore recommend that the EU develop (within the Commission) its own analysis and planning capabilities. This recommendation would help suppliers focus their production on common requirements, thereby closing the communication gap that we found to exist between suppliers and end-users.

Recommendation 5: In Chapter 3, our analysis showed that there is no evidence of any European institutional coordination of security demand. We therefore recommend that the Commission establish a European Security Framework to improve governance of the security sector as a whole. This would represent a step in addition to the ESRIF approach, providing industry with a coherent

agenda for cooperation and a structure within which to bring together the heterogeneous security end-users inside 7th FP activities.

Recommendation 6: Finally, our study produced converging analyses showing that the European Commission should step into the procurement phase of technology development, shaping the security market not only as a funder of research, but also a buyer. This is why we recommend that the role of the Commission as a customer be developed, focusing its activity on already mentioned blurred missions and fostering the development of dual-use equipment. Space systems are a key example of how this process should work **(Recommendation 6.1**).

The above 6 recommendations are dedicated to the consolidation of the security market, which we consider as a key issue in fostering blurring between the defence and security sectors. However, we also argue that the Commission should in parallel develop other initiatives to strengthen the link between the defence and the security segments, in particular the following two items.

Recommendation 7: We recommend the institutionalisation of the cooperation process already launched between the research activities of the European Commission and those of the EDA (including ESA for space-related issues). There is already an ongoing framework for coordination between the two institutions, but we wish to reinforce the positive effects of this cooperative approach in paving the way for the development of dual-use equipment.

Recommendation 8: Finally, having stressed the importance of efforts towards institutional coordination, we also support the potential for the Commission to play an active role in the development of defence technologies. This would clearly drive blurring towards the security segment. We are aware this is a sensitive issue and we therefore recommend a process of reflection on the possible inclusion of defence matters in 8th FP research projects.

Recommendation 1: European Technology Platforms in the security domain

The Commission should establish European Technology Platforms in the security domain, beginning with border security. These should be end-user rather than industry led.

What has already been achieved?

To date, the Commission has pursued a capability driven approach to security research, with the following specificities:

- A Group of Personalities (GOP) has been gathered to discuss the shape of a European Research Programme.
- ESRAB was established with membership drawn mainly from Member States' governments, industry and research organisations.
- ESRIF was created as a public-private security forum to allow for broad dialogue and the development of a security research & innovation strategy.
- In parallel, end-user engagement has been fostered as an important element of the 7th FP security theme.

Beyond the security sector, European Technology Platforms (ETPs) already play an important role in the governance of the European Research Area (ERA). European Technology Platforms are European networks bringing together researchers, industry and other relevant stakeholders in a particular technological field in order to foster European research and development in the concerned area. ETPs are designed to function in technology investment decisions at a pre-competitive stage, when industrial stakeholders can see benefits from cooperating with competitors. The first European Technology Platform, ACARE, was launched in 2001 in the field of aeronautics. Since then, others have followed in areas as diverse as biofuels, nanoelectronics, food, foresting, textiles and wind energy, to name but a few of more than 30 ETPs.

There seems to be little value in establishing a single European Technology Platform for security, because its remit would be too broad and complex to be of real value. This report has already noted that the security sector covers a very diverse range of missions and users. Equally, a

European Technology Platform for defence and dual-use technology might also face the problem of being too broad, since it would have to address a very wide range of technologies and applications.

Why should the Commission intervene?

ETPs are intended to promote Europe's competitiveness, in particular to "*define* R&D priorities" and develop corresponding timeframes and action plans. They are to "ensure adequate research funding in areas with a *high degree of industrial relevance*" by "orienting the Seventh Research Framework Programme to better meet the needs of industry[233]". Given their strategic guiding function, ETPs mobilise financial resources not only at European but also at national and regional levels and from private industry.

IF ETPs were to be applied to the security sector, the Commission would be providing significant support to the development of European capabilities in a potentially growing area.

What could the Commission do?

The Commission should consider establishing a European Technology Platform (ETP) adapted to the specific requirements of the security sector. Instead of being technology oriented, the ETP should be mission-oriented. We propose a first ETP for border security. There are a number of good reasons for creating an ETP for border security.

First, this is a field of strategic importance. ESRAB and ESRIF have both identified border control as a central task of long-term significance for the security of the EU.

Second, the ETP would have a clear objective. The goal of the ETP would be to provide the technologies needed for the effective control of EU external borders, along the lines developed in the ESRAB report and further outlined in the final ESRIF report.

Border control warrants action at European level. EU borders can only be surveyed and protected if Member States action is coordinated (i.e. if demand side "market failure" is overcome). Frontex could play an active role in this process, as it is intended to coordinate "operational cooperation

[233] Available at: http://rp7.ffg.at/RP7.aspx?target=114722&SetLanguage=2

between Member States in the field of external border management".

Moreover, industry can be expected to invest substantially and over the long term, as initial export successes in this area have proven the competitiveness of border security products. This success could be further enhanced by the creation of an ETP.

In addition, the Commission might wish to consider adapting the ETP instrument to other particularities in the security domain. In particular, the Commission might – in the context of an ETP - return to the issues raised by ESRAB with respect to funding. ETPs are currently financed 50% by the Commission and 50% by industry. The issue of matched funding was raised by ESRAB and was the subject of debate within the Commission. The Commission might want to consider what incentives it could give industry to become involved, including an increase in the Commission share of funding to 75%, already a possibility for SMEs. Of course, this could once again raise objections that the security sector is being treated differently to other sectors. Equally, the Commission would need to be mindful of constraints imposed by the World Trade Organisation. In particular, if the Commission were to fund civil security applications, it would have to be bound by WTO rules.

What challenges might the Commission face?

We have recommended that the Commission investigate the potential for Frontex to lead the proposed ETP. This will depend in large part on Frontex capacities and mandate. So far, the mandate and tasks of the Agency in the area of research and development have been limited to "follow up on" and "assess" the "developments in research relevant for the control and surveillance of external borders and disseminate this information to the Commission and the Member States".[234] Moreover, Frontex "plays a role in forming the research programmes". However, it would need to be seen whether the Agency could muster the resources and administrative know-how, as well as the political standing with stakeholders, to coordinate an ETP.

End-users and society at large need to be actively involved in security matters, but so far ETPs have not proved successful in involving end-users and societal stakeholders. A recent report on the performance of ETPs has found that "[s]pecial attention should be paid to the involvement of

[234] See Frontex official webpage: http://www.frontex.europa.eu/structure/research_and_development/

NGOs and end-users (consumers). It remains a challenge to explain to society why large investments in R&D are needed and what the potential benefits might be."[235] Hence, the ETP concept would need to be adapted to the specific needs of the security domain.

[235] Idea Consult, *Evaluation of the European Technology Platforms (ETPs)*, Brussels, August 2008. Available at: ftp://ftp.cordis.europa.eu/pub/technology-platforms/docs/evaluation-etps.pdf

Recommendation 2: Promoting standardisation

By promoting the creation of sectoral standards, the Commission can play a key role in reducing fragmentation in the security market, thus driving greater possibilities for blurring between the security and defence sectors. While among militaries of different countries and different services interoperability has been for a long time a topic of discussion and activities, especially within NATO, considerably fewer efforts have been made on the security side. The latter continues to be characterised by high fragmentation at national level and little experience in creating interoperability across borders. Moreover, as indicated in our analysis, the blurring between security and defence on the operational side has so far been rather limited. Should this requirement arise in the future, then the need for interoperability would open up opportunities for industry to provide technological support for an effort that is typically rather political and organisational in character.

Several technologies, not least those relating to information and communication, enable organisations and systems to work together. Companies could benefit from dedicated efforts to develop applications based on such technologies. For example, OperaMar's goal was to propose a model of interoperability for "Pan-European Maritime Security Awareness". It is expected to reduce the fragmentation characterising data management caused by the differences existing between the organisations in charge and their procedures both at national and European level. As noticed before, there are even some EU agency-led research programmes, such as SeBoCom coordinated by Frontex together with the JRC, aimed at improving interoperability.

Standardisation at EU level would be a significant enabler, allowing this opportunity to be seized. It would provide a necessary condition, particularly for SMEs, to market successfully their goods and services to a wide variety of customers. This standardisation should particularly focus on the exchange of data, detection, border control and maritime transport.

What has already been achieved?

Some parts of the security sector are already standardised, thanks to the work of the European Committee for Standardisation. The CEN/TC 384 committee is currently working on airport and aviation security, while the CEN/TC 325 is working on the prevention of crime through urban

planning and building. Much work is still to be done, however, as the ECS is only partially working in the security sector. A further initiative that could push forward standardisation is ESRIF's "EU Security Label" proposal, which intends to guarantee that security products and services respect European specified criteria. The proposal was put forward by the ESRIF Working Group on Innovation Issues, among other recommendations (WG9), which also propose the promotion of pre-commercial procurement of security solutions, the creation of the European Security Technological and Industrial Base (STIB), the promotion of "Innovation ecosystems" and other initiatives aimed at maximising synergies between stakeholders, technologies and services.[236] The "EU Security Label" certificate would guarantee the compliance of a product with common European legal, ethical (data protection) or technical requirements, strengthening confidence among all the stakeholders operating in the security sector (industry, customer and end-users). As a marketing tool, this would influence the opening of the market, facilitate innovative solutions and reduce risks both for the customer and for investors. The introduction of such a label could also reassure citizens and society in general, ensuring the introduction of security equipment and services guaranteed by competent European certification bodies.

ESRIF recommendations include an increase in interoperability to enhance European security and advance product harmonisation across the security market, because "the multitude of Europe's problems with territorial, organisational and cultural non-interoperability along its Member States' borders enables criminal and terrorist organisations to exploit the patchwork's inherent weaknesses".[237]

Why should the Commission intervene?

The European security market is even more fragmented and uncoordinated than the European defence market. The implementation of European security standards could have a huge impact on the level of demand, contributing to the maturation of the European security market and, indirectly, to areas of the blurred security and defence segment.

[236] ESRIF, *European Security Research and Innovation in Support of European Security Policies. Final Report*, Brussels, 2009, p. 198.
[237] *Ibidem*, p. 14.

Standardisation, specifically at the industrial and technological levels, will help blur the boundaries between defence and security and unify the markets through better communication and information-sharing between the various stakeholders, standardised equipment (as for GSM) and streamlined demand and supply.

Stakeholders predominantly view standards and norms as positive, particularly when they are legally binding. For suppliers, especially SMEs, standards often present an advantage, as these firms can develop compliant products that they know will interlink with other systems, thereby offering their solutions as part of comprehensive solutions in cooperation with others.

For some stakeholders, norms, standards, and certificates may increase market volume, but often imply a reduction in rates of return due to increased competition (but this, in turn, would mean better value-for-money for end users). It is mainly large firms who are able to shape standards and norms and might therefore gain competitive advantage. For SMEs, participation in this process is often too costly. In this field, it would therefore be better for the Commission to proceed with a top-down standardisation process with limited participation from stakeholders.

In any case, the process should be graduated. For what we have defined as "low-end" security missions (private and home security, for instance), a process of standardisation at the European level would probably lack value and act as a disincentive for innovation in small and medium enterprises. As a recently published report pointed out[238]

> *"one important issue considering the influence of legislative developments on market conditions for security equipment is that legislation – especially in the case of the EU where such legislation sets minimum performance standards for security equipments and systems - might actually become a limiting factor in the market and technological development. In fact, if minimum standards are met, then there may be a disincentive to invest in equipment or systems offering higher performance if this implies higher costs. To remedy this risk, the EU has introduced a sliding scale of performance standards that increases in stringency over time, therefore to avoid the risk where minimum standards become the norm".*

By contrast, for "High-end" security missions, such as maritime transportation, aviation and anti-

[238] ECORYS SCS Group, *Study on the Competitiveness of the EU security industry,* November 2009, p. 116.

terrorism, a process of performance standardisation at the European level would appear essential for two reasons. First, standards at this level should be global, because the markets are global. Second, European companies need to compete against US companies, where standards are increasingly enforced and recognised. The lack of EU standards would leave the US government and industry free to impose their own standards at the global level, possibly at the expense of EU industry.

What should the Commission do?

First, the European Committee for Standardisation should have as one of its objectives to develop standards for security equipment at both industrial and technical levels.

The Commission should also evaluate, through an *ad hoc* study group, which are the security sectors that most require standard-setting efforts. This group should focus on non-standardised segments with high security relevance, to be prioritised according to their growth prospects and relevance from the security perspective .

What challenges might the Commission face?

While standard setting expertise is relatively common in the defence sector, there is currently a real lack of such expertise in the security field. This is the first challenge the Commission will face.

Moreover, standardisation is a delicate process and requires caution if unintended negative consequences are to be avoided. The implementation of certain technological standards can be too costly for companies, even to the point of discouraging the entry of new players to the market (as is often the case in the defence field, where standards are common and demanding).

Similarly, standardisation might actually constitute a barrier to technological development. In fact, there may be a disincentive for suppliers to invest in technologies or systems offering higher-than-standard performance, if this implies higher costs. This problem can be tackled through a sliding scale of performance standards.

Recommendation 3: Joint Calls between security and other 7th FP themes and expanded 8th FP Security Research Theme

For the remaining lifetime of 7th FP, there is a strong case for further Joint Calls between the security research theme and other 7th FP cooperation themes, such as public health, nanosciences, nanotechnologies, materials and new production technologies (NMP), and socio-economic sciences and humanities (SSH). Furthermore this importance and widening of the spectrum of Security Research shall be taken into consideration in a future expanded 8th FP Security Research Theme.

What has already been achieved?

Different Security Research Calls have already addressed the subjects of other 7th FP research themes. Examples include the first Call from December 2006, which had a dual focus. On the one hand, it addressed the security of transport infrastructures and utilities; on the other hand, it addressed ICT security. The Joint Call between ICT and Security themes from August 2007 was also specifically dedicated to this topic, focusing on ICT infrastructure security and the public health aspects of ICT.

The second Security Research Call, from September 2008, addressed the topic of infrastructure and utility security in a wider sense, including, for example, sensitive manufacturing plants, energy production sites, storage and distribution, storage sites of nuclear waste and also administrative buildings of symbolic value. It called for research into the security of supply chains and the aftermath of crisis management.

The third Call, from July 2009, focuses in particular on the security of energy infrastructure, the restoration of basic services after a crisis and urban public transportation. The latter is also the subject of one of the Demonstrator Projects of this Call.

In sum, Security Research in 7th FP has yet to address the public health dimensions of security. The large number of topics covered by the 7th FP indicates how the EC is taking into consideration the widening of those security aspects. This could lead to a future 8th FP Security Research Theme.

Why should the Commission intervene?

Calling for research into the public health dimensions of security would complement the strategic mapping activities the Commission has already undertaken in this area. ESRAB, for example, identified several technologies as important to civil security that fall within the public health theme of 7th FP Cooperation. In particular:

- Rapid diagnosis of infectious diseases
- Novel antiviral, antibiotics, vaccines & drug development
- Chemical & biological knowledge & related databases
- The ESRIF Draft Final Report raises another public health dimension to security, namely the need for correct identification of individuals within health systems, combined with their correct and appropriate medical records.

We consider that security and public health may represent an area of potential growth that the Commission should investigate.

With regard to nanosciences, nanotechnologies, materials and new production technologies, we maintain that nanotechnology represents a generic technology that has applications in a variety of fields. We identified above nanomaterials as an important emerging technology area with important applications in the civil security field. These include improved sensors, protection devices, imaging systems and increased computing performance. Thus, nanotechnologies have potential applications in a number of the ESRAB key technology areas, including composite materials technology, anti blast glasses and concretes, light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surface treatments for improvement of life duration and corrosion reduction.

Studying the socio-economic and social aspects of security is warranted by the growing recognition that technology should only be one aspect of the civil security response. The importance of human and organisational factors in the effective adoption and application of security technologies is increasingly recognised as important and expressed, for example, in the priorities of several national security research programmes (Austria, Germany).

In the framework of the analysis of the social aspects of security, we have also noted the growing attention that is being paid to societal resilience, particularly to the socio-cultural causes of radicalism and terrorism, the response of individuals, groups and society to terrorist attacks and their capacity to recover from such events. The importance of Societal Resilience has been emphasised in the work of ESRIF and confirmed in the work of FORESEC.[239] It is also a growing theme amongst Member States (the UK was highlighted as a relevant example in our earlier discussion of Societal Resilience). We also note that ESRAB identified the importance of human sciences, in particular human behaviour analysis and modelling, population behaviour, human factors in the decision process, teams, organisations and cultures.

What should the Commission do?

There are obvious areas of synergy between the Security Research theme and other 7th FP Cooperation themes. We recommend that the Commission pay particular attention to three themes, namely: Public health, NMP and Socio-economic Sciences and the Humanities. This can be taken into consideration not only for the 7th FP, but also future 8th FP.

Public health and security

There are clear overlaps between civil security issues and the objective of the public health theme. The objective of the health theme includes "addressing global health issues including emerging epidemics" and "[the development and validation of] diagnostic tools and medical technologies".

A Joint Call could focus on the following two activities of the public health theme:

Biotechnology, generic tools and medical technologies for human health - detection, diagnosis and monitoring: to develop visualisation, imaging, detection and analytical tools and technologies for bio-medical research, for prediction, diagnosis, monitoring and prognosis of diseases, and for support and guidance of therapeutic interventions.

Transnational research into infectious diseases (new and re-emerging epidemics) to combat major threats to public health: the focus will be on confronting emerging pathogens with

[239] FORESEC official webpage: http://www.foresec.eu

pandemic potential including zoo-noses (i.e. SARS and highly pathogenic influenza). Where appropriate, provisions will be made for rapidly initiating collaborative research aimed at expediting development of new diagnostics, drugs and vaccines for efficient prevention, treatment, and control of infectious disease emergencies.

Research into organisational health management, the economic aspects of pandemics and health related prevention and crisis management would make an important contribution to the preparedness of European societies for pandemics. Matters could be addressed as diverse as the creation of medicine stockpiles, slack capacities to allow for research and production surges in times of crisis, the interaction between authorities, or how most effectively to involve private actors of the different industries in the resilience effort of the EU.

NMP and security

The central objective of the nanosciences, nanotechnologies, materials and new production technologies theme is "to improve the competitiveness of European industry and generate the knowledge needed to transform it from a resource-intensive to a knowledge-intensive industry".

Specific research efforts could focus on those applications with a high relevance for civil security, such as improved CBRNE sensors, blast and ballistic protection devices (energy absorbing nanomaterials/CNT-based bullet proof armour/smart fabrics), nanotechnology-based imaging systems (X-ray, terahertz imaging). Other research topics in this context concern increased computing performance with applications in high-end intelligence and defence.

A screening mechanism should be developed that allows for the systematic identification and transfer of the latest research and development results in NMP to the security area. Given the high relevance of NMP also for defence and space, this topic could become the subject of research cooperation between the Commission and the EDA, and even ESA.

SSH and security

The objective of the Socio-economic Sciences and Humanities theme is to "generat[e] an in-depth, shared understanding of the complex and interrelated socio-economic challenges Europe is confronted with, such as growth, employment and competitiveness, social cohesion, social,

cultural and educational challenges in an enlarged EU, sustainability, environmental challenges, demographic change, migration and integration, quality of life and global interdependence, in particular with the view of providing an improved knowledge base for policies in the fields concerned".

The Socio-economic sciences and Humanities theme is already engaged in the funding of research that has relevance to the issue of Societal Resilience. A Joint Call could be undertaken with one or more of the following SSH themes:

Major trends in society and their implications - The aim is to understand and assess the causes and implications of particular key trends in society that have major consequences for European citizens, their quality of life and for policies, and thus to provide an underpinning for many policy areas. One of the major trends is that this work focuses on cultural interactions in an international perspective, including traditions from different societies, diversity of populations including ethnic groups, multicultural issues, differing identities, languages and religious practices, and possible issues in this context including discrimination, racism, xenophobia and intolerance.

Europe in the world - The aim here is to understand changing interactions and interdependencies between world regions, including emerging and developing areas, and their implications for the regions concerned, especially for Europe. There is the related issue of addressing emerging threats and risks in a world context and their connection to human rights, freedoms and well-being. One track is of direct relevance to this report, namely conflicts, their causes and resolution, and fostering peace. This covers the relationship between security and destabilising factors such as poverty, crime, environmental degradation, resource scarcity, uneven development, financial instability and debt; terrorism, its causes and consequences; security-related policies and perceptions of insecurity and civil-military relations.

The citizen in the European Union – in the context of the future development of the EU, the aim is to improve understanding of, first, the issues involved in achieving a sense of democratic

"ownership" and active participation by citizens as well as effective and democratic governance at all levels, including innovative governance processes to enhance citizens' participation and the cooperation between public and private actors, and, second, Europe's diversities and commonalities in terms of culture, religion, institutions, law, history, languages and values.

What challenges might the Commission face?

We see three challenges that the Commission might face in following our recommendations. First, Joint Calls tend to be administratively time consuming in terms of internal Commission negotiation and coordination. However, this is not a good reason to reject the idea of further Joint Calls. We have already noted our view that Joint Calls have the potential to generate powerful synergies with other 7th FP Cooperation themes that have the possibility of generating important new knowledge and capabilities that can be used in the civil security domain.

A second challenge is the difference in approach between themes. The Security Research theme is mission-oriented and includes a strong emphasis on user engagement, while other themes do not have these characteristics. In this respect, the Public Health theme would appear to be the closest to that of Security Research , since there is strong user engagement through clinicians and public health agencies, and a focus on a mission related to global health issues. SSH is likely to be the furthest from the mission-oriented and user engagement approach.

A third challenge is the difference in perspective between the themes. In approaching other themes, officials with responsibility for the Security Research theme should be aware and should respect potential differences in perspective. In the case of Health, the Joint Call should be focused on areas which could strengthen generic public health capabilities to address pandemic and other threats, whatever their origin. A Joint Call should avoid areas that appear to “securitise” aspects of the health agenda. Equally, it should be recognised that the SSH community tends to adopt a “critical” perspective on the security agenda. This is useful and important, since there is recognition (not least as expressed at the recent FORESEC Final Conference) that the security community has found it challenging to engage with civil society.

Recommendation 4: Enhance threat and risk analysis capabilities

The Commission should improve European threat and risk analysis capabilities through the stimulation and coordination of efforts at the national level (either through the office of the President/Prime Minister or through Ministries of the Interior).

What has already been achieved?

By way of example, we have identified the French Ministry of the Interior's attempt to develop a capability planning culture by creating, in July 2008, the "*Délégation à la prospective et à la stratégie"*. The aim of this new delegation was to "define and invigorate the Ministry's strategic actions"[240], but it already appears to be suffering from budgetary constraints. Moreover, while the *Délégation* should be prioritising the adoption of the MoI's initiatives and structures over the coming five to fifteen years, it does not seem to have any real capability planning focus. As one interviewee put it, "the [French] MoI is about people, not technologies and capabilities". This may very well be true for most European MoIs.

Why should the Commission intervene?

A clear and up-to-date analysis of the threats and risks facing European security is critical for the planning of possible responses. This would help public security customers, and in the future even EU security agencies such as Frontex, define precise capability requirements from the supplier base. Stakeholders often complained during the interviews about a lack of technology knowledge and awareness on the part of the public security end-users, who often struggle to identify their capability needs. This issue is particularly difficult for suppliers coming from the defence sector, which are used to having a clear-minded interlocutor (MoDs). Capability at European level in risk analysis would contribute to closing the gap between public security end-users and the supply base, increasing the ability of suppliers to plan production in advance and provide the required equipment at the right moment.

[240]From the French MoI website, http://www.interieur.gouv.fr/sections/a_l_interieur/le_ministere/organisation/dps

What should the Commission do?

The Commission should encourage national MoIs to develop a culture of capability planning fostering the identification and sharing of best practice.

These developments could also ease transatlantic dialogue

The ultimate goal could be to establish a permanent EU risk analysis capability at an institutional level. The ESRAB/ESRIF process has produced important findings, but there is a need for a politically driven risk analysis capability in order further to develop common missions and systems.

What challenges might the Commission face?

These processes are very clearly linked to national sovereignty. Taking into account the boundaries of sovereignty would therefore be indispensable to envisage MS involvement.

Recommendation 5: Establish a European Security Congress

In Chapter 3, our analysis has showed that there is a lack of European institutional coordination of security demand. This is a very sensitive policy issue. Therefore, we have recommended that the Commission establish a European Security Congress to launch a process of improvement of the governance of the security sector as a whole. This would represent an additional step compared to the ESRIF approach and would provide industry with a coherent agenda for cooperation and a structure within which to bring together the heterogeneous security end-users inside 7th FP activities.

What has already been achieved?

Much analysis and many proposals are already available on this matter. In September 2007, for example, the European Security Research and Innovation Forum was established as an informal and voluntary group of experts tasked to develop a "joint security research and innovation agenda" which finally resulted in its final report published in December.[241] The European Organisation for Security, representing suppliers from different security domains, has also produced a series of White Papers on "priorities for a future European Security Framework" (border management, civil protection, civil aviation security, energy infrastructure, etc.).[242]

The Commission should exploit and capitalise on this existing work.

Why should the Commission intervene?

The single main challenge identified by the stakeholders we interviewed is the fragmentation of demand in the security sector. A Security Framework linking together, under a common umbrella, all the different activities of the security and defence fields would maximise synergies and offer a coherent market for suppliers' involvement. This is an ambitious step which could be launched through a Security Congress.

[241] ESRIF, *European Security Research and Innovation in Support of European Security Policies. Final Report*, Brussels, 2009.

[242] See EOS official webpage: http://www.eos-eu.com/WHITEPAPERS/tabid/225/Default.aspx

The EU has in fact launched a wide array of initiatives in the field of security, and to a lesser extent in the defence one. Within the European Security Research Programme, the EC has been funding research activities to develop security technologies and knowledge. The EC has also proposed a European Programme for Critical Infrastructures Protection (EPCIP), whose aim is to enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures. In the field of defence, the most notable EC initiative is the Defence package, which includes two Directives respectively on intra-EU transfers of defence products and on defence and security procurement and a framework Communication (Strategy for a stronger and more competitive European defence industry).

The systematic involvement of "end users" in the Security Research programme is a useful answer to the need for creating a better understanding between demand and supply. Nevertheless the development of security research has some policy implications that cannot be taken into consideration by operational users. This is why the European Commission should foster dialogue between the policy-making and industrial sides of security.

What should the Commission do?

The Commission should promote dialogue around Security themes involving all stakeholders, from politicians to industrialists.

An annual "European Security Congress" could be a high level event, with thematic sessions involving EU and MS representatives around policy platforms. Extremely useful would be the fostering of debate around the policy issues emerging from the implementation of security technologies in Europe. Such a congress should involve any organisation and institution operating in the security sector.

The production of an annual policy document, linked to the congress, should be envisaged, addressing key issues such as "threat definition and security policy", "regulation policy", "market overview", "assessment of ongoing EU efforts".

Such a congress should be conceived as an internal EU effort, and not a communication event to be delegated to the rotating presidency. This is why we recommend establishing a permanent

Security Congress Committee, under the responsibility of one DG, involving other services and institutions, such as the European External Action Service and the EDA.

What challenges might the Commission face?

The setting up of such a Committee for the Security Congress would be politically sensitive, potentially leading to intra-Commission discussions around competencies. A decision would have to be made as to which DG the Committee for the Security Congress should be attached.

Recommendation 6: The Commission as customer

The European Commission should start shaping the security market not only as a funder of research, but also as a customer. There are many ways to do this, such as technology development or pre-commercial procurement.

What has already been achieved?

The Commission has already fostered security research through the 6th and 7th FP. This has been a considerable effort, opening the way for the development and use of security technologies. This research and development phase would produce additional effect if it were translated into procurement activity.

Why should the commission intervene?

As we analysed in Chapter 3, the 7th FP is structuring security research by producing a "supply stimulus". 7th FP programmes for security should lead to the development of cooperative equipment projects, to be considered as the next step after conclusion of the research phase. The Commission could collaborate with other institutions, such as the EDA and ESA, for such procurement programmes, but retaining a key role in financial and political endorsement. The Commission could launch and finance programmes to be subsequently developed by agencies with technical competencies.

What should the Commission do?

To develop its role as a customer, the Commission could focus on the already mentioned missions:

- ***Crisis management***: on the basis of the institutional developments, programme documents and political statements considered above, we expect EU crisis management missions (civilian, military, and in particular joint civilian-military) to increase in number and size in coming years. It is not evident, however, that this trend will go hand in hand with significant developments in market opportunities for the defence and security

industry.

- ***"High-end" security***: the majority of stakeholders interviewed are strongly convinced that the "High-end" security sector will become an attractive market in the future, for both defence and security companies.

Generally speaking, and in terms of capability and equipment, the European Union seems to lack two types of global system, or systems of systems: information and data integration gathering. Greater business opportunities for system integrators from both the defence and civil sides would be generated if we could move from an equipment-based approach and instead adopt a higher level of integration.

On the basis of feedback received from stakeholders, surveillance appears as an opportunity for the EU to shape demand. Surveillance of the EU's external borders is considered a major potential market (especially maritime borders/Baltic Sea, Black Sea and the Mediterranean[243]). Border protection requires a joint effort by various security actors and armed forces and a coordination of capability needs. However, opinions tend to diverge on the existence of common requirements in this area. Situation awareness is recognised by all security actors (military and non-military, EU and EDA) as a major blurring opportunity that should be approached in common. All the actors involved would benefit if the information available could be analysed and processed by a common system before a decision is taken, allowing the delivery of appropriate responses by the various actors concerned. For example, numerous stakeholders are hoping to develop new capabilities for surveillance, such as UAVs. Frontex identified UAVs as solutions to future capabilities needs. The military are also in the process of defining their UAV needs and there is a willingness to develop UAVs for civilian and military use. On the Security Research side, we can observe a high number of projects which are developing this awareness capability, for example in the maritime surveillance field.

Concerning the equipment, the need for large scale technological responses, such as UAVs or satellites, is controversial. Opinions diverge between the defence and security communities about the platform to be used. For defence, space oriented technologies can provide worldwide

[243] Terrestrial borders are less important, since they are mainly between Member States (Schengen) and their protection is purely for traditional police forces.

coverage. For security, it is argued that local deployment (such as UAVs, balloons or helicopters) could better fit needs. The geographical coverage needed for surveillance of the EU's external borders (border monitoring) or crisis management outside the EU is not so different. Surveillance platforms such as satellites, UAVs, balloons may in fact be complementary, as their use depends on the type of operation concerned. The debate about platforms is often skewed by organisational culture or willingness for independence, affecting the decisions taken.

Directly related to the surveillance sector, we found relevant business opportunities in the market of autonomous self-organised networks of smart sensors. As emphasised in Chapter 2, these smart sensor networks are aimed at building a comprehensive picture of an operating environment, and are particularly relevant since they can take the form both of unmanned vehicles and fixed networks of sensors. As seen, such technologies clearly have a blurred application in security and defence contexts, and will be particularly effective in border control activities, since they enhance intelligence gathering and surveillance. Furthermore, as these technologies could involve innovations in hardware and software used to sense signals, store sensed data, communicate and process information, they could also be applied to other security tasks, such as the identification and detection of improvised explosive devices.

The Commission could procure surveillance capabilities to EU MS through European agencies. This could be also done through a "capability oriented approach", as described in Chapter 5, enabling the Commission to buy services to enhance European security. Another approach could be that the Commission directly contributes to the pooling of surveillance resources, with direct ownership of systems.

What challenges could the Commission face?

The main challenges lie with the institutional evolution needed to develop European procurement for security systems. National sovereignty still rules most security policies, which raises some considerable difficulties for the development of common European systems. Nevertheless, some areas could be chosen for the development of « start-up » programmes which would introduce technologically based added value for security operators, with limited competition with existing

and legacy systems. The Commission action could launch pre-commercial procurement for security equipment or services in areas where market development possibilities are very low.

Recommendation 6.1: Development of dual-use space systems

What has already been achieved?

In Europe, space technological development has been mainly driven by research, building on programmes led by the European Space Agency (ESA). Space applications specifically for the defence and security sectors have been developed more recently.[244]

The need for global capabilities to support external operations has lately emerged among European countries, after the 1990s Balkans conflicts.[245] Particularly, European military space EO is relatively recent. Since 1996, there has been a shift in military EO needs: feedback from international operations (Balkan-type) has helped define new operational needs, calling not only for intelligence capabilities but also for operational support for planning with products such as rapid mapping.

Recent crisis management activities have led to a renewed expression of requirements for EO satellite support in terms of flexibility and increased revisiting time. In the meantime, the evolution of European crisis management has increased cooperation between defence and non-defence actors, providing a new template for the security mission. Typically, security elements within a crisis management operation bring together public security actors, such as defence forces and the police (Carabinieri/Gendarmerie), specialised administration teams (such as Foreign Affairs) and civil protection capabilities (when crisis management expands to emergency/safety).

This shared approach has lead key European countries to create a dual-use EO space programme.[246] The dual-use concept, actively promoted by the Italian authorities, is providing a solution to the blurring of missions, particularly in "crisis management" and "High-end" security.

---

[244] Historically, France was the first country in Europe to develop autonomous space tools for its defence needs, as space telecommunications and intelligence were considered necessary to complement French nuclear capabilities: satcom satellites were used to communicate with nuclear submarines and EO satellites provided intelligence. The post cold war era has created a shift in the use of these communication and EO capabilities, expanding from the nuclear strategy to the support of external operations which have characterised renewed military activity. The French EO Helios satellite programme corresponds to this shift.

[245] For a global analysis of space and defence assets in Europe, see the 2007 IAI/FRS Study for the European Parliament: "The cost of non Europe in the field of satellite based systems".
http://www.europarl.europa.eu/activities/committees/studies/download.do?file=19571

[246] In 2004, Italy signed a contract to provide a constellation of 4 EO satellites, COSMO SkyMed. From the outset, COSMO SkyMed was intended as a dual use civilian and military programme. It has been funded by both the Ministry of Research and the Ministry of Defence and will provide EO services for both communities. It is important to underline that COSMO SkyMed has been designed to provide services to public users, from military to civilian, with

The example of COSMO SkyMed indicates an interesting trend and highlights a transformation in the "defence" function, which, for some systems, is beginning to define more open multi-user systems:

- The COSMO SkyMed programme is a new system for a new community of users, responding to crisis management and territorial monitoring needs. Even if the military already had access to EO systems, this programme creates a new tool which does not have to manage legacy systems. Its implementation has not been without difficulty, as some potential communities of users have had to create new procedures, but it represents an added-value compared to existing systems.
- COSMO SkyMed is a publicly funded system, meaning that it can provide services for public administrations (military or civilian) as well as selling commercial services. This public funding framework is built on a matching of resources from both the defence and research ministries, which also has the effect of compensating for budget difficulties. The military side of COSMO SkyMed has "national security" features, but it also contains an innovative system for prioritisation and data access which meets the needs of civilian public actors.
- The system has also been built to meet Italian requirements for collaboration in international agreements, such as data sharing. Cooperation with France and participation in GMES are two main drivers of this specification.

This Italian programme is not isolated. It has been developed within the ORFEO French-Italian bilateral agreement signed in 2001 in Turin. This agreement defines an integrated cooperation between Italian COSMO SkyMed and French Pléiades EO satellites constellation.[247]

These dual-use space programmes have generated important industrial developments. They define a market for strategic technologies and promote a pooling of user communities on a multilateral basis. Both dual-use space policy programmes take into consideration the blurring of

applicability also to security missions and the general enhancement of security. Available at: http://www.asi.it/it/attivita/osservazione_terra/cosmoskymed

[247] Pléiades optical satellites will be launched between 2010 and 2011. Pléiades is a CNES programme funded through the Ministry of Research, but it is defined and budgeted as a dual use "security and defence" programme. The Pléiades programme indicates the evolution of French space policy, which takes into consideration new defence and security needs through a dual-use approach.

missions as a starting point, setting up dual-use defence/civilian systems. If we look at how they deal with the different communities, there is a division between "public users" (civilian or defence) and commercial users. A segmentation of priorities and products has been undertaken to fulfil different users' needs and requirements. It is not "defence" against the others, but more a graduated treatment of requirements. Clearly this flexible and qualified approach is a solution to the blurring, producing flexible products able to adapt to all communities, including particularly data security and very different "Post Cold War" and "High-end" security (border control) mission requirements. Furthermore, it is important to take into consideration the fact that space origin data is often considered as an autonomous added-value, and does not have an impact on the existing division between civilian and military organisations. There is no need for "joint" interoperability, but the sharing of the same information source through access to a new technology.

Why should the Commission intervene?

The European Commission already plays a key role in dual-use development through its "flagship" programmes. Space appears already to be a high profile policy for the European Commission. The ESA/EU Global Monitoring for Environment and Security (GMES) programme aims to provide an independent European EO capacity to deliver services in the environmental and security fields[248]. The 2001 GMES action plan described the potential contribution of such a "network of systems" to Common Defence and Security Policy, also referring to emerging needs for crisis management. From the beginning, the "S" of GMES described the setting up of services in order to fulfil EU security missions, typically "blurred" security and defence missions. This analysis shows similarities with the Italian and French dual-use space policy. The idea behind GMES was a mix of coordination of existing capabilities with the development of new assets (the Sentinel satellites) in order to enhance EU monitoring capabilities. Since 2001, GMES has made considerable progress, also with the benefit of EU funding through the 7th FP. Since 2008, four pre-operational services have been launched (land monitoring, marine, atmospheric composition and emergency response). Both climate change and security services seem to need further definition before they enter the pre-

[248] http://ec.europa.eu/gmes/pdf/communication_589_en.pdf

operational phase. This difference in implementation indicates the difficulties in gathering an EU security community able to put into use a common network of monitoring systems.

A very important factor to be taken into consideration is the multilateral framework of dual-use space systems. Until now, France, Italy and Germany have established bilateral agreements based on the exchange of capabilities.

In order to obtain a more "European" system, the European Commission could invest in its own security systems, thereby providing capabilities to be exchanged with countries already operating their own system. This would solve the problem of national ownership and return on investment, which seems to be a strong barrier to a pan-European system. Furthermore, European investment in space technologies is an important enabler for a high tech industrial sector. This potential for genuine "EU" investment in dual-use space based awareness capabilities is a key issue, as it seems to be the only way to reach a form of real European system. The GMES planned infrastructure (sentinel satellites) will strengthen European capabilities in the field of environmental monitoring. For security, Europe relies on existing systems and agreements based on an exchange framework (for example of images) which, de facto, exclude non-space countries from services. Direct EU investment could overcome this problem creating, EU ownership of space-based security capabilities.

What could the commission do?

The Commission is already engaged in significant efforts to support and finance space policy. The security side of GMES, the "S" of GMES, has been identified as a political priority, but it has still to be developed. There is growing interest, among the stakeholders we interviewed, in the improvement of space-based systems for security. The Galileo programme pools together existing experience and is defining a cooperation framework between the EC and ESA for the launch of such a programme. The Commission could use an already existing institution, such as the European Union Satellite Center (Torrejon), to manage a European Union EO security capability. The European Commission could also adopt a mix of different approaches to develop space technology procurement: the development of proprietary systems (with ESA playing the role of a technical agency) and the investment in service contracts with existing providers (already

mentioned dual-use systems) to deliver European capability and contribute to sustaining and participating in the development of the next generation of satellites.

What challenges could the Commission face?

The development of dual use space systems raises two types of challenge. The first is the same as quoted in the former recommendation, meaning the need to resolve sovereignty concerns over the use of security systems. The second deals with the technical capabilities required to implement space systems. ESA could represent the solution to the technical requirements of such programmes, while innovative solutions should be sought to ensure appropriate governance of the systems via the existing European agencies.

In this final section, we look at the two remaining recommendations outlined in the introductory paragraphs to this chapter. We follow the same structure used to analyse the first set of recommendations.

Recommendation 7: Strengthening coordination of research activities between the Commission, EDA and ESA.

Based on the opportunities offered by the Lisbon Treaty, the Commission should identify, in cooperation with ESA and EDA, possible ways to rationalise research investment efforts in the blurred areas of common interest. The purpose of this section is to raise some points that the Commission may wish to reflect upon as it engages with the EDA on this important matter.

What has already been achieved?

Since the inclusion of security research in the Seventh Framework Programme, the European Commission and the European Defence Agency have already interacted fruitfully in the research area. Software Defined Radio and the insertion of UAVs into civil airspace are agreed to be examples of successful cooperation (although these were not cooperative projects strictly speaking, but rather parallel investments in a common area of interest). In each case the European Commission and the EDA have contributed according to their respective responsibilities for civil security and defence (ESDP) missions.

From the beginning, cooperation has been on ad hoc basis, where common mutually beneficial opportunities have been identified through informal and ad hoc processes driven by officials in each organisation. The Framework Cooperation for Security and Defence Research adopted in November 2009 by EDA's Defence Ministers will provide a more official framework for the identification of common research themes. Nevertheless, it remains for the moment a formal document which still needs to be translated into concrete common research initiatives. This will not be an easy task, since common funding mechanisms between the Commission and EDA are still controversial. Until the Institutions concerned come to an agreement on the interpretation of the Lisbon Treaty on this issue, it would be beneficial to develop this cooperation along the line of the "Structured Dialogue on Space", between the Commission and ESA. This Dialogue has

produced a list of critical technologies, activities on the space-related security aspects of GMES, as well as the issue of space situational awareness (SSA).

Why should the Commission intervene?

The EDA and the Commission have the task, among many others, of strengthening the competitiveness of the European defence and security industries respectively. It should be recalled, however, that MSs have long developed national rules and specific market control mechanisms for the defence sector, since they do not consider defence as subject to EU internal market regulation. The Commission should have an interest in preventing such practices from also developing with regard to the security industry. It has a mandate, a diverse set of tools and ample experience to deal with industrial policy issues. Close cooperation with the EDA on the aspects mentioned above will allow the Commission to affect industry and market issues that MSs might otherwise decide to deal with on a national basis.

Participation by the Commission in common research projects will also be an incentive for smaller countries to make an active contribution, as they regard the Commission as a counterweight to the interests of “large” Member States.

What could the Commission do?

We suggest that the Commission reflect upon four particular aspects as it engages with the EDA on this matter. First, the EDA is likely to recommend the establishment of a Coordination Committee comprising members of staff, participating Member States, the European Commission, the European Space Agency and other European stakeholders. This is an important development which will institutionalise cooperation and provide the “suitable framework” requested by the Council of Ministers. The Commission should ensure that this is a standing body whose remit goes beyond situational awareness, the first area of interest, to allow the identification of other areas for mutually beneficial cooperation.

Second, the Commission needs to provide the necessary consideration as to how it will identify common capabilities. The EDA has a process in place which attempts – within the limits of the sensitivities and varying openness of participating Member States - to identify capability

requirements and their translation into R&T priorities. The Commission will therefore need to develop its own approach and mechanisms towards the capability process. It is true that some civil security capability requirements have been identified through the ESRAB process. However, end users were hardly represented in this process, and it is not representative of the entire end-user community in this area. For an appropriate identification of civil security requirements, the Commission would need to bring together more experts/users from MSs. The Commission could serve – as in the ESRAB process – as a secretariat, which would identify not only priority technologies, but also Technology Roadmaps. This process would provide a systematic foundation to identify common civil security and defence requirements with the EDA.

Third, on this basis common priority areas could be defined and agreed upon. In this context the Commission needs to ensure that there is a common understanding amongst all stakeholders as to the criteria used to define priority areas for funding. The priorities of the European Commission and the EDA have much in common, but there are areas where they differ. The Commission must ensure that its agenda is respected. Four criteria in particular should determine the selection of areas for cooperation:

- Capability requirements - the Commission has pursued a capability gap driven approach to research prioritisation, complemented by a bottom-up process which scopes and examines technologies to assess how they could contribute to European security.
- Security of supply/European autonomy - industry has repeatedly expressed concerns about security of supply issues for such components as infrared detectors and electronic components. This suggests that security of supply/European autonomy considerations should be taken into account in identifying priority areas for cooperation. In turn, this would require identification of vulnerable technologies. Here the Commission and EDA need to arrive at a common understanding about the strengths and weaknesses of the industrial and technological base supporting defence and security.
- Growth, employment and competitiveness issues – the potential market of an area should be taken into account in the selection of priorities since a large potential market will encourage more investment by private industry. These industry structure issues have received attention from the European Commission, but less so from the EDA. Some of the largest MSs have insisted on a capability (demand-side) focus to all EDA activities and have

opposed anything that they see as supply-side driven.

- Finally, the Commission needs to ensure an adequate funding of research activities. It has been made clear that under the Framework Agreement there will be no joint funding and the management responsibilities in both frameworks will remain unchanged. The Commission must seek reassurance that Member States (through the EDA) will make the necessary financial commitments to ensure the success of the proposed Situational Awareness programme and any subsequent joint programmes.

What challenges might the Commission face?

A fundamental challenge for the Commission is to understand the grand strategy behind the Defence Ministers' call for a Framework Agreement between the EDA and the Commission. At the moment, there is significant ambiguity in the Council's position. On the one hand, the Council of Ministers during the co-decision process for the 7th FP made it clear that the Security Research theme should be limited to civil security applications. On the other hand, the Defence Ministers in the EDA Steering Board have tasked the EDA with establishing a Framework Cooperation agreement with the explicit intention of institutionalising cooperation between the EDA's R&T agenda and the Commission's Framework Programme. Equally, some of the Defence Ministers have supported (and funded) ad hoc cooperation between the EDA and Framework Programme in the fields of Software Defined Radio and the insertion of UAVs into civil airspace.

Thus, it is important that the Commission ask the EDA at the highest political level for clarification of the intentions and "vision" of the Ministers of Defence.

On a practical level, the EDA and the Commission are very different organisations with different modus operandi. While the EDA has well established processes and mechanisms in place that cover the entire area from capability development to the identification of R&T priorities further to collaborative projects, the Commission's organisation is much looser. Moreover, the Agency needs to coordinate only one type of end user, the MoDs. It can, therefore, be expected that the EDA is much better suited to formulate and present its position.

Both organisations have different objectives. The EDA has a strong capabilities focus, and defence R&T is closely linked to procurement, frequently based on the assumption of full government

funding. The EDA places a strong emphasis on promoting synergies and overcoming duplication through rationalisation. The Security Research theme of the Framework Programme places an important emphasis not only on capabilities but also on its contribution to growth and employment and the competitiveness of the European security industry. The Security Research theme is based upon a "competition of ideas" approach in which proposals are evaluated not only on user engagement but also according to scientific considerations. In addition the Security Research theme is based on shared funding of projects. The EDA and the Commission have different rules not least with regard to intellectual property rights (IPR).

Further questions that need to be addressed are:

- What happens after the research programme?
- Will defence Ministers (EDA) be willing to provide the necessary funding?
- How many MSs will participate?

As already mentioned, there may be opposition to a closer relationship between defence and security research. On the one hand, Member States have welcomed the Commission's role in SDR and UAVs and encouraged the Commission to play an enhanced role;[249] the European Parliament has also called on the Commission and the EDA to take an enhanced role. On the other hand, it should also be noted that, within the European Parliament, there was a minority dissenting position. Furthermore, Member States have made clear their intention that the focus of the 7th FP should be on civil security research. For the next 8th FP, the integration of defence related research could be an option.

[249] Cf council decision http://www.eu2008.si/en/News_and_Documents/Council_Conclusions/May/0526_GAERC-ESDP.pdf

Recommendation 8: Including defence research in the 8th FP

We recommend that the Commission begin a process of reflection on the opportunities and challenges arising from including defence research in the 8th FP. This should include, in particular, the appointment of a Group of Personalities on defence research. This reflects the highly contested nature of this issue and, only after detailed reflection, – including participation by stakeholders outside the security community and especially with civil society – should the Commission consider establishing a Preparatory Action on Defence Research.

We emphasise that by "defence research" we have in mind not the full spectrum of defence, but rather very specific aspects that are of interest to the entire Union, not just to particular Member States. On the whole, this means research activities that would enhance European capabilities in support of the ESDP Petersberg Tasks.

What has already been achieved?

The inclusion of a security research theme in the 7th FP focused on civil security applications and non-lethal technologies. This was an important step. Dual-use technologies may have been funded on an ad hoc basis under previous Framework Programmes, but the Security Research theme is the first formal step of the Commission into the civil security realm.

Respecting declarations by the Council of Ministers and the founding principles of the EDA, the Commission and the EDA have explored ways of working together in *ad hoc* ways and reflecting their different competencies. Software Defined Radio and the insertion of UAVs into civil airspace show the benefits of such an approach.

In the context of the Lisbon Treaty, there is discussion among stakeholders at the European level about the possibility of including defence[250] research in the 8thFP.

[250] We emphasise once again that "defence" in this context means the ESDP Petersburg Tasks.

Why should the Commission intervene?

The Commission should begin a process of reflection on the opportunities and challenges of including defence research in the 8th FP for three main reasons. First, the issue is already being discussed informally amongst stakeholders, and an official reflection process would make the discussion more open and transparent. Second, the idea is highly controversial and highly contested and requires detailed and in depth consideration before any policy initiative is undertaken. Third, there are significant contradictions in the position of Member States on this and related matters and a reflection process could help clarify for the Commission the position of the Member States.

A need for clarity

We have emphasised that there is a need for greater clarity as to the intention of Member States in the field. At the moment, there is significant ambiguity in the Council's position, which presents a significant barrier to the inclusion of defence as a theme within the Framework Programme. Clarity is required regarding the views of the Council of Ministers on these matters. In particular, any further development requires the Council of Ministers to remove its stricture on civil security applications of Framework Programme funding and accept their use for Petersberg Tasks.

Our consultation with stakeholders suggests that the idea of introducing "defence" (however defined) into the Eighth Framework Programme is likely to be highly contested. Accordingly, we now set out a potential rationale for including defence research in 8th FP, before considering some of the potential objections to such an approach.

Rationale for the inclusion of defence in the 8th FP

We have emphasised throughout this study that the security-defence distinction is becoming increasingly blurred at the technology level. Moreover, this distinction is slowly blurring at the operational level. Consequently, it is increasingly difficult to make a distinction (as the 7th FP security research theme is obliged to do) between research for civil security applications and research for Petersberg Tasks.

We note that the Council Conclusions on ESDP of 11/11/2008 called for greater R&T efforts coordinated with the Commission. In particular: "The Ministers for Defence now call for: – greater efforts in the area of defence research and technology, coordinated with the Commission, in order

to develop at European level the technological responses to medium-term and long-term operational requirements".

We also note the European Security Strategy Implementation Report of 11/12/2008 which called for better institutional coordination and declared that "we must strengthen our own coherence, through better institutional co-ordination and more strategic decision-making".

Furthermore, we note that the legal mandate of the Lisbon Treaty has been interpreted by some Commission officials as opening up the possibility of the Commission undertaking defence research within the Framework Programme. In our consultation with stakeholders we did not find any dissent from this interpretation. Equally, it has to be considered that some stakeholders are only now beginning to consider the implications of the Lisbon Treaty.

The argument against the inclusion of defence in 8th FP

The Commission should also recognise that there are very strong and persuasive arguments not to include defence in the 8th FP. Including any kind of defence R&D in the 8th FP would raise important questions that need consideration, not only by the defence and security community, but also by the broader scientific community and civil society. Those questions include:

- What would it mean for the character and priorities of European science and technology and the ERA?
- Would it mean that some Associate countries might be excluded from this activity, because of the sensitivity of the technologies being developed?
- How would the necessary secrecy and confidentiality of some of these areas (both during project evaluation and also dissemination) affect the future character of the Framework Programme, also taking into consideration the 7th FP experiences in classified projects?
- Would the immediate mission-oriented and procurement-oriented characteristics of the defence innovation model impact on the "competition of ideas" model and the emphasis on scientific peer review that characterises the Framework Programme? The EC security research can be considered as a model but should be adapted to Defence specificities. In addition, there are very different IPR arrangements for defence (EDA) and civil security (Commission): in the former, IPR remains with the funder, in the latter, IPR is with the research consortium.

- What might be the implications of a growth of Framework Programme research focused on security and defence for other areas (competition with other important and powerful stakeholders, for instance in the aeronautics or ICT programmes)?
- What would be the response of industry? Some in industry would welcome this as a source of additional R&D funding. However, there are others who point out that FP is different to defence R&D.

What could the Commission do?

The highly contested nature of this subject leads us to recommend that the Commission engage in a broadly based reflection process before embarking on any such policy initiative. For this purpose, the experience gained with the insertion of the Security Research theme into the 7th FP is specifically valuable. A critical reflection on the lessons learned and an adaptation to the specific nature of the defence topic could yield valuable ideas of how to design such a process. In the following we sketch out this mechanism and comment on it (For a timeline see Table 6, p. 227).

Establish a Group of Personalities

We recommend that the Commission begins by establishing an advisory group on defence research. This Group of Personalities (GoP) would be tasked with exploring the modalities, issues, processes and wider questions related to the implications for the nature of European science and civil society associated with defence research in support of ESDP missions. The Group of Personalities would be comprised of representatives from Member States' Ministries of Defence, the Council, the EDA, EC, EP, the defence industry and other industry, research institutes, representatives of the European scientific community (including the European Science Foundation and national scientific bodies) and civil society.

We recommend that the Group of Personalities be tasked with developing and assessing a variety of options, amongst which might be:

- Establishing defence as a theme under the 8th FP, managed by the Commission
- Establishing defence as a theme under the 8th FP, managed by the EDA
- Establishing defence as a theme for a joint research programme funded jointly by the

Commission from the 8th FP and the EDA

- Funding research in support of the civil dimensions of the Petersberg Tasks only.

Options for reflection by the Group of Personalities

We now turn to consider the options that we recommend the Group of Personalities should consider. Of course, there may be others that the GoP identifies and these should be given equal consideration. These options are:

Establishing defence as a theme under the 8th FP and managed by the Commission

We emphasise once again that by "defence" we have in mind mission-oriented research undertaken in support of the capabilities necessary to fulfil the Petersberg Tasks. Several conditions would be necessary to make this option viable, such as political support of the Council of Ministers and the European Parliament and the establishment of a new ESRAB-like process.

Establishing defence as a theme under the 8th FP and managed by the EDA

The High Representative will be responsible for CFSP, including the EDA, and will also be Vice-President of the Commission. Consequently, it might be anticipated that the traditional institutional boundaries of the old Pillars will be less significant as the full implications and institutional geography of Lisbon becomes apparent.

A large part of the Seventh Framework Programme is managed on behalf of the Commission by the Research Executive Agency, a fact that might be seen as a precedent. The EDA has the advantage of having in place the necessary security arrangements to manage such activities. The Agency has a different intellectual property regime that may be better suited to defence research. Moreover, the EDA has the potential of pulling through the outcomes of research projects to users in a way that the Commission has found difficult in the Framework Programme. Although it has to be added that the EDA has also found this difficult in some cases, there is a closer link between research and procurement.

A major problem however may arise with respect to the equity of budget arrangements. The Danish government has opted out of any decision-making with defence implications and, hence, does not participate in the EDA. Consequently, Framework Programme funds (open for bids from

applicants from all 27 Member States) would be used for an activity and potentially transferred to an institution from which one Member State has chosen to opt-out. More than that, if the EDA were to manage these funds through its Cat A process, this would also exclude the UK that has a policy of not participating in Cat A projects. As a result, the more appropriate approach would be to manage FP funds through a new arrangement to be developed.

Establishing defence as a theme for a joint research programme funded jointly by the Commission out of the 8th FP and the EDA

Ultimately, however, if FP funds are to be transferred to the EDA for management, it would seem more appropriate for this to form the basis for true joint programmes. The EDA Defence Ministers' statement on the Framework Cooperation agreement made it clear that this would not lead to joint programmes, but this does not discount such joint programmes in the future. Joint programmes would go beyond the *ad hoc* approach used for Software Defined Radio and UAVs, paving the way for jointly funded programmes to meet jointly agreed priorities and are jointly managed under the supervision of a single Management Board.

This recommendation has some obvious difficulties. In particular, Member States have employed variable geometry in their participation in EDA projects. We have noted that the UK does not participate in Cat A projects. SDR and UAV have had differing memberships. Thus we would face a situation in which all Member States fund projects (through the Framework Programme), but only some Member States provide the "matching funds" through the EDA. Equally, there is the question of which intellectual property approach would be used, that of the EDA or the Framework Programme.

Finally, would funding be allocated on the basis of a "competition of ideas" as with the Framework Programme, or a more user-driven approach?

Funding research in support of the civil dimensions of the Petersberg Tasks only

Another alternative has been put to us during the course of our engagement with stakeholders, namely that civil security research money could be used to fund technologies that support the civil dimensions of the Petersberg Tasks only. This argument starts by pointing out that few out of the twenty three ESDP missions have been military in nature. The bulk has been civilian i.e. monitoring, rule of law and police missions. Accordingly, it could be argued that future (indeed

even existing) security research funding could be used for research that supports the technologies necessary for these, non-military and non-lethal, external missions.

Establish a Preparatory Action on Defence Research

Our discussion of the possible options and some of the challenges suggests that the inclusion of defence in the 8th FP would be far from straightforward and would raise some fundamental and serious issues that must be seriously debated, including by the broader non-security science community and civil society. In the event that the GoP recommends further action in this field, however, we would strongly advise that the Commission establish a Preparatory Action on Defence Research. The inclusion of defence research in the 8th FP would be an important development that would raise significant new issues of process and content for the Commission, EDA, Member States and other stakeholders. Accordingly, the Commission would be well advised to pursue the same approach that it used in the security research field when it established the Preparatory Action on Security Research (PASR).

What challenges/issues might the Commission face?

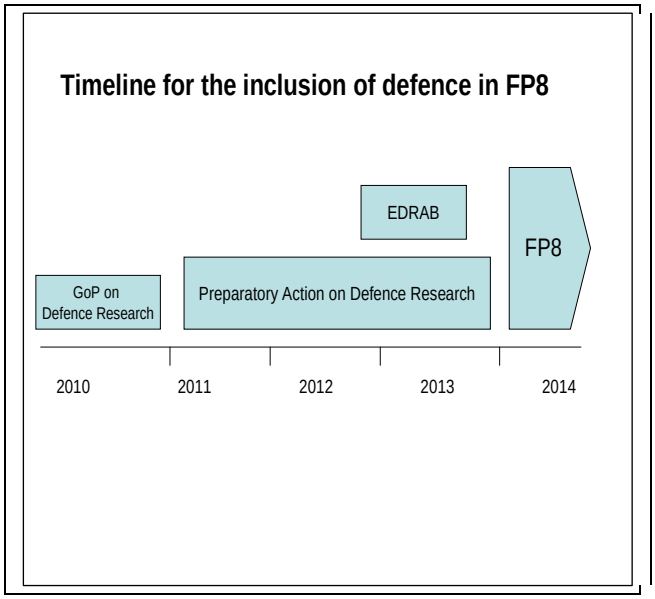
The challenges and issues that might arise in the inclusion of defence in the 8th FP have been a central focus of the discussion, since they are at the core of questions about the desirability and feasibility of such an initiative. Here we focus rather on the timeline that the Commission would need to meet if defence research were to be included in the 8th FP. Assuming that this followed a similar timeline to the introduction of civil security in the 7th FP, we make the following points:

- The Group of Personalities would need to be established very soon to allow it to report by the end of November 2010. This would require a political decision by the Commission as to the desirability of such an action, supported by initial consultation with key stakeholders, in particular the Member States and the new High Representative. Once such a decision was taken, the Commission would need to determine the membership of the GoP, appoint a *Rapporteur* and establish its terms of reference (we recommend that the terms of reference be based on a consideration of the options that we have set out above).
- The Preparatory Action on Defence Research would need to be established with a First

Call early in 2011. A three year PADR would allow all practical issues of procedure and operation to be evaluated.

- The content of the defence theme under the 8th FP would need to be considered and agreed. We have already recommended that the Commission should argue the case for a permanent institutional structure between key stakeholders along the lines of the Structured Dialogue on Space and Security. If this were to be established, then this body would be most appropriate for establishing the research agenda. Otherwise, the Commission would need to establish an ESRB-like body to consider such matters, what we have called in the timeline "EDRAB" – the European Defence Research Advisory Board.

Table 6: Timeline for the inclusion of defence in 8th FP



Annex 1. List of stakeholders interviewed

Industry

- *Aero Sekur*
- *BAE Systems*
- *Boeing Europe*
- *Bosch*
- *Capgemini UK Plc*
- *DCNS*
- *Diehl*
- *EADS*
- *EADS Astrium*
- *Finmeccanica*
- *Fujitsu UK & Ireland*
- *IBM Europe*
- *IBM UK Limited*
- *Jenoptik*
- *L-3 COMMUNICATIONS ASA LIMITED*
- *MBDA*
- *Oracle Corporation UK Ltd*
- *QinetiQ Group*
- *Raytheon Systems Limited*
- *Rheinmetall*
- *Rolls-Royce*
- *SAFRAN*
- *Safran (Sagem)*
- *SELEX Galileo*
- *Smiths Detection*
- *Steria Services Limited*
- *Thales*
- *Thales Alenia Space*
- *Thales Deutschland*

- *VDI/VDE Innovation + Technik GmbH*

Industry associations

- *Aerospace and Defence Industries Association of Europe (ASD)*
- *European Organisation for Security (EOS)*
- *European Security Directory (ESD)*
- *Federation of German Industries (BDI)*
- *German Aerospace Industries Association (BDLI)*
- *German European Security Association (GESA)*
- *INTELLECT*
- *Society of British Aerospace Companies*
- *UK Trade & Investment Defence & Security Organisation*

European Institutions

- *Council of the EU (Civilian Planning and Conduct Capability, CPCC)*
- *Council of the EU (DG A 4 Finances)*
- *European Commission (DG Enterprise)*
- *European Commission (DG Internal Market)*
- *European Commission (DG Justice, Freedom and Security)*
- *European Commission (DG RELEX)*
- *European Defence Agency (Armament Directorate)*
- *European Defence Agency (Capability Directorate)*
- *European Defence Agency (Research Directorate)*
- *European Parliament*
- *FRONTEX*

National institutions

- *Délégation Prospective et Stratégie*
- *Direction de la Sécurité Civile*
- *Direction des Affaires maritimes*
- *Direction Générale de la Police Nationale*
- *French Ministry of Defence Direction Générale de l'Armement, DGA*
- *French Navy*

- *Gendarmerie - Centre de prospective de la gendarmerie nationale*
- *German Federal Ministry of Defence*
- *German Federal Ministry of the Interior*
- *Italian Air Force*
- *Italian Army General Staff*
- *Italian Army Medical Corps*
- *Italian Carabinieri General Headquarters Staff*
- *Italian Coastal Guard*
- *Military Mission of the Permanent Representation of France to the EU*
- *Ministère Economie et Finances*
- *Secrétariat général de la défense nationale*
- *Segretariato Generale della Difesa*
- *UK Home Office - Office of Security & Counter Terrorism*
- *UK Ministry of Defence International Relations Group, DE&S*

Other Institutions

- *Associazione Nazionale Alpini (Medical Director and logistician)*
- *Bundesanstalt Technisches Hilfswerk (THW - Federal disaster relief organization)*
- *European Security Research and Innovation Forum*
- *Fraunhofer Society*
- *German Aerospace Center (DLR)*
- *Greek Fire Brigade*
- *Greek Police*
- *INHES*
- *Italian Civil Protection (Communications Technician)*
- *Italian NGOs*
- *Italian Space Agency*
- *World Food Programme (Information Officer)*
- *Capitanerie di Porto*
- *DEMOS*
- *Laender Ministry of the Interior (Brandenburg)*
- *Royal United Services Institute*
- *Italian Red Cross (C.R.I.)*

Annex 2. Defence and security customers involved in blurred missions

MISSION	ACTOR	AUTHORITY	OPERATIONAL ROLE	EU MS BODIES
CRISIS MANAGEMENT				
	ARMY, AIR FORCE, NAVY	MoD	- Conducting security and stability operations, Supporting National Army or National Police.	
	ARMY, AIR FORCE, NAVY	MoD	- Advisory activities.	
	GENDARMERIE-TYPE FORCES	MoD/MoI	- Military Police.	CARABINIERI (ITALY); GENDARMERIE (FRANCE); ROYAL MARECHAUSSEE (NETHERLANDS); GENDARMERIE (ROMANIA); GUARDIA CIVIL (SPAIN); NATIONAL REPUBLICAN GUARD (PORTUGAL).
	GENDARMERIE-TYPE FORCES	MoD/MoI	- National Police Training.	CARABINIERI (ITALY); GENDARMERIE (FRANCE); ROYAL MARECHAUSSEE (NETHERLANDS); GENDARMERIE (ROMANIA); GUARDIA CIVIL (SPAIN); NATIONAL REPUBLICAN GUARD (PORTUGAL).
	CUSTOM & REVENUES POLICE		- Border Police Training on (custom regulations; border control; fight against drug, people and arms smuggling).	GUARDIA DI FINANZA (ITALY).
	POLICE		- Training (on road safety, stolen vehicles recovery,	POLIZIA STRADALE (ITALY); METROPOLITAN

			management of dangerous materials). Advisory activities.	POLICE (UK).
	PRIVATE MILITARY COMPANIES		- Personal and assets protection; bodyguard services (at least within the EU framework).	

SUPPORT TO CIVIL PROTECTION				
	ARMY, AIR FORCE, NAVY	MoD	- Logistic support; transport tasks.	
	FIRE CORPS	MoI	- Search & Rescue activities.	VIGILI DEL FUOCO (ITALY); SERVICES D'INCENDIE (BELGIUM); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); BOMBEIROS (PORTUGAL); DSPC (FRANCE) ;
	Mountain POLICE	MoI	- Support in S&R activities in mountain contexts.	POLIZIA DELLA MONTAGNA (ITALY); CUERPO NACIONAL DE POLICIA - SERVICIO DE MEDIOS AÉREOS (SPAIN);
	LOCAL POLICE		- Organizational support.	POLIZIA LOCALE (ITALY); POLICE MUNICIPALE (FRANCE); POLICIA MUNICPAL (SPAIN); POLITIA COMUNITARI (ROMANIA).
	COASTAL GUARD	MoD; MoD/MoI	- Logistic support in maritime environment.	GUARDIA COSTIERA (ITALY); GUARDIA CIVIL (SPAIN).

PROTECTION AGAINST TERRORISM				
	POLICE SPECIAL	MoI	- Special, covered,	NOCS (ITALY) ,THE

	FORCES		interventions during terrorist events. Protection of sensitive target both people and structures.	SERIOUS ORGANISED CRIME AGENCY (SOCA) (UK); CUERPO NATIONAL DE POLICIA – GRUPO ESPECIAL DE OPERACIONES G.E.O. (SPAIN) NATIONAL GENDARMERIE INTERVENTION GROUP (GIGN) (FRANCE); FRENCH POLICE RECHERCHE ASSISTANCE INTERVENTION DISSUASION UNIT (RAID) (FRANCE); NATIONAL POLICE INTERVENTION GROUP (GIPN) (FRANCE); GSG 9 DER BUNDESPOLIZEI (GERMANY); GRUPO DE OPERAÇÕES ESPECIAIS (PORTUGAL).
	POLICE BOMB SUADS	MoI	- Intervention on explosive materials in case of potential terrorist attacks.	ARTIFICIERI (ITALY) CUERPO NATIONAL DE POLICIA - GRUPOS OPERATIVOS DE DESACTIVACIÓN DE EXPLOSIVOS (SPAIN); CENTRO DE INACTIVAÇÃO DE EXPLOSIVOS E SEGURANÇA EM SUBSOLO – CIEXSS (PORTUGAL).
	MEDICAL AND SCIENTFICA POLICE	MoI	- Medical support in case of bioterrorist attacks	POLICIA CIENTIFICA (SPAIN) ; CUERPO NATIONAL DE POLICIA - GRUPO OPERATIVO N.B.Q. (SPAIN); SANITARIO DELLA POLIZIA DI STATO (ITALY).
	INVESTIGATION POLICE	MoI	- Monitoring and investigation on terrorist threats	DIVISIONE INVESTIGAZIONI GENERALI E OPERAZIONI

				SPECIALI (ITALY);
	POLICE DOG SQUADS	MoI	- Intervention on explosive materials in case of potential terrorist attacks.	BRITISH TRANSPORT POLICE - DOG SECTION (UK); GRUPPO ARTIFICIERI – NUCLEI CINOFILI (ITALY)
	DATA PROCESSING CENTER	MoI	- Information support for the investigative and operational activities.	CENTRO ELABORAZIONI DATI POLIZIA DI STATO (ITALY); SÄKERHETSPOLISEN DOCUMENTATION UNIT (SWEDEN).
	ANTITERRORISM UNITS	MoI/MoD	- Investigation on immigration and financial aspects of the fight against terrorism. - Surveillance activities in airports, ports and rail stations.	GUARDIA DI FINANZA - SEZIONE ANTI TERRORISMO PRONTO IMPIEGO, UNITÀ CINOFILA ANTICONTRABBANDO E ANTITERRORISMO (ITLY); GUARDIA CIVIL (SPAIN); NATIONAL COUNTER TERRORISM SECURITY OFFICE (NaCTSO) (UK); SÄKERHETSPOLISEN (SWEDEN SECURITY SERVICE).
	CIVIL PROTECTION	Generally MoI	- First response activities in case of NBCR attack; Medical support; detection of dangerous materials.	DIPARTIMENTO DI PROTEZIONE CIVILE (ITALY); DIRECTION DE LA DEFENSE DE LA SECURITE CIVILE (FRANCE); CIVIL NUCLEAR CONSTABULARY (CNC) (UK); PROTECCIÓN CIVIL Y EMERGENCIAS (SPAIN); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); PROTECÇÃO CIVIL (PORTUGAL).

	FIRE CORPS		- Intervention in case of non-conventional risks such as criminal acts against people with the use of nuclear, biological radiological and chemical weapons.	VIGILI DEL FUOCO SERVICES D'INCENDIE (BELGIUM); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); PROTECÇÃO CIVIL (PORTUGAL).

BORDER SECURITY				
	NAVY	MoD	- Patrol, surveillance and interception activities in blue waters.	
	MARITIME POLICE	MoI	- Surveillance, positioning and interception activities in brown waters (within 12 miles);	POLIZIA DEL MARE (ITALY); PORT OF DOVER POLICE, PORT OF LIVERPOOL POLICE (UK); GENDARMERIE MARITIME (FRANCE)
	COASTAL GUARD	MoD/MoIT; MoD/MoI	- Surveillance and interceptions activities in both blue and brown waters. Surveillance of national coasts.	GUARDIA COSTIERA GUARDIA CIVIL (SPAIN); KUSTBEVAKNINGEN (SWEDEN).
	CUSTOMS AND BORDER POLICE		- Aerial surveillance and exploration in territorial waters. - Surveillance, prevention and contrast activities towards illegal immigration. In charge of the coordination of different authorities involved in such tasks.	POLICE -DIRECTION CENTRALE DE LA POLICE AUX FRONTIERES (FRANCE) ; UK BORDER AGENCY (UKBA); POLIȚIA DE FRONTIERĂ (ROMANIA); POLIZIA DELL'IMMIGRAZIONE E DELLE FRONTIERE, GUARDIA DI FINANZA (SERIVIZIO AERONAVALE).
	POLICE AIR FORCE			POLIZIA REPARTO VOLO (ITALY) CUERPO NACIONAL

				DE POLICIA - (SPAIN).

CRITICAL INFRASTRUCTURE PROTECTION				
	ARMY	MoD	- Logistic support.	
	RAIL POLICE	MoI; MoI/MoD	- Surveillance and monitoring on railways and in the stations.	POLIZIA FERROVIARIA, BRITISH TRANSPORT POLICE (UK); SERVICE NATIONAL DE POLICE FERROVIAIRE (FRANCE); GUARDIA CIVIL (SPAIN).
	COMMUNICATIONS POLICE	MoI	- Operational room in charge of communications and coordination; Intelligence activity: data and info gathering and analysis for prevention purposes.	SÄKERHETSPOLISEN (SWEDEN SECURITY SERVICE); POLIZIA DELLE COMUNICAZIONI – CNAIPIC (ITALY).
	CUSTOMS AND BORDER POLICE	MoI	- Surveillance activity (in particular in ports and airports).	POLIZIA DELL'IMMIGRAZIONE E DI FRONTIERA (ITALY); POLICE -DIRECTION CENTRALE DE LA POLICE AUX FRONTIERES (FRANCE) ; POLIȚIA DE FRONTIERĂ (ROMANIA);
	POLICE MARKSMAN UNITS AND BOMB SQUADS	MoI	- "Remote protection" of critical infrastructure during public manifestation or events; Intervention on explosive materials in case of potential terrorist attacks.	ARTIFICIERI (ITALY) CUERPO NATIONAL DE POLICIA - GRUPOS OPERATIVOS DE DESACTIVACIÓN DE EXPLOSIVOS (SPAIN); CENTRO DE INACTIVAÇÃO DE EXPLOSIVOS E SEGURANÇA EM SUBSOLO – CIEXSS (PORTUGAL).
	MEDICAL AND SECURITY POLICE	Moi	- Medical support in case of biologic or chemical attack to	SERVIZIO SANITARIO DELLA POLIZIA DI STATO (ITALY);

			critical infrastructure.	POLICIA CIENTIFICA (SPAIN); POLICE SCIENTIFIQUE (FRANCE); CUERPO NATIONAL DE POLICIA - GRUPO OPERATIVO N.B.Q. (SPAIN).
	PORT AUTHORITIES	MoD; MoIT MoIT	- Surveillance and monitoring of activities within ports and their vicinities.	CAPITANERIA DI PORTO, AUTORITA' PORTUALI (ITALY); PORT OF DOVER POLICE; PORT OF LIVERPOOL POLICE (UK).
	ANTI-HACKING SQUAD		- Provides defence of critical information systems against information fraud.	GUARDIA DI FINANZA - NUCLEO SPECIALE FRODI TELEMATICHE (ITALY); CUERPO NACIONAL DE POLICIA - BRIGADA DE INVESTIGACIÓN TECNOLÓGICA (SPAIN); NATIONAL COUNTER TERRORISM SECURITY OFFICE - NaCTSO (UK).
	FIRE CORPS	MoI	- Monitoring, inspection and prevention activities against fires and industrial risks; - Mitigation activities in case of fire, uncontrolled release of energy, risks deriving the use of CBRN. - Intervention in case of non-conventional risks such as criminal acts against infrastructure with the use of CBRNE weapons.	SERVICES D'INCENDIE (BELGIUM); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); PROTECÇÃO CIVIL (PORTUGAL); VIGILI DEL FUOCO (ITALY).
	CIVIL PROTECTION	Generally MoI	- First response activities in case of attack or accident; Medical support;	DIRECTION DE LA DEFENSE DE LA SECURITE CIVILE (FRANCE) ; CIVIL

			detection of dangerous materials.	NUCLEAR CONSTABULARY - CNC (UK); PROTECCIÓN CIVIL Y EMERGENCIAS (SPAIN); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); PROTECÇÃO CIVIL (PORTUGAL); PROTEZIONE CIVILE - NUCLEO DI DIFESA CIVILE E NRBC (ITALY).
	PRIVATE SECURITY COMPANIES		Access control, remote CCTV monitoring and visual verification, mobile patrolling and installation surveillance, GPS tracking and control of vehicles.	- Security division of critical infrastructure companies. - Sub-contracting security companies (i.e. UK's FIRST SECURITY and EUROPA).

CIVIL PROTECTION				
	CIVIL PROTECTION	Generally MoI	- Overall management of disasters and catastrophes. Search&Rescue, mitigation, medical support; restoration of vital functions;	DIRECTION DE LA DEFENSE DE LA SECURITE CIVILE (FRANCE) ; PRTOECTION CIVILE (BELGIUM); PROTECCIÓN CIVIL Y EMERGENCIAS (SPAIN); ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG) ; PROTECÇÃO CIVIL (PORTUGAL); PROTEZIONE CIVILE
	ARMY	MoD	- Logistic support; transport tasks; restoration of vital functions.	(FORMATIONS MILITAIRES DE LA SECURITE CIVILE (COMFORMISC) FRANCE)
	FIRE CORPS	MoI	- Monitoring, inspection and prevention activities	SERVICES D'INCENDIE (BELGIUM);

			against fires and industrial risks; - Mitigation activities in case of fire, uncontrolled release of energy, risks deriving the use of nuclear, biological radiological and chemical. - Intervention in case of non-conventional risks such as criminal acts against infrastructure with the use of CBRNE weapons.	ADMINISTRATION DES SERVICES DE SECOURS (LUXEMBOURG); PROTECÇÃO CIVIL (PORTUGAL); VIGILI DEL FUOCO (ITALY).

Annex 3. Implications of Lisbon Treaty for security and defence

The Lisbon Treaty: new openings for the European defence and security sectors?

At present, under the provisions of the Treaty on European Union251 (TEU), the broad concept of SECURITY mainly applies to two major areas of the activity of the EU, independent one from each other:

- The Common Foreign and Security Policy (CFSP), which includes the European Security and Defence Policy (ESDP)
- The Police and Judicial Cooperation in Criminal Matters (PJC)

Said briefly, the main difference between these two areas is that the CFSP/ESDP responds to the European request of external security and defence, while PJC is mainly aimed at ensuring internal security and an effective fight against (various types of) crime.

At present these two matters are subject to the Treaty on European Union, respectively at Title V and Title VI. Thus, whilst awaiting the ratification and the entry into force of the Lisbon Treaty, the EU's policies on these issues are still disciplined and regulated through the so-called pillar-system. The pillar structure consists of different legislative procedures, the "Community method" used for the first pillar, and the intergovernmental cooperation applied to the CFSP/ESDP (second pillar) and the PJC (third pillar).

However, with the introduction of the Lisbon Treaty the EU will be granted legal personality (Art. 47) and the pillar structure will be abolished, with the inclusion of both the CFSP/ESDP and the PJC in a single, unique, framework subject to the Treaty on the Functioning of the European Union252 (TFEU, former Treaty Establishing the European Community).

[251] Consolidated version of the Treaty on European Union, 24-12-2002.
http://eur-lex.europa.eu/en/treaties/dat/12002M/pdf/12002M_EN.pdf
[252] Consolidated version of the Treaty on the Functioning of the European Union, 9-05-2008.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:EN:PDF

Apart from this substantial change on the legal status of the EU, the Lisbon Treaty will introduce several procedural innovations for both the CFSP/ESDP and the JPC, providing the EU with the tools to further develop its activity in the broad SECURITY domain.

In the first part of this report we will try to the major innovative provisions that will be introduced with the entry into force of the Lisbon Treaty in the CFSP/ESDP and in the JPC. In the second part we will try to estimate if some of these changes might represent potential opportunities and/or challenges for the development of the European defence and security markets.

New rules for the European security sector

The Common Foreign and Security Policy/European Security and Defence Policy

The introduction of the Lisbon Treaty won't change substantially the European decision-making process on external security and defence matters. In fact, although the new Treaty will grant the EU a legal personality, decisions would on such issues will continue to be taken by unanimity (Art. 31 and Art. 38).

What seems to be particularly relevant is that, for the first time, the Lisbon Treaty introduces in the Treaty on European Union253 a set of specific "Provisions on the Common Security and Defence Policy" (Artt. 42-46). Thus, ESDP will be renamed Common Security and Defence Policy (CSDP).

In particular, Art. 42 states that "the common security and defence policy […] shall provide the Union with an operational capacity drawing on civilian and military assets. The Union may use them on missions outside the Union for peace-keeping, conflict prevention and strengthening international security […] and shall include the progressive framing of a common Union defence policy".

Starting from these general provisions, a set of issues are implemented, better defined or newly introduced by the Treaty:

[253] Consolidated version of the Treaty on European Union as modified by the Treaty of Lisbon, 9-05-2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF

The High Representative of the Union for Foreign Affairs and Security Policy

The figure of the High Representative will be sensibly strengthened after the entry into force of the Lisbon Treaty. In fact, according with art. 18, he shall conduct both the Union's common foreign and security policy and the common security and defence policy, contributing by his proposals to the development of the EU activities in such domains. Moreover, he shall preside over the Foreign Affairs Council.

The High Representative will also have relevant responsibilities within the European Commission, since he will be one of its Vice-Presidents, in charge of ensuring the consistency of the Union's external action. Furthermore, he will be responsible for the Commission's external relations and for coordinating other aspects of the Union's external action.

European Defence Agency

The Lisbon Treaty clarifies the role of the European Defence Agency (EDA), providing it a firmer legal base than simply a Council's Joint Action. According to art. 42, the EDA (together with MS) is expressly in charge of improving the military capabilities at the EU's disposal. The Agency, indeed, […] shall contribute to identifying and, where appropriate, implementing any measure needed to strengthen the industrial and technological base of the defence sector, shall participate in defining a European capabilities and armaments policy, and shall assist the Council in evaluating the improvement of military capabilities.

Moreover, art. 45 accurately defines the EDA's objectives focused on creating a common ground for European military capabilities' assessment, procurement, implementation and production:

- to contribute to identifying the Member States' military capability objectives and evaluating observance of the capability commitments given by the Member States;
- to promote harmonisation of operational needs and adoption of effective, compatible procurement methods;
- to propose multilateral projects to fulfil the objectives in terms of military capabilities, ensure coordination of the programmes implemented by the Member States and management of specific cooperation programmes;

- to support defence technology research, and coordinate and plan joint research activities and the study of technical solutions meeting future operational needs;
- to contribute to identifying and, if necessary, implementing any useful measure for strengthening the industrial and technological base of the defence sector and for improving the effectiveness of military expenditure.

- *Permanent structured cooperation*

- The new Treaty also establishes that a permanent structured cooperation (PSC) within the EU framework could be set up by "those Member States whose military capabilities fulfil higher criteria and which have made more binding commitments to one another in this area with a view to the most demanding missions.
- Particularly relevant is the Protocol n. 10 "on Permanent Structured Cooperation Established by Art. 42"254, which better defines the objectives of such cooperation:
- to proceed more intensively to develop its defence capacities through the development of its national contributions and participation, where appropriate, in multinational forces, in the main European equipment programmes, and in the activity of the [EDA].
- to have the capacity to supply by 2010 at the latest, either at national level or as a component of multinational force groups, targeted combat units for the missions planned, structured at a tactical level as a battle group, with support elements including transport and logistics, capable of carrying out the [extended Petersberg tasks].

To achieve these ambitious goals, MS taking part in PSC will:

- cooperate, as from the entry into force of the Treaty of Lisbon, with a view to achieving approved objectives concerning the level of investment expenditure on defence equipment, and regularly review these objectives, in the light of the security environment and of the Union's international responsibilities;

[254] Protocol (No 10) on Permanent Structured Cooperation Established by Article 42 of the Treaty On European Union, 9-05-2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0201:0328:EN:PDF

- bring their defence apparatus into line with each other as far as possible, particularly by harmonising the identification of their military needs, by pooling and, where appropriate, specialising their defence means and capabilities, and by encouraging cooperation in the fields of training and logistics;
- take concrete measures to enhance the availability, interoperability, flexibility and deployability of their forces, in particular by identifying common objectives regarding the commitment of forces, including possibly reviewing their national decision-making procedures;
- work together to ensure that they take the necessary measures to make good, including through multinational approaches, and without prejudice to undertakings in this regard within the North Atlantic Treaty Organisation, the shortfalls perceived in the framework of the 'Capability Development Mechanism';
- take part, where appropriate, in the development of major joint or European equipment programmes in the framework of the European Defence Agency.

Extended set of security missions

The so-called Petersberg Task will be extended by the Treaty (Art. 43), as already done by the European Security Strategy255, and will include: joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation, even in order to enhance the fight against terrorism in third countries' own territory.

Mutual assistance clause

The Treaty's art. 42, par. 7 establishes a sort of "mutual assistance", saying that if a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of

[255] A Secure Europe in a Better World - European Security Strategy, 12-12-2002. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

the United Nations Charter. In particular, the mutual assistance clause seems to make clearly reference to military support to a MS which suffers an armed aggression on its territory.

Solidarity clause

The clause is not included in the part of the Lisbon Treaty dedicated to the "EU's External Action and Common Foreign and Security Policy", but it is part of the Treaty on the Functioning of the European Union (Art. 222). According to the clause, the Union and its Member States shall act jointly in a spirit of solidarity, [with all the instruments at its disposal, including the military resources, in order to] prevent the terrorist threat in the territory of the Member States; to protect democratic institutions and the civilian population from any terrorist attack; to assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack; to assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster. The clause mainly refers to civil protection's activity, although even police or military units may take part in the event's operational management. It cannot be invoked for anti-terrorism operations outside the EU's territory.

Enhanced cooperation

Finally, the Lisbon Treaty (Art. 20 e Art. 329) will extend the possibility to activate an enhanced cooperation also to matters with military or defence relevance. Such possibility in not currently contemplated under the provisions of the Treaty on European Union.

The Police and Judicial Cooperation in Criminal Matters (PJC)

According to the art. 4(j) of the Treaty on the Functioning of the European Union, the EU and the member states share decisional competences on the newly created area of Freedom, Security and Justice (as defined by the Title V of the Treaty on the Functioning of the European Union).

The Treaty's art. 67 provides a precise and detailed delimitation of EU' and member states' tasks and competencies on the matter. According to the article the European Union shall:

- ensure the absence of internal border controls for persons and shall frame a common policy on asylum, immigration and external border control;
- endeavour to ensure a high level of security through measures to prevent and combat crime256, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws;
- facilitate access to justice, in particular through the principle of mutual recognition of judicial and extrajudicial decisions in civil matters;
- define the strategic guidelines for legislative and operational planning within the area of freedom, security and justice.

To achieve these objectives, the Lisbon Treaty will extend the co-decision procedure (the ordinary legislative procedure, Art. 294 TFEU) to the decision-making process in the area of Freedom, Security and Justice (FSJ), strengthening the role of the European Parliament and the Commission on such matters. Indeed, FSJ policies will be generally disciplined through legal acts (regulations, directives, decisions, recommendations) although some exceptions will remain in force even under the Lisbon Treaty provisions for:

- acts adopted before the entry in force of the Lisbon Treaty which will be valid until they are not repealed, annulled or amended in the implementation of the treaties.
- legislative acts adopted under a special legislative procedure and disciplining issues on passwords, IDs, residence; family law; extension area of crimes; European Public Prosecutors' Office; operational cooperation between police, customs etc..; operations in the territory of another MS.

[256] According to art. 83, the new Treaty sensibly extends the areas of crime to: areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime

According to the Treaty, both the European Commission and the Court of Justice will have full power on these legal acts, though their institutional activity on activity will be limited by the transitional provisions set out in the TFEU and by the dispositions of art. 276 which says that in exercising its power in regarding the provisions on the FSJ, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

Together with these important institutional innovations, the Treaty of Lisbon also sets up relevant procedural changes in the area of freedom, security and justice, which might help the EU and its MS in operating more successfully to fight the various challenges emerging in the sector.

The European Public Prosecutor's Office (EPPO)

Treaty's art 86, establishes that the Council (through the special legislative procedure: unanimity after having obtained the EP's consent) may set up an European Public Prosecutor's Office (EPPO) in order to combat crimes affecting the financial interests of the Union. The EPPO shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offences against the Union's financial interests […]. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offences.

The European Council may, at the same time or subsequently, […] extend the powers of the European Public Prosecutor's Office to include serious crime having a cross-border dimension.

According to art. 85 the European Parliament and the Council, through the ordinary legislative procedure, will have the possibility to strengthen the status of Eurojust developing its structure, operation, field of action and tasks. In particular, such tasks may include:

- the initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union;
- the coordination of [the above mentioned] investigations and prosecutions;
- the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network.

Police Cooperation

According to Art. 87, the Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences. In particular the EU may establish measures concerning:

- the collection, storage, processing, analysis and exchange of relevant information;
- support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection;
- common investigative techniques in relation to the detection of serious forms of organised crime.

Moreover, the article will provide the Council with the legal base to establish (through a special legislative procedure) stronger measures concerning operational cooperation between police, customs and other specialised law enforcement services. The Treaty also foresees the possibility to establish an enhanced cooperation on such operation matters.

Europol's will be further reinforced by art. 88, which states that the agency's mission shall […] support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy. According to the Treaty's provisions, Europol's tasks may include:

- the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies;
- the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States' competent authorities or in the context of joint investigative teams, where appropriate in liaison with Eurojust.

Standing committee for internal security

As provided by art. 71, the European efforts on internal security matters will be strengthened and coordinated through the creation of a standing committee set up within the Council. The standing committee, will facilitate coordination of the action of Member States' competent authorities, and will involve also representatives of the EU bodies, offices and agencies concerned. The standing committee might become the *alter ego* of the PSC for matters related to internal security, concentrating in its hands relevant powers of political guidance and control.

Antiterrorism measures

Trying to address the emergent challenge represented by terrorism, the Treaty's art. 75 introduces some provision aimed at […] preventing and combating terrorism and related activities, enabling the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, [to] define a framework for administrative measures with regard to capital movements and payments, such as the freezing of funds, financial assets or economic gains belonging to, or owned or held by, natural or legal persons, groups or non-State entities.

Opportunities and challenges for the defence and security markets

Analyzing the institutional and procedural innovations introduced by the Lisbon Treaty, it appears clear that not all of them will directly influence the process of definition and evolution of the EU's defence and security markets. However, it can be stressed that they show an increasing incidence of the EU institutions in the management of security issues (both internal and external).

Although it is not automatic that the Treaty's provisions will directly foster the development and the effectiveness of the EU's defence and security markets, they will surely provide an enhanced framework for a common management of defence and (probably more) security issues.

If adequately supported by political will, the effect of these provisions might be double, influencing both the demand and the supply side. In particular, the demand side might be affected by those innovations which extend the EU's missions in the filed of defence and security (i.e. extension of Petersberg tasks, Art 43 TEU) or which expand the police operational cooperation, and by those which emphasize the EDA's role in identifying capability objectives and procurement methods. On the offer side, we underline the Treaty's provisions which either institutionalize the role of the EDA in the innovation and research domain, or those which establish new legal frameworks for the cooperation on equipment and on research in the field of FSJ.

Finally, concerning the possible blurring between the security and defence sectors, the Lisbon Treaty does not provide major indication about this trend, leaving the EU's situation on this matter substantially unaltered. There is one area, however, in which such convergence seems to be emerging, at least on the theoretic side: the fight against terrorism. Terrorism, in fact, is mentioned both in the provisions which discipline the Common Foreign and Security Policy (Art. 43 TEU) and the area of Freedom, Security and Justice (Art. 88 TFEU). Furthermore, also the so-called solidarity clause (Art. 222 TFEU) provides the legal instrument to MS to address the threat of terrorism. Particularly interesting is that such clause contemplates the opportunity to act with the military resources, in order to prevent the terrorist threat in the territory of the Member States, associating the typical external-use of military force to EU's internal security purposes.

The Common Foreign and Security Policy/Common Security and Defence Policy CFSP/CSDP

Opportunities

Lisbon's provisions on CFSP/CSDP might foster some virtuous developments in particular on the demand side of the defence and security market. The extension of the Petersberg tasks (humanitarian and rescue tasks; peace-keeping tasks; tasks of combat forces in crisis management, including peacemaking), which will be integrated by joint disarmament operations,

military advice and assistance missions, and conflict prevention tasks, might represent a stimulus towards the development of new military equipments and capabilities.

In particular, according to art. 43, the CSDP efforts will be aimed at contributing "to the fight against terrorism, including by supporting third countries in combating terrorism in their territories". Although the EU is already committed in similar operations, (the EUBAM Rafah border monitoring mission in Gaza, and EUPOL missions in Ramallah and in Afghanistan), those introduced by the Treaty seem to have deeper security implications for the EU's external forces. They would probably require more intelligence and counter-insurgency capabilities compared to those required by operations purely focused on monitoring and law-enforcement efforts.

Of course, without the clear political will of EU's MS to proceed towards this direction, this opportunity risks to remain a groundless, hypothetical option.

In these circumstances, the Permanent Security Cooperation (PSC) might provide a permanent framework to those MS which have made more binding commitments to one another with a view to the most demanding missions. Such framework would offer MS the possibility to focus on these missions, and most important, to create an institutional architecture where issues on defence capabilities, military expenditures and requirements harmonization will be addressed through a cooperative approach. At least in theory, this joint activity would facilitate the emergence of common input (or partially common, according to the number of MS participating to the PSC) in the defence/security market demand.

The European Defence Agency might play a relevant role in facilitating these developments: the Treaty officially institutionalizes the Agency, while its role in this field is also emphasized by the Protocol 10. On the demand side, indeed, the EDA is the "natural partner" for those countries wishing to strengthen their military institutional and operational cooperation on defence and security matters. The Agency might help MS involved in PSC in identifying and fulfilling their military/security capability objectives through compatible procurement methods and multilateral projects (i.e. joint elaboration of European Equipment Programmes).

The institutionalization of the Agency's activities might have some relevance also on the supply side, in particular thanks to art. 45 provisions concerning the support of the defence technology

research and on the enforcement of the industrial and technological base (as already defined in the Council Joint Action 2004/551/CFSP).

Challenges

However, the dual relevance of the EDA both on the demand and the supply side might represent a risk and a challenge for the proper functioning of the defence and security market. In fact, since the Lisbon Treaty does not resolve relevant competence institutional disputes on the issue of defence market integration, it risks to amplify a useless and confusing duplication of roles within the EU framework.

Indeed, being the EDA involved both in demand and supply dynamics, its activity risks to create contrast and competition with the European Commission, among whose responsibilities we find the enhancement of the competitiveness and the internal EU trade, the strengthening of the industrial and research policy, and the promotion of standardization and intra-community transfers, both in the military and civilian sector.

To work properly towards the common objective of an integrated European defence and security market, those institutions (together with the other EU and national bodies involved in the sector) will have to use the provisions introduced by the Lisbon Treaty to clarify their competences and to well define their roles in the two different components (supply and demand) of the market. An overlap of competencies and an intra-institutional competition would heavily threaten the development of an efficient market.

The area of Freedom, Security and Justice

Opportunities

The Treaty's discipline of FSJ does not provide clear and manifest opportunities for the enforcement of the EU's internal security market; however, subjecting the matter to the so-called ordinary legislative procedure might be seen as a first relevant step of the EU towards a common management of security and its respective industrial market.

On the supply side, the establishment of deeper cooperation (exchanges of staff and equipment) between MS's police, customs and other specialised law enforcement services, and the extension of the areas of crime subject to the FSJ according to art. 83, might provide significant incentives for the standardization of requirements and the identification of new emerging need, in order to develop common police and security capabilities. For instance, "the collection, storage, processing, analysis and exchange of relevant information" between members states presuppose that national authorities rely upon common, or at least interoperable, tools to manage these activities; if not, standardization and harmonization efforts would be required in order to reach such objectives.

Of course, to start such dynamics, it is required the leading role of an EU body which might gather, coordinate and reprocess all the inputs offered by MS's joint activities. A body able to promote efficiently joint programmes and to set common needs, more or less in the same way the EDA does in the military sector. Unfortunately, the Treaty does not contain explicit provisions which create (or transform) an EU body in order to provide these functions and services and to achieve these goals.

Although the Treaty aims at strengthening the mission of Europol, the provisions contained in art. 88, will not be enough to transform the body in a leading institution for the development of common security requirements and for the definition of an integrated EU public procurement in the sector. However, the Treaty's provisions, together with the 2008-decision to confer EU agency status on Europol, might shed some light to further significant developments in this sense.

Furthermore, after the introduction of the Treaty, it will be necessary to define the competencies and to determine the role of the Standing committee for internal security within the EU institutional framework. If the Standing committee would become the respective of PSC for JFS matters, there is the possibility that it would take some responsibilities also in the political direction of the development of internal security capabilities.

Challenges

On the demand side, inactivity represents the main challenge for the definition and evolution of the EU's internal security market; indeed, since the Treaty does not contain specific measures on

this issue, it would be difficult to identify the competent organism in charge of coordinating MS in setting up and harmonizing operational and technical requirements. This situation would be accentuated by the fact that the security market is more “off-the-self”-based compared to the defence market; this characteristic generally tempts security end-users to reduce their coordination efforts towards the definition of common requirements, taking their decision more on price-based calculations.

Towards blurring?

Although not providing specific provisions on the matter, the Lisbon Treaty offers some interesting stimulus for reflection over the possibility of an increasing blurring of lines between the external and internal security.

The most relevant change will be represented by the new role of the High Representative of the Union for Foreign Affairs and Security Policy, who will cover crucial positions in the two main institutional promoter of the EU’s R&T activities in the security domain. Since the High Representative will be concurrently the Head of the European Defence Agency and Chief of the EDA’s Steering Board, the Vice-President of the Commission with competencies in the management of the Union's external action, he might have a pivotal role in the setting of the EU’s external agenda, including the definition of a broader (simultaneously military and civilian) approach towards the European security and its reference market.

The solidarity clause, introduced by art. 222, which prefigures the possibility for both the EU and MS to intervene, even with military resources, in the territory of the MS who requests assistance. What seems particularly relevant is that article introduces the possibility using military resources, the typical tool to guarantee State’s external security, in the internal security domain (to prevent the internal terrorist threat; to protect democratic institutions and the civilian population; to assist a Member State in its territory). The clause, sensibly extending (at least theoretically) the use of military force in the internal sphere at the EU level, emphasizes the growing interdependence between defence and security sectors.

The operational characteristics of the three CFSP/CSDP new tasks introduced by art. 43, joint disarmament operations, military advice and assistance missions, and conflict prevention tasks,

require deeper integration of defence and security forces and means involved in the EU's external efforts.

Finally, terrorism is emerging as key threat to be addressed by the EU in its internal domain as well as in its external efforts. Provisions on the fight against terrorism are included both in the part which discipline the CFSP/CSDP and in the part which deal with FSJ. Typical defence forces like militaries, and internal security actors like police, will be increasingly involved in common efforts against the terrorist menace, presupposing a clear convergence of technical and operational requirements.

Annex 4. EOS, ESD and ESRIF membership

EOS			ESD			ESRIF		
NAME	**SIZE**	**TYPE**	**NAME**	**SIZE**	**TYPE**	**NAME**	**SIZE**	**TYPE**
Alcatel Lucent	**L**	**CIV, SEC** – IT	FN Herstal	**L**	**SEC, DEF**, small arms	Barco Corporate Research	**L**	**CIV SEC**
Amper	**L**	**SEC, DEF** – communications	Alpes Lasers	**S**	**CIV, SEC, DEF**	EADS	**L**	**CIV, DEF, SEC**- aeronautics
Atos Origin	**L**	**SEC,** IT	Amper HLS	**L**	**SEC DEF**, communications	Finmeccanica	**L**	**DEF SEC** aerospace
Avio	**L**	**DEF SEC** aerospace	Astrium	**L**	**CIV, SEC, DEF**	FREQUENTIS	**L**	**CIV DEF SEC** communications
BAe Systems	**L**	**DEF**	Bosch Security systems	**L**	**SEC**	KÜRT Corp. Information Managment	**M**	**CIV, SEC, DEF**
Bumar	**L**	**DEF, SEC**	CEIS	**M**	**SEC**	Petards Group plc	**L**	IT **SEC**
COTECNA	**L**	**SEC** - risk assessment	COTECNA	**L**	**SEC** –risk assessment	Saab AB	**L**	**DEF SEC** aeronautics
Diehl	**L**	**DEF, CIV, SEC**	CS	**L**	**DEF, SEC**	Sagem Défense et Sécurité	**L**	**DEF, SEC**, Sensors, Aeronautics
EADS	**L**	**CIV, DEF, SEC**- aeronautics	Crossmatch Technologies	**M**	**SEC** - biometrics	Smiths Group plc	**L**	**SEC**
Engineering	**L**	**CIV, SEC – IT**	Dhiel	**L**	**DEF, SEC**	Thales Security Solutions & Services Division	**L**	**SEC**
Edisoft	**S**	**DEF, CIV, SEC**	EADS Defence and Security	**L**	**DEF, SEC**			
G4S	**L**	**SEC,** services	Edisoft	**S**	**SEC DEF**			
Hai	**M**	**CIV, SEC, DEF**	Emcco	**S**	**SEC**			

IBM	**L**	**CIV, SEC** – IT	ESG	**L**	**SEC**			
Indra	**L**	**CIV, SEC** – IT	Finmeccanica	**L**	**DEF, SEC, CIV**			
Iveco	**L**	**CIV, DEF, SEC** – vehicles	INDRA	**L**	**CIV, SEC** – IT			
Sagem Sécurité	**L**	**SEC, DEF -** Sensors, Aeronautics	Ineo	**L**	**SEC, DEF**			
Selex SI	**L**	**DEF, SEC –** sensors, electronics	Martec	**M**	**SEC**			
Siemens	**L**	**CIV, SEC –** IT	Nanotech	**S**	**SEC**			
Smiths detection	**L**	**SEC -** IT, electronics, sensors	Plath	**L**	**SEC**			
SAAB	**L**	**DEF –** Aeronautics	PyroAlliance	**M**	**CIV, SEC**			
Teletron	**S**	**SEC**	Sagem Sécurité	**L**	**SEC, DEF -** Sensors, Aeronautics			
Thales	**L**	**DEF, SEC, CIV**	SAP	**L**	**SEC -** IT			
			SECUNET	**M**	**SEC -** IT			
			SmartQuantum	**?**	**SEC -** crypto			
			Thales	**L**	**DEF, SEC, CIV**			
			Thales Alenia Space	**L**	**DEF, SEC, CIV**			
			VCS	**M**	**CIV, SEC**			

Annex 5. Country studies

Annex 5.1. Blurring between security and defence in France

1. Conceptual change in France

1.1 The current situation

In France, it is not easy to deal with the concept of "security". The main strategic documents have avoided discussing this issue for a long time.

The notion of "national defence" gradually appeared at the end of the 19th century. Originally, it was exclusively related to the military realm. The ordinance of January 7th, 1959, which dealt for the first time with the general organisation of defence, provides a broad definition of "defence": "Defence aims to ensure at all times, under any circumstances, and against any form of aggression, the security and the integrity of the territory as well as the life of the population".[257] Consequently, defence has been permanent (i.e. not related solely to wartime) and global (i.e. including all military and non-military aspects of the protection of the nation against aggression).

However, as a result of institutional practices, rivalries between the President of the Republic and the Prime Minister led to a confusion of roles whereas the rivalries between the Minister of Defence[258] and the Minister of Interior, both proud and protective of their prerogatives, led to a clear dividing line between defence and security.[259] Both rivalries prevented a real evolution in the realm of security. National defence was still primarily related to military matters: from 1959 to the end of the Cold War, priority was given to the development of military tools (i.e. conventional and nuclear armed forces, military reserves, and armed forces).

[257] Ordinance of January 7th, 1959, dealing with with defence's general organization, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006069248&dateTexte=20090413

[258] In 1969, France substituted the "Minitry of Armies" by the "Ministry of National Defence".

[259] In this respect, personalities of ministers matter a lot.

During this period, "defence" and "security" were clearly distinct. Defence was an action to contain a threat or protect against a threat, while security was the condition of feeling secure (thus involving long-term prevention).

As a result, the 1972 and 1994 White Papers on Defence barely mentioned security. Security was not an issue *per se*. The idea of a defence/security continuum had been discussed during the drafting of the 1994 White Paper, but it was not adopted in the final document.
In 1972, the first White Paper was obviously marked by the Cold War context and thus laid out an "all-deterrence" approach.
The second one, in 1994, drew lessons from the end of the Cold War, as well as from Desert Storm and Balkans' operations. It insisted on the importance of projecting force and was followed in 1996 by the end of national mandatory military service and the professionalization of the French armed forces, one of the deepest reforms that France has undertaken in recent years. In this first strategic document following the end of the Cold War, security was seen as one of many elements constituting "global defence".

In 1994, the notion of defence was influenced by the end of the Cold War. As a result, the 1994 White Paper was characterized by:

- An emphasis on external threats – the main risk being "regional conflicts".[260]
- The definition of the first objective of defence as the protection of French interests.
- The existence of increasing vulnerabilities due to a diversification of risks and the rise of uncertainty.
- Internal and external security became increasingly linked to each other, requiring the definition of a comprehensive defence approach, i.e. "global defence".

This 1994 White Paper acknowledged that purely military logic was becoming progressively less relevant in the post-Cold War context. However, non-military threats were not seen as security issues but as defence ones: "Certain forms of aggression, such as terrorism, or some consequences of drug trafficking have taken on such dimensions that they could threaten the country's security

[260] 1994 French White Paper on Defence, p.22, http://lesrapports.ladocumentationfrancaise.fr/BRP/944048700/0000.pdf.

or integrity, the life of its population or impede the fulfilment of international commitments. Therefore, they are included in the defence approach, as defined by Article 1 of the Ordinance of January 7th, 1959".[261]

In 2007, a consensus was reached concerning the need for a new strategic document, as France needed to adapt to the new international and strategic environment. The White Paper Commission chaired by Jean-Claude Mallet, who was in charge of the drafting of the 2008 White Paper, discussed the expansion of the security spectrum, culminating in the notion of national security. As a result, "security" has become the main issue of the 2008 White Paper.
While the 1972 and 1994 White Papers only addressed the defence realm, the new White Paper on Defence and National Security (released in June 2008) outlines a comprehensive strategy for dealing with existential threats and risks to the nation in a globalised world.
Defence and security are described as a common field cut in two: Two separate worlds exist, but they share common interfaces. The border between the two notions is blurred.

If this new document acknowledges the importance of addressing the security realm, it does not give a definition of what security means. In addition, it has raised some fears – especially in the industry sector – that eventually, the security sector will be swallowed up the defence sector[262].

1.2 Factors driving blurring of boundaries

According to the 2008 White Paper, the main factor driving blurring of boundaries between defence and security depends on the new international and strategic environment. This document acknowledges that, given the interdependent nature of threats and the increasing interaction between internal and external security, it is also necessary to integrate the areas of defence, domestic security, foreign policy, and the economy in an overarching strategy. This document is a reform that comes after 9/11 and responds to the strategic challenges and the new threats from globalisation, interdependencies and uncertainty. Strictly speaking, it goes beyond defence policy and defines France's first formal national security strategy.

[261] 1994 French White Paper on Defence, p. 17.
[262] Interview with French stakeholders.

The new strategy builds upon five basic strategic functions to achieve overall national security; namely knowledge and anticipation, prevention, deterrence, protection, and intervention. These five functions cover both external and internal security, as well as military and civilian resources, thereby reflecting the comprehensive approach of the strategy.[263]

This new White Paper is characterized by:

- The emergence of the "national security" concept that "combines, without merging, defence policy, homeland security policy, foreign policy and economic policy".[264]
- The continuity between internal and external security.[265]
- The redefinition of the conditions of national and international security, the modification of the role of military tools.[266]
- The preservation of French military and strategic power as well as ensuring the independence and protection of the country as the new objectives of French defence and security.[267]
- The calling for further development of a European defence policy, urging a strengthening of the EU's capacity for independent military action and "the search for a new balance between Americans and Europeans within NATO".[268]

On this basis, the new National Security Strategy developed in the 2008 White Paper is introduced as a strategy "defined in order to provide responses to all the risks and threats which could endanger the life of the Nation". This innovation is considered as enabling French authorities to tackle both risks and threats by setting up a global approach through military and non-military means, as well as internal and external tools.

---

[263] Four of these five strategic functions were already in the 1994 White Paper. The new "Knowledge and Anticipation" function is not only recognized as a stand-alone strategic function; it is also at the heart of the White Paper.
[264] 2008 French White Paper on Defence and National Security, p. 10, http://lesrapports.ladocumentationfrancaise.fr/BRP/084000341/0000.pdf.
[265] 2008 French White Paper on Defence and National Security, p. 57.
[266] Ibid, p. 13.
[267] Ibid, p. 7.
[268] 2008 French White Paper on defence and national security Press kit, http://www.defense.gouv.fr/content/download/128605/1125557/version/1/file/LB+pr%C3%A9sentation+en+anglais++white_paper_press_kit.pdf

Terrorism is identified as the largest threat, while, more generally, non-conventional threats are increasingly significant. For example, "major attacks against information systems are a rising concern, as the combined consequence of the rapidly growing role of cyberspace in societal, economic and security terms, and of the adoption of aggressive cyber-attack techniques and postures by state and non-state actors".[269]

Some scholars prefer another approach to defence and security: that of defence and security representing two different fields that can share a common area.

According to this approach, defence would include:

- Military and operational activities
- Intelligence, prevention, surveillance
- Fight against terrorism

Security would include:

- Public order, individuals and goods security
- Economic security
- Intelligence
- Fight against terrorism

According to this analysis, defence and security overlap with respect to intelligence and terrorism.[270] Some French scholars have tended to refer to this overlapping area as a "national security" area – even if it remains unclear what "national security" actually means.

1.3 Factors constraining blurring of boundaries

The 2008 White Paper has two shortcomings though:

- It includes several of issues under the "national security" conceptual umbrella
- It is not very precise concerning the boundary of national security

The idea that external and internal security is narrowly interwoven is commonly accepted. But its implementation remains limited. "National defence" was already a broader concept than *stricto*

[269] 2008 French White Paper on defence and national security Press kit.
[270] Interview with French stakeholders.

sensu military operations or territorial defence. But the global perspective adopted by the 2008 White Paper goes further towards developing an integrated approach of both dimensions.

In some respects, this could lead to excesses and abuses; that is to say the inclusion in the concept of national security of everything that is related to "security" (from anti-terrorism to closed-circuit television or public order). The White Paper does not fully succeed in addressing fears of a militarization of domestic security issues, confirming that there is nothing wrong with military personnel taking part in counter-terrorism activities on national territory. There have also been fears about a protective posture and criticism regarding the "resilience" concept as a symptom of an anxiety-producing world vision.

However, French officials emphasize the relevance of the resilience concept which ensures the continuity of the institutional, economic and social activities.

2. Organizational issues in France

2.1 The current situation

The disappearance of the border between defence and security only began recently. In France, the defence sector only involves one customer: the Ministry of Defence (MoD). As the sole actor on the demand-side, the MoD controls, either directly or indirectly, all the aspects of the industry, including research policy, managing of defence programmes, procurement of equipment and industrial policy[271]. On the other hand, the security sector is made up of a much more diverse range of institutions, agencies and companies, spanning both public and private sectors. The security market is very heterogeneous and unstructured, mainly led by suppliers, whereas the defence market is very structured – products are for one customer and dedicated to one sector. The defence market is a demand market, since customers (MoDs) are the base of this market.

Since 1994, some have advocated that the White Paper on defence has taken into account evolutions that have led to the progressive disappearance of the border between external security and internal security, and thus between defence and national security. Particularly in France,

[271] See: "Plan prospectif à 30 ans" (MoD, June 2005) and "Politiques et Objectifs Scientifiques" (DGA, MoD, 2008)

terrorism was already a reality with the 1986 attacks of Iranian origin. The "*Groupe Islamique Armé"* (GIA) did not wait long before striking in 1995. Despite everything, the 1994 White Paper did not address this evolution, even though terrorism was identified as a threat.
On the other hand, the 2008 White Paper on Defence and National Security has confirmed the disappearance of the border between external security and interior security thereby yielding the concept of national security. This evolution can be qualified as overdue and accounts for the late reform of the administrative organization of defence and security in France.

The 2008 White Paper on Defence and National Security must be considered within a broader framework. It confirms the reform movement initiated by President Nicolas Sarkozy that aims at reforming the French political system as such. In the areas of security and defence, it is seamlessly interwovened with the *Loi de Programmation militaire 2009–2014*, adopted by the government in October 2008 and passed in June in the French Parliament, the reform of the Ordinance of 1959, France's return to NATO as well as the strengthening of the Parliament and the confirmation of the major role of the President in such areas (at the expense of the Prime Minister).

2.2 Factors driving blurring of boundaries

The implementation of the 2008 White Paper on Defence and National Security is leading to many structural reforms:

- The reform of the 1959 ordinance dealing with the defence organization. This 1959 ordinance is now going to address defence and national security, according to this new strategy.
- The reorganisation of the SGDN (Secretariat-General for National Defence): its name has changed (becoming Secretariat-General for National **Security** and Defence, SGDSN)[272]. It is still under the supervision of the Prime Minister but is now closely working with the President of the Republic. It will expand its inter-governmental mission. It is aimed at coordinating the governmental national security and defence plans and at insuring the

[272] Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale,
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021533568&dateTexte=&categorieLien=id

setting up of the French national security strategy, especially during crises. The SGDSN is divided into two departments: State protection and security, and, International, scientific and technological affairs. By defining a national security strategy that goes beyond the defence strategy, the President is strengthened in his defence and security prerogatives.

- The Defence and National Security Council (Conseil de Défense et de Sécurité National, CDSN) chaired by the President of the Republic has been created.[273] This council is aimed at dealing with military programming, deterrence, military planning, crisis management, intelligence, economic security, energy security and domestic security (when related to national security and fight against terrorism). This Council gathers the President of the Republic, the Prime Minister, the Minister of Defence, the Minister of Interior, the Minister of Economy, the Minister of Budget and the Minister of Foreign affairs. The everyday work will be provided by the SGDSN. This is a consequence of the adoption of the strategy that makes national security the federating and mobilising objective of government action. "Its field of competence includes all the public policy issues involved in the areas of defence and national security where the President of the Republic's powers are defined in the Constitution."[274] The Prime minister will manage the implementation of the decisions taken by the CDSN.
- The National Intelligence Council (CNR)[275], chaired by the President, is one of the major bodies of the CDSN. It will substitute the CIR (Interministeral Intelligence Committee), which was chaired by the Prime Minister, and will have broader functions. It is aimed at "setting forth the major orientations assigned to the Intelligence services (strategies and priorities), conduct planning for human and technical resources, and examine the evolution of the legal framework governing intelligence operations."[276] It is meant to ensure better co-ordination between the various intelligence services.

[273] Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021533568&dateTexte=&categorieLien=id

[274] French White Paper on Defence and National Security, Press kit.

[275] Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021533568&dateTexte=&categorieLien=id

[276] French White Paper on Defence and National Security, Press kit,

- The designation of a National Intelligence Coordinator reporting to the President[277]: he is the point of contact for the domestic and foreign intelligence services with the President of the Republic. He supervises the planning of the intelligence objectives and assets and their implementation.

These reforms following the release of the 2008 White Paper highlight the blurring of borders between defence and security, as well as the "presidentialisation" of the defence and national security areas. In adopting a broad conception of "national security" that includes defence against external threats as well as homeland security management, the French White Paper contributes to the process of blurry borders.

Another substantive and significant reform has been the transfer of the Gendarmerie, whose responsibilities combine defence, security and judiciary police missions, from the Ministry of Defence to the Ministry of Interior. Since 2005 Nicolas Sarkozy, then Minister of Interior, has advocated for the incorporation of the Gendarmerie into his ministry. Yet it is Michele Alliot-Marie, current Minister of the Interior and former Minister of Defence in 2005 when she opposed this merger, who has led this reform in 2009. Thus, since January 1st, 2009, the French Gendarmerie has been under the supervision of the Ministry of Interior – even if this body remains a military institution. This shows the evolution as regards defence and security.

Meanwhile, the *Loi Organique relative aux lois de finances* (LOLF, the French budget reform), in introducing a new budgetary structuring based on missions and performance, had identified the security mission that was shared between the Ministry of Defence and the Ministry of the Interior. This reform of budgetary order that was implemented in 2005 constituted a first breach of the tight border between defence and security.

Another example of the disappearance of the blurry of boundaries is in the Ministry of Defence itself: the *Direction Générale de l'Armement* (DGA), the procurement agency within the MoD and

[277] Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021533568&dateTexte=&categorieLien=id

the *Agence Nationale pour la Recherche* (ANR, the national agency for research) are conducting research on national security issues. Both are public administrative institutions and clear links exist between the defence research planning in DGA and the ANR.

2.3 Factors constraining blurring of boundaries

According to the French Constitution of the Fifth Republic (1958), "The Prime Minister […] shall be responsible for national defence", while "the President of the Republic shall be Commander-in-Chief of the Armed Forces. He shall preside over the higher national defence councils and committees". The Constitution makes the distinction between the prerogatives asserted by the Prime Minister in terms of national defence and the prerogatives directly asserted by the President.

Moreover, some areas will remain clearly separated. For instance, in the public research and strategic thinking area, the IHEDN (Higher Institute for National Defence) and the CHEAr (Centre for Higher Armament Studies) are being merged to create a single defence research centre. At the same time, the IERSE (Institute for the Study and Research on Corporate Security) and the INHES (National Institute for Higher Studies in Security) are being merged in order to create a "domestic security" research centre. However, the *Conseil supérieur de la formation et de la recherche stratégique* (CSFRS)[278] has been created in November 2009[279] in order to supervise those two new bodies, coordinate the study of threats and risks France and Europe will be facing in the future and define new strategic views based on the concept of comprehensive security, integrating national defence, public security, corporate protection and environmental security[280].

Besides, despite reforms, blurring of boundaries between defence and security is far from being a homogeneous trend. First, the institutional fragmentation has not disappeared (mainly due to bureaucratic and cultural issues) and is preventing a complete blurring of boundaries between

[278] *High Council for Strategic Research and Training*, suggested by a report from a working group chaired by Alain Bauer, President of the National Crime Monitoring Centre, http://lesrapports.ladocumentationfrancaise.fr/BRP/084000174/0000.pdf

[279] Avis relatif à une décision portant approbation de la convention constitutive du groupement d'intérêt public dénommé « Conseil supérieur de la formation et de la recherche stratégiques », JORF n°0266 du 17 novembre 2009, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021277599

[280] Interview with Pierre-Antoine Malfait, INHES, March 17th, 2009.

defence and security. Second, resistances may arise, mainly for budgetary, cultural and organisational reasons. Within the Ministry of Defence, the DGA and the military staff are worried about the fact that the blurring of borders between defence and security will lead to the reducing of the budget available for defence missions, especially for defence technology and defence capabilities.

3. Technological Developments

3.1 Current situation

According to French stakeholders interviewed for this study, technological products having common application in security and defence do exist, but they are still limited.
Yet one still wonders whether it is possible to claim that technological development is a driving force behind the blurring of the lines dividing security and defence. From a general point of view, there is no unanimity on this point in France.

> According to some French industrial stakeholders, the entire defence industry is, in a sense, historically dual-use oriented as a result of technological development. The idea of a technological development that blurs borders between security and defence would thus be artificial. For instance, the aeronautical or the space industries have always had a dual-use vocation.

At the same time, other French stakeholders consider that technological developments lead to a major utilisation of “civilian” technologies for defence purposes; an affirmation that would strengthen the idea of blurred borders between security and defence. As of the example of telecommunication networks’ protection against hackers, more and more civilian technologies are being used. The civilian offer seems easier to use, faster to develop (military programmes being developed over longer periods) and less expensive. Another example relates to the observation of the earth. Different systems exist for intelligence and civilian purposes, but the technology that is implemented is the same. The mission is different, but the technology is the same. In France, the

driving force for the creation of a real security market was a statement from former Ministry of Defence Michelle Alliot-Marie, stating that France's security system needed to "move from a man-based security to a technology-based security". A system such as Spot Images, which was originally a civilian technology used in the security sector, is more and more used in the defence sector.

Finally, some other stakeholders state that there are no obvious ties between defence products and security products, because missions and technologies are different. Basically, Thales asserts that about 80% of technologies are not common. In this regard, the blurring between defence and security is very small: it is mostly related to IT, maritime security and supply security. For instance, there is no commonality between a UAV used in Afghanistan and a UAV used for urban or suburban purposes. Needs, threats, costs and fields (mountains in one case, cities in another case) are different[281]. UAVs used for security missions do not require the same secure communication as UAVs used for military missions[282]. For a UAV used in Afghanistan, communication is subject to military standards (NATO) whereas in urban purposes, standards are those of security forces. As the threat is different, standards are different: standards of security forces are less sophisticated. NATO standards, on the other, are very secure and very costly as well.

However, other industrials think that the blurry border can be wider. Just to give an example, some manufacturers think that the market will be divided between UAV respecting the specifications of the MTCR regime, and by consequence really difficult to export, and others that will be developed with less stringent criteria, but having an utilisation also on the security market and being exportable without particular problems. The defence operational requirement of MALE UAV under the specifications of the MTCR regime is limited in number. But there is a huge defence and security market for MALE UAV with less stringent specifications than the ones of the MTCR regime for border security but also for intelligence, for instance to be used during an operation of the Petersberg type. This is why the IAI Israeli industry developed the Heron UAV. Even if the communication system is not the same, there will be a large communality between a security and a defence UAV in this spectrum of UAV.

[281] Interview with an industrial stakeholder
[282] 300Kg payloads and 500km range

Despite the differences of approach between stakeholders, everyone agrees that some areas in which dual-use technologies are used today in France have tendencies to grow. This is the case for counter-terrorism technologies, which are being used more and more for police intelligence purposes. Another example is the development of detection technologies in airports and other "civilian" institutions, or surveillance technologies (the problem of container and ship detection seems to be a key issue for the next ten years, especially according to the fact that the maritime surveillance market is expected to develop massively due to the Long Range Identification & Tracking Agreement). Finally, a particular role in the development of dual-use technologies seems to be being played by the telecommunication industry via cryptology and detection instruments for security and defence purposes.

3.2 Factors driving blurring of boundaries

Four drivers emerged during interviews with French stakeholders:

The first driver is politically related and oriented. The French State is more and more inclined to develop security/defence programmes. A document from the DGA[283] shows that R&T programmes have both security and defence applications. For instance, the DGA is planning to develop R&T on the following sectors:

- Information Engineering (transport of information, analysis of information, modelling, command of systems)
- Waves (detection, imagery, detection, laser…)

All these sectors develop technologies that can be used for both defence and security purposes.

One of the reasons of this new orientation – second driver – relies on financial issues. One of the obligations of the national administration is to obtain the best value for its money. If a defence or civilian technology can be used for both purposes, they have the obligation to try to take advantage of potential synergies.

However, the idea of a security budget increasing and supporting the defence one is a misconception. The security budget is growing, but at a slow pace. The security area lacks a

[283] Politique et Objectifs Scientifiques, DGA, Edition 2008

planning process similar to that of the defence sector, which also considers R&T, R&D, and the launch of large-scale programmes.

French stakeholders generally believe that the domain of "exclusively defence-related technologies" will be reduced in the next few years. The two drivers of such a trend are both economical and technical. From an economic point of view, the civilian security market is much larger than the defence market, and is growing faster in terms of complexity as well as in terms of economic development. From a technical point of view, civilian technologies have become progressively more complex, and are today in some cases more complex than defence technology. In the field of nanotechnologies, for instance, the telecommunications industry has gained extensive experience on account of mobile phone processing.

If we limit our analysis of technological developments to the French case, two documents offer a clear vision of French policy in the area of R&T and R&D, as related to security and defence: the 2008 White Paper on Defence and National Security (Chapter 16) and the new "*Loi de Programmation militaire 2009-2014*".

This orientation includes the following:

- The French priority in the sector of defence and security research is the space sector, in order to prepare future programmes in the field of telecommunications, observation, and surveillance. This priority is linked directly to the decision to give pre-eminence to the strategic function "*knowledge and anticipation*".
- Security and defence research should be pooled. An inter-ministerial coordination structure will be created in order to achieve this goal. At the organisational level, capacity to drive the R&T process will be strengthened within the Ministry of Defence (MoD) and within the Ministry of Interior (MoI). The MoI will communicate with all of the security sector actors (security operators, "gendarmerie", MoD, industry) within the "*conseil économique et scientifique de la sécurité*". Pooling will also give value to civilian research in the development of security and defence programmes. Generally speaking, the French White Paper notes that 60% of defence research benefits the civil market, while only 20% of the security research benefits the defence

market[284]. The idea is to increase the synergies between those two fields to avoid overlapping and improve interoperability.

- Sustaining small and medium enterprises is also a priority for the new French White Paper. The idea is to facilitate their access to the defence market.
- Finally, the French White Paper calls for a leading role of the European Defence Agency and the European Commission. Both institutions should cooperate in order to better coordinate R&T efforts in the security and defence areas.
- Some leading technologies on the horizon (2020-2030) are also identified: robots, artificial intelligence, new materials for force protection, new detection technologies, lasers, and bio and nanotechnologies[285].

French strategy implies and demands an ambitious European policy in the research field as well as the maximisation of benefits derived from dual-use technologies, in order to reduce costs and maximise technological development.

French policymakers emphasise the need to reorient the defence budget in order to maximise investment resources. The development of global partnerships with the defence industry is indicated as a potential source for strengthening French and European DTIB. The progress of French and European exports is also indicated as a goal of the French strategy, and implies increased influence due to a major role in the standardisation process.

3.3 Factors constraining blurring of boundaries

If there was a blurring between defence and security technologies, industrials would definitely know it and take advantage of it, as it could allow them to reduce the costs of R&D. However, this is not the case.

[284] 2008 White Paper on defence and national security, page 270.
[285] 2008 White Paper on defence and national security, page 271

There must be an evolution of the demand side to favour the continuum, but the objective is often to save money. But this is a political choice: it would mean that savings are more important than the threat.

For instance, in order to save money and to use the same product for defence and security missions, armed forces should use the same SUVs as security forces. Those cars would be cheaper, but would not protect soldiers as much as military cars. But this is not an option today: for military staffs, soldiers protection come first, as we can see in Afghanistan, where the French MoD launched several Urgent Operational Requirement (UOR) in the area of armoured trucks and vehicles specifically conceived for defence missions, and largely protected. Those kinds of vehicles would be totally useless in the typical security missions. If states want to use the same cars as security forces, policymakers have to take responsibility for making this choice.

Another constraint relates to the economical model of defence and security. In the security sector, the economical model is different, and in some sense still undefined. In the model of the 7th FP, the financing is limited to 50%, with a subvention system, and the idea of commercializing a product remains undefined. Moreover, a national demand still does not exist. The example of the border surveillance system sold by EADS to Saudi Arabia shows that, while in the defence market the purchasing of a system by the country of the manufacturer is a good argument for export, companies working in the security sector cannot use this argument. National markets for security products still do not exist. Some French industrial stakeholders also stated that even if they agree to the economical model of the 7th FP, with some reservations though, they do not want to have the same economical model for the defence research. They consider that public institutions have to fully finance the defence research as there is no private market. As a result, even at this level, the blurring of borders between defence and security is limited to few technologies or capabilities.

4. Industrial and market developments in France

4.1 Current situation

Do the French defence or security industries reorganize itself in order to respond to the blurry of

borders? The response seems to be complex, but there are no clear sign of this reorganization.

While EADS for instance has an integrated Defence and Security Divisions and one of its asserted strategic priorities is to develop its security activities worldwide, the reality seems slightly different. Under the acceptance of “defence and security division”, 5 controlled companies act in a heterogeneous way, some of them, like the missile manufacturer MBDA or the Eurofighter company, have absolutely no link with the security area. The company Defence and Communication systems seems to be the only one acting in the blurred area, by developing radio devices and communication systems to be used for border and maritime surveillance. Meanwhile, the fact that the division, “Defence and Communication,” account only for 1.4 €billion on a global turnover of 44 billion euro has to be considered.

The Safran group is a world leader in biometric technologies for fingerprint, iris and face recognition, and a major player in smart cards, identity management solutions, and access management and transaction security. The Safran leadership in this sector comes naturally by the presence of the activities of the former Sagem in the group. Meanwhile, for the first time, Safran decided to merge its activities in the defence and security area, showing a willingness to exploit the blurring of borders between those two sectors. But a few months later, the defence and security units were divided, facing the reality of the persistency of two different markets.

More important, French media related some rumours, during December 2009, concerning a large deal between Safran and Thales. Safran would acquire Thales security activity, in exchange for its defence activities to be sold to Thales. If this agreement is concretised, Thales would be a defence only player, while Safran would become the larger national security player. This would also imply that neither society believes in the future of the blurry

The growing importance of security equipments in the fields of surveillance, detection, and reconnaissance has pushed defence industries to develop a “security” business area. This is the case of Thales for instance. Still, as we can see, French companies prefer to maintain the division between defence and security. According to officials interviewed for this study, “defence” and “security” customers and products are still too different to be merged. Nevertheless, the current trend is to try to follow the development of the security market. At the same time, the fragmentation of the demand is indicated by defence industry as a source of complication. For a defence players, used to act with a sole customer, financing all the activities by the research to the

maintenance, with a risk degree close to zero, to adapt and finance new activities in an heterogeneous sector like the security one is still something complicate.
Nevertheless, French industries operating in the defence field become increasingly interested in the security area for different reasons:

1) The defence budget crunch and the security market growth enable defence manufacturer business models to try to enlarge their order book and boost their business environment;
2) Security and defence products may have common technologies or devices, and the application of dual-use technologies is a driver for savings;
3) Eventually, the involvement of the European Commission and the potential for a larger European role in the field of security research and the procurement of security equipment is a good reason to support this area, also if the 7th FP is widely criticised for its complexity, and for the lack of a "product based" approach.

If defence players invest in the security market, the reason seems to be searched in the assumption that they shouldn't miss a market seeming to have a promising future

Moreover, the growing need for security could mean the development of larger programmes that are not affordable at the national level, as can be seen today with the Galileo programme. This could make it easier to develop large European programmes in the field of defence and security.

However, the importance of the security portfolio of larger groups, such as EADS or Thales, remains marginal (1.4 billion euro on 44 for EADS, 3 billion euro on 12 for Thales). Yet we can attest of a growing interest from such important actors within those small and medium enterprises involved in the security business, which could potentially lead to absorption of security actors by European conglomerates.

Are the French defence and security markets becoming blurred? Some elements would push for a positive response to this question. A general assumption in France is that "Cold War style" defence programme are today useless. The defence budget crunching and the restructuring of the armed forces have sped up the change of these circumstances. By contrast, nowadays some larger

equipment programmes are still preserved for reasons of industrial policy. Some programmes such as the Rafale jet fighter, cannot have any utilisation in the security area. Moreover, the size of these programmes is largely influenced by industrial considerations. Still, compared to the 80s and 90s, no or a few new large equipment "defence only" programmes have been launched in the last few years. Accordingly, the defence industry, developing technologies susceptible of being used in the blurred area or in the security area, try to use this opportunity (satellites, sensors and helicopters for instance). Moreover, defence industry stakeholders believe that the broader demand for all manner of security (i.e. social security, healthcare, environmental preservation, food care, physical security) would require European states to increase their budgets accordingly, while demographic dynamics (ageing population and so on) will necessitate a cut in defence budgets. Those elements create a new focus on security, but not necessarily on the blurred area, as we saw previously. Actors like EADS and Thales are investing in security R&T, via the 7th FP, while DGA (*Direction Générale de l'Armement*, which is the French Armament Procurement Agency) is trying to help this conversion by financing security-related programmes.

Still, the blurring of borders between security and defence and its implication for industry has large limits. Some security and defence missions are still totally different. Maritime security does not really need heavy gunships, aircraft carriers or anti-missile frigate. It rather needs faster patrol boats with small guns and commandment ships with lot of capabilities, with sensors and communications tools.

Furthermore, defence and security equipments and budgets are still largely different. The National Police uses a significant amount of relatively "simple" equipment, from a technical point of view, that is bought in quantities (i.e. shotguns). On the other hand, defence equipment is generally extremely complex, from a technical point of view, and produced in smaller quantities. The French defence equipment budget is much more important than that of the Ministry of Interior.[286] Moreover, the planning process remains largely different, defence planning covering a longer timeframe.

In addition, while the defence equipment customer (the French State) is unique, the demand side for security equipment includes many institutions (infrastructure operators such as airport

[286] The equipment budget of the French MoD could be estimated at 10 billion euros, while the equipment budget of the Ministry of Interior is than 1 billion euros.

companies, rail operators, maritime institutions, telecommunication operators, national police and gendarmerie, etc.). This situation makes it more complex for industries to identify the security demand. Moreover, whereas the Ministry of Defence is used for interfacing with the defence industry and to manage an industrial policy, many security actors still have not integrated this dimension.

The security goals of the French state are mentioned in the 2008 White Paper on defence and national security. Apart from the developments already mentioned in the "technological developments" chapter, which also describes the industrial French policy, the enlargement of the defence industrial policy to the security sector is explicitly mentioned. The goal is to maximise synergies between the two fields, to reduce duplication and to improve interoperability between, for example, communication and crisis management instruments, but also in the fields of maritime surveillance, border control, intelligence and NRBC detection, to name a few. New synergies and more cooperation between civilian services associated with the security sector and the Ministry of Defence are requested, along with a fusion of technological intelligence ("*veille technologique*") tools.

The United States plays an important role as a trendsetter and has considerable political influence on security developments. French stakeholders seem to consider that the European Union should balance this influence and play a major role in the "normalisation" process. The USA is also considered to be a leading force of innovation and R&T, while the French DGA seems to have evolved to endorse the role of procurement agency.

Yet according to French officials, it is difficult to learn any lessons from the US experience. The defence and security "structure" in the US seems not to be merged at all, with a budgetary and institutional division of actors.

While the French Ministry of Interior has a budget line for investments of 508 million euro (210.8 million euro for the National Police and 297.2 for the Gendarmerie)[287], those investments essentially concern low technologies products, being difficult to be considered within the blurred area between security and defence. Moreover, this investment budget is parcelled in hundreds of micro procurement actions, the most important procurement actions being the modernisation of the communication system for the national police (project ACROPOL, for 37 euro million). Those programmes are absolutely non comparable with large defence equipments programmes, making it easy to understand the difficulties faced by defence industry to "understand" and penetrate this market.

By contrary, within the Defence mission of the French Defence budget, managed by the Ministry of Defence, some equipment programmes refer to security.

Those programmes are in the Programme 146, Action 10 "protection and safeguard", mostly in the function "Insuring the security of the State, the nation and the citizens". Thus, "this capability covers all the land actions led by armed forces within the homeland, thus contributing to the general and civil security (assistance and rescue to the population), in backing up national agencies and administrations in charge of security at the first place". Here too, no large programmes exist. The DETECBIO system (biological surveillance) accounts for 34 euro million. More generally, while the investment budget of the Ministry of interior accounts for 504 euro million for 2010, the Ministry of defence one correspond to 16.53€ billion.

Studying key documents on market policy from an administrative point of view confirms that a border still exists. Budgets remain separate, although some cross-pillar missions show that a strict border between defence and security is a non sense.

The compartmentalization between Ministries remains, mostly because each ministry protects its own budget. The LOLF, i.e. the Organic Law on finance laws, a new "financial constitution" that has become the main lever to reform public management, has enabled some decompartmentalization. For instance, the Gendarmerie's budget has been included within the Security budget before the institutional reform transferring the "Gendarmerie" from the Ministry of Defence to the Ministry of Interior (2009).

[287] Annex of the Loi de finance on « Sécurité » , p.13. This sector is responsible for activities centred on equipment and infrastructure, amongst others. This includes management of both the operational and investment budgets for the national police force, as well as equipping the departments. http://www.performance-publique.gouv.fr/farandole/2009/pap/pdf/PLF2009_BG_SECURITE.pdf

This situation stems from the differences between the defence and security worlds. The planning process of Ministry of Defence is extremely complex and includes programmes developed for 30 to 40 years. On the contrary, the Ministry of Interior, because of the type of equipments procured, has tendency to buy "off the shelves" and it is starting to procure common equipments for the National police and for the Gendarmerie (life jacket for instance).

It is quite complicated to determine exactly the amount of private budgets in the field of security.
In a large sense, according to the Atlas 2009, "Panorama économique du marché de la sécurité" – that analyses the 2007 situation – the security market in France represents in 2007 about 246,000 jobs and a global income of 16.7 billion of euro, a 6% increase from 2006. But those figures include areas unrelated to both the security and defence area, such as fire security (2.5 billion of euro, i.e. 15.5% of the whole – a 4.9% increase from 2006) or work security (2 billion of euro, i.e. 11.5% of the whole – a 2.1% increase from 2006).
More in detail, anti-terrorism and homeland security area represents 1.46 billion euro of its own, half of it made by EADS and Thales. Airport safety represents 374 million of euro (it has been multiplied by four in ten years) and closed-circuit television is about 910 million of euro (it has been multiplied by two in ten years). Only five French companies are listed in the European top 50 security companies and only 6 in the world's top 100 security companies.

4.2 Factors driving blurring of boundaries

It appeared very clearly from interviews carried out in France, both with public and industry authorities that the blurring of the border between defence and security, when it is accepted, remains a marginal phenomenon. Its origin is mostly identified with the interest of private companies to the growing security market and with the conceptual evolution of French authorities, searching for budget savings.

The development of international terrorism has obviously enlarged the French security market. Here, the two main drivers are international terrorism, with some attacks in France in the 80s and 90s and which later gave impulse to the market following the attacks of 11 September 2001 in the United States, and the growing security demand on the part of citizens. The security issue became

a key argument in France during the presidential elections in 2002 and even more so in 2007. The need to fight terrorism, illegal immigration in one hand and trade globalisation in other hand have led to better protection of transports and national borders – both on land and by sea. As a consequence, this need has been translated into the development of air and maritime security and that of land borders, but also into the development of security tools in cities.

Here it is worth underlining that the development of certain tools presented as being meant to protect the population against terrorism, are actually used for all kinds of activities that are potentially criminal. The development of surveillance cameras, in particular, serves to identify all types of criminal actions. According to this specific point of view, the border between equipment aimed at protecting the community and equipment aimed at protecting individuals disappears, along with the border between the fight against terrorism and the fight against crime.

In any case, the security market was born out of a need felt by the population and taken up and intensified by the public authorities, the concept having done nothing but follow this development without preceding it.

4.3 Factors constraining blurring of boundaries

Also if for the moment the movement seems to be marginal, we cannot exclude that the more the volume of blurred equipments becomes important, the more this interest will grow. At the moment, the French case shows that some defence companies (Thales, EADS) are attentive to the developments of the security market, which is viewed as a mean of diversifying activities, but with an interrogation on the concept of a blurred market.

Among the blocking elements, the fact that the relationship between the State and the supplier are not the same in the fields of defence and security is important. Long-term planning is not available at the Ministry of the Interior, nor has it ever created long-term partnership with private companies as it happens with the Ministry of Defence for equipments programme. The type of purchases remains “off the shelf” in most of the cases within the Ministry of the Interior, the technological content being different.

In France, the defence industry seems to still reflect a rigid separation between the security and defence markets. The perimeter of their activities is defined by the contracts that are won much more that by conceptual developments. As a consequence, the definition of the security market tends to vary from business to business.

Concerning the market, the non-existence of a centralized purchasing structure, or even of R&T and R&D between the Ministry of Defence and the Ministry of the Interior is without a doubt a brake. In certain fields, such as maritime security, many actors are present and the competencies are split up between different ministries, which do not make a global approach to the problem easier.

On the one hand, in France, there is currently no clear interaction between the national and European levels.

Annex 5.2. Blurring between security and defence in Germany

1. Conceptual change in Germany

1.1 Current situation

Since the end of World War II the Federal Republic of Germany has made a very strict distinction between the external and internal dimensions of security. This has lead to a clear separation between the institutions for external security such as the military or border control and internal security such as the police forces. It has further led to a decentralization of power over the means of violence between the federal government and the governments of the sixteen federal states (*Laender*). Finally, it has affected the ways and culture in which the different organizations have cooperated among each other and with industry.

German security policy advocates a comprehensive or "networked security" approach that conceptually blurs the boundaries between security and defence.[288] Until 1989 security policy had emphasized the military threat posed by other states and the military capability to protect the territory of the state in order to secure it political sovereignty. Since then all three parameters of this notion – states as main sources of violent threats, focus on the defence of the territory, emphasis on military means – have undergone fundamental changes. The classical territorial defence is now considered to be only one among a number of security policy tasks.[289]

Conceptually "blurring" or "convergence" is understood as the fact that territorial borders of the state have lost their significance for security policy but not for legal and hence organizational purposes. Due to the process of globalization,[290] non-state actors can circumvent borders due to the free movement of persons and goods; however, as well as state actors, they can evade borders by using non-kinetic weapons. It requires a security policy response that is equally not limited by border signs. However, the territorial border has not lost its significance as a demarcation of a legal space, in which particular rules for the society living on that territory apply.

[288] Instead of the "blurring of boundaries", some stakeholders speak of the "convergence of the security and defence domains".

[289] Garais, S.B. (2009b) 'Militärische Beiträge zur Sicherheit'. In Böckenförde, S. and Garais, S.B. (eds.) *Deutsche Sicherheitspolitik* (Opladen & Farmington Hills: Verlag Babara Budrich).

[290] The MoD White Paper delineates globalization as "the evolution and progressive networking of international flows of trade, investments, travel, communication and knowledge" (Bundesministerium der Verteidigung, 2006).

In other words, the increasing inseparability of "abroad" and "home" or "internal" and "external" holds for security policy, especially in face of threats that often have far away or indeterminate causes; from a legal perspective, which also concerns the question of how to respond to those threats, however, "internal" and "external" continue to be clearly separate. Hence, the redistribution of functions and tasks among the different security actors, especially regarding military, police and other law enforcement offices remains a challenge.[291]

Based on this analysis Germany has developed a networked approach to security policy, in which the traditional territorial defence by the national armed forces is but one task. The new policy aims to be multinational, globally oriented, forward looking and comprehensive, with the latter being of particular interest for our purposes. German security policy is "*comprehensive*" in that it employs a wide spectrum means ranging from diplomatic, economic, developmental, policing, military and only if necessary also armed missions. This explicitly involves a close inter-ministerial cooperation in the creation of the all-around picture of a situation and the formulation of a strategy.[292] The broad and comprehensive approach to security is buttressed by the parallel development of an approach to "civil crisis prevention". It involves activities of the Ministries of the Economy, for Environment, Finance, Education and Cultural Policy. The goal is to avoid causes of conflicts before the latter reach a violent stage.[293]

Despite this aspiration to comprehensiveness the military still plays a major role in German security policy. The *Bundeswehr* has embarked on a "transformation" that should enable it to flexibly and quickly provide the adequate military means for any unexpected security challenge.[294] Effectively, this implies a switch from a force focused on territorial defence to one that engages in expeditionary warfare, including the likely task of "international conflict prevention and crisis management, including the fight against international terrorism".[295] Transformation involves a new thinking in terms of military capabilities, which are created through the combination of personnel, equipment, concepts of the traditional three services. A communication and

[291] Böckenförde, S. (2009) *Die Veränderung des Sicherheitsverständnisses* (Opladen & Farmington Hills: Verlag Babara Budrich).

[292] Bundesministerium der Verteidigung (2006) 'White Paper 2006 on German Security Policy and the Future of the Bundeswehr'. available at: http://merln.ndu.edu/whitepapers/Germany_White_Paper_2006summary.pdf

[293] Bundesregierung (2004) 'Aktionsplan "Zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung", Berlin 12. Mai 2004'. Berlin, available at : http://www.ifa.de/pdf/zivik/aktionsplan2004.pdf

[294] Garais, S.B. (2009b)

[295] Bundesministerium der Verteidigung (2006)

information system that connects all levels of the armed forces will allow for the "networked operations control" for joint operations among the services and combined missions with allied forces. As we can see, so far, the changes have to an internal adjustment of the military but not to the conceptualization and creation of a new type of armed forces that, for example, combine military and police.

These conceptual changes, in particular the "transformation" may also have implications for industry. For example, it would require the procurement of new equipment such as airlift or communication capabilities. It would also mean a shift away from a procurement strategy that is centred on the replacement of older generations of weapons platforms with the implied long-term planning towards a procurement of capabilities, which can be easily adapted and incrementally enhanced. The conceptual changes might open the way to new fields of activities for the defence industry and new roles in the process of developing new capabilities. Moreover, transformation would entail the involvement of new types of suppliers, especially from the information and telecommunications industries, requiring new forms of cooperation between MoD and industry, on the one hand, and among defence companies on the other.[296]

1.2 Factors driving blurring of boundaries

As for the conceptual change, there are four drivers for convergence: since the end of the Cold War the security environment has significantly changed. The process of globalization involved that borders of territorial states became more porous. Hence, states became more vulnerable to new types of actors and threats that have effects across borders.[297]

"Brussels" is seen as a second important driver in the changing debate and way of thinking about security and defence. While for most interlocutors this factor is rather vague, some interlocutors see the Commission and the Parliament as actively advancing a convergence policy agenda.[298]

---

[296] Theile, B. (2006) 'Die Transformation verändert das Geschäftsmodell der wehrtechnischen Industrie'. In Borchert, H. (ed.) *Zu neuen Ufern. Politische Führungskunst in einer vernetzten Welt* (Baden-Baden: Nomos Verlagsgessllschaft).

[297] Böckenförde, S. (2007) 'Sicherheitspolitischer Paradigmenwechsel von Verteidigung zu Schutz'. *Europäische Sicherheit*, Vol. 8, pp. 29-30.

Workshop at BDLI (2009) *Industrial consequences of the convergence of security and defence in Germany, Workshop held on 14 May in Berlin*.

Interview CU (2009) *Interview conducted by the author on 17 March with a German defence expert*.

[298] Interview NP (2009) *Interview conducted by the author on 13 March with a German defence expert*. Interview DS (2009) *Interview conducted by the author on 3 March with a German security and defence expert*.

Technology is generally considered to be a major driver for the requirement to think security and defence as one. On the one hand, industry has sought opportunities to diversify the customer base by offering similar solutions to military and border/police forces, despite the different technical requirements. Helicopters, for example, are easier to "downmarket" for a defence than for a civil manufacturer of rotary aircraft. On the other hand, technology is purposefully developed and applied to enable convergence, for example in the case of cross-cutting technologies enabling integration, connectivity, and interoperability (telecommunications or IT-security) between different actors. This aspect is strengthened by the fact that "technical" change is often preferred to organizational or cultural change, as it is associated with less tough decisions and zero-sum situations.[299]

Finally, the thinking in terms of capabilities rather than platforms or legacy weapons systems fosters convergence, due to different reasons. On the one hand, it requires a thinking crossing the traditional lines of arguments, responsibility, and action. On the other, it brings the relevant players on the industrial but also the public sides together.

1.3 Factors constraining blurring of boundaries

At the same time Germany faces numerous challenges to the implementation of the networked security approach and, thereby, to the convergence of the security and defence domains. Not least among them is a strategic culture whose fabric is woven out of the "historical lessons" learned after the Third Reich and from the socialist experiment in East Germany. It involves a deep doubt in the use of military force in politics in general and within the borders of the country in particular.

Moreover, it inspires a suspicion towards any concentration of power in one institution and insists on strong oversight mechanism ranging from parliamentary participation in deployment decision, over the continuation of conscription to the concept of the "civilian in uniform", which remains at the basis of every soldiers education. While these cultural traits make a convergence difficult to achieve at the personal level, they are further buttressed by constitutional provision and legal practice, as the review of organizational aspects of the convergence of security and defence will reveal.

[299] Workshop at BDLI (2009). Interview CU, 2009

2. Organizational Issues

2.1 Current situation

Organizational issues represent the single most important type of obstacles for a blurring of the boundaries between security and defence. They remain normatively, organizationally, and culturally strictly separate. The Constitution clearly outlines the institutional and organizational setting in which public and private security and defence actors operate. It distributes the authority for security and defence among numerous actors at Federal and *Laender* levels. Given that these numerous actors also represent the demand side of the market, demand remains highly fragmented with little chance for consolidation either in a national or European framework.

The fundament for the constitutional setting is laid down by the German *Grundgesetz* (Constitution, Basic Law, or GG). It entails a number of provisions that clearly limit the possibilities for the security and defence domain to converge. First, it provides for a distribution of power between Federal Government (*Bundesregierung*) and the German *Laender*, between executive branch and Parliament (*Bundestag*) and between the different law enforcement services. Another principle concerns the strict functional and organizational separation between police and intelligence services. The latter have extensive powers to preventively gather information even without suspicion but no executive powers. The police, on the other hand, has broad executive but only limited investigative powers, as it can only become active based on concrete suspicion. These norms ensure a continued separation of the security and defence domains.[300]

The continued clear distinction between security and defence is even more powerfully institutionalized in the distribution of responsibilities between Federal Government and *Laender.*[301] As for internal security the *Bundesregierung* has legislative powers regarding the cooperation between the federal and *Laender* level. While these provisions enable the Federal Government to shape the way security is provided in Germany, it is required to involve the *Laender* in cases, where the legislative acts affect their interests and competences.[302]

---

[300] Garais, S.B. (2009a) 'Die Organisation deutscher Sicherheitspolitik. Akteure, Kompetenzen, Verfahren und Perspektiven'. In Böckenförde, S. and Garais, S.B. (eds.) Deutsche Sicherheitspolitik (Opladen & Farmington Hills: Verlag Babara Budrich).

[301] *Grundgesetz* Article 30 and 71-74.

[302] Garais, S.B. (2009a)

The constitutional separation between Federal and *Laender* levels corresponds to the institutional division of security tasks, leading to strict separation between military and police forces. The *Bundeslaender* are responsible for maintenance of public order and security in everyday life that is for the protection of civilians from crime, hazards and dangers that occur in the boundaries of the *Laender*. For this purpose they can to a large degree independently adopt their own laws with regard to domestic affairs, police, justice, protection of the constitution.[303] The Federal Government is in charge of the "overall national security" and allowed to create armed forces "for the purposes of defence" and in "expressly permitted" cases.[304]

This provision, supported by legal practise limits the possibilities for the deployment of the military inside the country.[305] The military must not be deployed inside the country to provide security but for strictly circumscribed tasks. These concern except for the state of emergency, for example, the support of law enforcement authorities such as the search of missing persons or cases of natural disasters.[306] However, in neither case does the authority or responsibility pass from the law enforcement organization to the military. This strict principle was re-endorsed by a recent verdict of the Federal Constitutional Court.[307]

Regarding the effective cooperation between security and defence actors, the *Grundgesetz* does not allow for the creation of new types of hybrid forces or authorities. Hence, Germany has no and cannot have any forces like the *Gendarmerie* in France or the *Carabinieri* in Italy which fulfil police *and* defence functions. The only way how existing bodies can cooperate within the boundaries set by the Constitution is through the establishment of networks that bring together the numerous actors of various types at the different levels of government. Consequently, existing organizations are not re-organized as to merge them and to blur their tasks and responsibilities; rather they are linked with each other through new interfaces. These concern the Joint Counter-terrorism Centre

[303] Ibidem

[304] *Grundgesetz,* Article 87.1 and 2 respectively. Though the concept of "defence" is not explicitly defined it could be understood in relation to Article 26, which declares: "Acts tending to and undertaken with intent to disturb the peaceful relations between nations, especially to prepare for a war of aggression, shall be unconstitutional" (Article 26.1).

[305] The provision has also consequences for the deployment of armed forces outside Germany, which is, however, not an issue in the present analysis.

[306] *Grundgesetz,* Article 35.2 and 3

[307] Bundesverfassungsgericht (2006) 'BVerfG 1 BvR 357/05 vom 15. Februar 2006 (Luftsicherheitsgesetz)'. available at <http://www.bverfg.de/entscheidungen/rs20060215_1bvr035705.html>.

(GTAZ) and the Joint Analysis and Strategy Centre for Illegal Migration (GASIM). Both work with the participation of security and defence actors.[308]

Finally, the provision of Article 87 GG entails the separation between armed forces and defence administration, which contrasts starkly with the situation in most other EU countries (and the structure of the EDA). Only at the very top is the *Generalinspekteur der Bundeswehr* – the German version of a Chief of Staffs – responsible for the "planning, implementation, and control of operations as well as the equipment of the armed forces".[309] This partition between demand and supply side *within* the defence organization makes an effective cooperation between the users of equipment and industry a demanding task.

The fact that the Constitution has provided for a number of actors with extensive powers that complement rather than duplicate each other implies a formidable challenge for a convergence of security and defence. The political system in Germany (and Europe for that matter) is characterized by a "cooperative federalism".[310] It implies that the tasks carried out at *Laender*, *Federal* (and European) levels complement rather than duplicate each other. Autonomous security authorities on each level are always only a part of the entire system. To achieve in such a system organizational changes in the security and defence domains requires the involvement of all political levels (there are sixteen *Laender* in Germany). At the same time such changes almost always have a constitutional dimension, which poses a serious obstacle for their adoption and implementation, given the political challenges of constitutional amendments.

Given these institutional setting, the organizational scene of security and defence actors remains separated and fragmented with concomitant consequences for the demand side of the markets. On the defence side is a single customer with the Ministry of Defence (BMVG). Through its Bundesamt für Wehrtechnik und Beschaffung (BWB) is procures the research, equipment, and services for the military including the German special forces, the KSK (*Kommando Spezialkräfte*) but not for the anti-terror unit GSG 9, which is subordinate to the Ministry of the Interior. This

[308] Möllers, M.H.W. (2009) 'Die innenpolitische Dimension der Sicherheitspolitik in Deutschland'. In Böckenförde, S. and Garais, S.B. (eds.) *Deutsche Sicherheitspolitik* (Opladen & Farmington Hills.

[309] Garais, S.B. (2009b)

[310] Schatz, H., van Oyen, R.C. and Werthes, S. (2000) *Wettbewerbsföderalismus. Aufstieg und Fall eines politischen Streitbegriffs* (Baden-Baden: Nomos).In the case of Europe it is more appropriate to speak of "cooperative subsidarity".

structure ensures that defence companies face one customer and a single set of rules, and a single strategy according to which goods and services are procured for the military forces.

Two relatively recent developments further structure the situation in terms of consistency and transparency. Since 2005 the highest military officer – the *Generalinspekteur* – has also been responsible for equipment procurement, which should ensure that the military (and not a civil) office formulates the equipment requirements in line with military strategy and doctrine. Moreover, in 2007 government and industry have agreed on a common list of "national armaments core capabilities". Far from formulating a "defence industrial strategy" as the UK in 2005, this four page document represents a basic agreement to maintain the major defence-industrial assets either at a national or a European basis.

On the security side the structure of demand is far more fragmented. At federal level there are the Federal Police and the Federal Criminal Police as well as three federal intelligence services.[311] Each of the sixteen *Laender* has an own police organization and an Offices for the Protection of the Constitution. Every single *Bundesland* has its own rules as to the equipment of the police forces and decides on what and when to procure. However, equipment standards are harmonized through the permanent Conference of Interior Ministers (*Innenministerkonferenz* or *IMK*), an important coordinating body (see below). Finally, there are fire brigades in each of the *Laender*. Other important users are disaster protection and relief organization and private security companies.

Fire brigades are, as police forces, legislated in each of the sixteen *Laender*. While norms for technical equipment and training are almost identical throughout Germany, organization and financial authority various considerably. There are about 100 professional, 800 corporate, and about 23,000 voluntary fire brigades in Germany.[312] Their procurement is very fragmented, since the sixteen *Laender* legislate the procedures and in some cases leave responsibility even to the large communes.

Disaster relief and protection does not involved permanent forces or a specific authority but is rather an organizational principle that allows for the mobilization of all kinds of capabilities depending on the severity of the disaster. Thus a relief effort might involve the military, police, fire brigades as well as allied armed forces on German territory. They are supported by aid

[311] Garais, 2009a. Moeller, 2009.
[312] Deutscher Feuerwehrverband (2009) 'Über den DFV, About DFV'. Available at: http://www.dfv.org/

organizations such as the Federal disaster protection organization (*THW*), the Red Cross, German Life Rescue Society, or Malthese Aid Service. In addition private companies can be ordered to support the relief effort such as transport, logistic or construction companies or firms that provide cooling or heating technology.

Private security firms work mainly on private assignments. In Germany there are about 3,500 security firms, employing 177,000 people. About two thirds of the firms SMEs accounting for 4% of the yearly turnover of the sector of € 4.35bn.[313] This is one reason why this group, despite it continued growth accounts only for a small portion of the procurement volume of security and defence equipment.[314]

The sheer number of different actors and the division of responsibility between Federal, *Laender*, and communal levels makes a coordination or harmonization of their equipment requirements challenging. Problems of interoperability between fire brigades and disaster relief organizations as well as the police abound. The situation is worsened by the fact that also the responsibility for procurement decisions is dispersed.

It should be noted here that SMEs actually appreciate the fragmentation of the procurement market. They consider the decentralization as an advantage, since customers could specifically ask for what they need and a special treatment of single suppliers is avoided. However, it has to be assumed that the demand of different public procurers really that different; and will it not lead exactly to the special treatment of a single *regional* or *local* supplier that SMEs say, is avoided.

2.2 Factors driving blurring of boundaries

The discussion has shown that there are hardly any drivers for the blurring of boundaries between security and defence on the organizational and institutional side. The German Constitution clearly separates the authorities for defence and security between the Federal Government and the *Laender* governments as well as between the different types of armed forces. These provisions are reflected in a strict organizational separation between security and defence and a fragmentation of the security domain. Coordination between the numerous actors in the latter exists to a narrow

[313] BDWS (2008) 'Der Bundesverband Deutscher Wach- und Sicherheitsunternehmen, 1 July 2008'. Available at: http://www.bdws.de/cms/index.php?option=com_content&task=view&id=510&Itemid=32>.

[314] Spiegel Online (2003) 'Das Geschäft mit der Angst'.
Available at: http://www.spiegel.de/sptv/extra/0,1518,242755,00.html

extent but is mainly limited to missions and does not extend to questions of equipment policy or procurement.

The other exception for close cooperation between security and defence organizations are missions. They concern missions abroad and at home, for example during the FIFA World Cup in 2006. Missions have proven as an important driver for blurring, as the experience gained by all actors in joint missions played an important role to reduce prejudices and facilitate communication and learning.

The work of the German Federal College for Security Studies (BAKS) should be named as an organizational driver for change. The BAKS can be regarded as a forum that promotes the blurring of boundaries between security and defence in conceptual and cultural terms. Its mission states that it is "Germany's highest-ranking interministerial institution for advanced education and training in the field of security policy". The institution is comparable to the National Defense University in Washington, the *Institut des Hautes Etudes de Défense Nationale* (IHEDN) in Paris, or the Royal College of Defence Studies (RCDS) in London but has only been operating since 1992. Its main contribution to blurring is the Seminar for Security Policy, a six-month course bringing together about twenty mid-level experts from Ministries, public institutions but also private companies in the area of security and defence but is open also for researchers and representatives of NGOs, the media, unions, and the church; from Germany, European countries, and other states.

2.3 Factors constraining blurring of boundaries

Organizational factors represent the single most important type of constraints to convergence between security and defence. Chief among all is the organizational fragmentation of security actors between Federal and Laender levels. The number and diversity of final users without much pooling and coordination of procurement of security equipment makes coordination with defence customers/users a challenge. Moreover, there is no coordination between different security customers and between security and defence customers at EU level.

A concomitant obstacle is the deeply ingrained difference between the many actors of external and internal security. It is this "difference of cultures", "languages", and "thinking" that is by some considered to pose the greatest challenge to convergence. The reason can be found in the quite different working environment, which implies different mindsets and approaches to equipment.

While a soldier often faces a life or death confrontation, the operational environment for the police is habitually more benign. Similarly, the mindset of the soldier is much more exclusively aimed at survival but a law enforcement officer has to take other values into consideration. For the latter “security” and “protection” can never be “total”. They can only be “as good as possible in certain circumstances” and in consideration of other goals such as the repercussions on public order. These different mindsets translate directly into different approaches to do business with equipment manufacturers. MoDs tend to be much more confident and clear-cut with regard to the specificity of the requirements and the demand for delivery than MoI (Interview DT, 2009). They have ample experience with the management and coordination of (even international) large scale procurement projects and the regional and industrial policy opportunities, which is largely absent or of a different character in the security domain.

The strict separation of security and defence organizations has consequences for the demand, as customers in the defence and security markets have different values according to which they select a piece of equipment. Hence the success factors for companies differ in both cases. The defence market is compared to the security market considered to be much more sensitive, as it is associated with the international position of a state, its room for manoeuvre in foreign policy, its sovereignty and its survival. Security, on the other hand, is still mainly linked to public order, protection of civilian in cases of disaster and, hence, subject to other, less stringent and, for example, less secretive rules. The following discussion, attempts to bring out these different concerns and the relative weight that is attached to them, highlighting the differences that prevail with regard to the requirements of security and defence actors.

Generally, Western militaries rely on the (asymmetric) technological sophistication of their equipment as opposed to the higher number of military personnel for example. Traditionally military equipment has been specifically designed for the purposes i.e. missions and operational scenarios envisioned by the military. Compared to the security market military equipment requirements place a premium on performance rather than cost. Using of-the shelf components has become an increasing practice only after the end of the cold war but is still not wide spread in the culture, structure and processes of the organizations dealing with the issue, neither on the demand nor on the supply side. Only in as much as the formulation of military requirements involves the consideration of capabilities needed to carry out security tasks it would come to a further blurring of boundaries between security and defence. This is likely to occur for (peace

mission and stabilization operations) scenarios in which the military will need to take on police tasks or in scenarios of joint operations with police forces. The formulation of requirements should then involve all the Ministries concerned.

Another difference between security and defence concerns the degree of European cooperation in the elaboration of equipment requirements. National Armaments Directors (NADs) of European countries have, in different configurations, cooperated on this issue since the mid-1970s in the IEPG, WEAG, LoI/FA, and the EDA. These efforts have involved also the lower level experts of the procurement administrations, dealing with other areas such as research or economic matters (at times even from the Ministries of the Economy and Business). No such forums exist at European level for the meetings of equipment procurement officials of Ministries of Interior.

There has also been a privileged involvement into the definition of military requirements of the largest defence companies of European countries through EDIG, AECMA and other industry associations, and now ASD; for the large information and communication technology or security firms to this day, such access exists neither to NADs and Ministers of Defence nor to Ministers of the Interior and their procurement heads.

Another obstacle to blurring exists due to different attitude as for security of supply of critical components. The Ministry of Defence is more concerned with issues of security of supply of critical systems or components than the customers in the security domain. Often “security of supply” is in the defence realm understood in a particular way, namely that the country needs to be autarkic or keep the industrial and technological capabilities “onshore”. Security of supply can also be achieved by making sure that a variety of different sources of supply remain accessible (Moran, 1990), a way of thinking that is much more prevalent in the security sector.

Finally, there is a significant gap in the way how procurement is used as a means of industrial policy in the two sectors, which has negative consequences for convergence. In the defence sector there is a long history of using procurement contracts for industrial policy. While the effects on innovation, regional development, and employment are debated there is an array of established policy instruments with experienced experts of the supply and the demand side as well as a considerable body of academic literature on this topic. All does hardly exist at this point for the support the security industry. While research programmes at national and European levels have had their first positive impacts, the potential of public procurement for the promotion of innovation in the security industry still has to be realized. For this purpose the security still

requires accepted framework conditions such as established standards and norms for the orientation of the many public procurement actors. Given the fragmentation of the demand side of the security market, security has so far not yielded many results with regard to innovative procurement solutions. Single key projects can provide but a first step of this development.

A related problem concerns the size of a viable investment, which differs significantly among both domains due to the fragmentation of the security market. The benefits of these investments usually exceed the benefits that the investor can gain. For example, from the security of a container benefit municipalities, transport infrastructure operators, and consumers and not only the port authorities but it is the latter that need to make the investment. Given the fragmented structure of the security market it is very likely that in many cases the investment requirements will exceed the resources of the buyer. In comparison to the defence market there is the challenge in the security market to spread the cost of an investment to the beneficiaries of increased security. Germany's federal structure increases this challenge and so far inertia has mainly been overcome when the Federal government has not only led the initiative but also financed it, as in the case of the introduction of software defined radio (*BOS*) for the police.

3. Technological Developments

3.1 Current situation

Technological developments represent some of the strongest drivers for the convergence of security and defence. As the following section will show, research activities remains to a large extent separate given that research procurement agencies follow a strict distinction between civil and military research putting little emphasis on synergies between the two fields. The application of research results and of technologies, however, represents a strong impetus for blurring.

Until 2007, Germany had no systematic and strategic research specifically focusing on civil protection. In that year, the government launched the first-ever national cross-departmental program of security research. Rather than exclusively focusing on the development of new technologies the programme equally promotes research in the social dimensions of security.[315]

[315] As mentioned above, security companies in some segments complain about the strong technology focus and consider research for systems integration and new applications equally important (Bundesministerium für Wirtschaft und Technologie, 2009).

The Federal Ministry of Education and Research (*BMBF*) has become an important procurer of research services. Parallel to the EU's security research programme the BMBF set aside € 123m for a four year period starting in 2007 to finance the security research activities.

So called "innovation-platforms" are used as forums to shape the research area and future security requirements. As for the research area the programme clearly aims at influencing EU research activities. Regarding security requirements innovation-platforms offer a way to promote the successful market implementation of security technologies. They can, for example, serve to identify obstacles to innovation as well as for the setting of new industrial standards. At the same time they allow for a "layered" communication with among a "core group" of researchers, an "associated circle", "an expert scene", and the public. It serves to shape the perception and the conditions for the acceptance of new security technologies as well as security research.

While the programme is announced as promoting "non-military" security research, it aims to enhance the "mutual exchange of research know-how". However, stakeholders have indicated that the separation between security and defence persists. Both, the Ministry of Defence and the Federal Ministry of Education and Research insist that their budgets are used by the research institutions exclusively for defence research projects with military applications and security research projects with civil application respectively.

The programme clearly focuses at the promotion of German research and technology. Using standardization as a common "non-political" and "technical" tool has repercussions for competition in the Common Market and is, hence, of outmost interest for the Commission. Rather than letting new national standards emerge, the Commission should pursue an active policy of standard setting in the area of security and defence.

Public German research and development activities in the security and defence domains are mainly carried out in two federal institutions: the German Aerospace Centre (*Deutsches Zentrum für Luft- und Raumfahrt* or *DLR*) and the Institutes of the *Fraunhofer-Gesellschaft* (FI), which concentrate on basic and applied research respectively. In addition, there is with FGAN a specialized for applied research for the armed forces as well as the institutions of higher education for military and police officers.

The DLR focuses on research in the four fields of aeronautics, space, transportation and energy. The topics of defence and security research continue to be treated in separate ways. Regarding defence the DLR has lately integrated its expertise in the four themes in a "defence" department,

since projects of the MoD are sufficiently regular and significant in size. Such a re-organization has not been done with regard to security research, where the DLR plays more of a coordinator role. The recently adopted five-year plan does also not envision an organizational unit for security research.

In comparison to the DLR, the Institutes of the *Fraunhofer-Gesellschaft* can easily be re-grouped according to the research requirements (Interview NP, 2009). Thus, several institutes have formed a Group for Defence and Security, aiming to maintain the "traditional combination of research fields with civil and military applications".

An important intermediary in the research field is The Association of German Engineers (*VDI*). It is a "financially independent and politically unaffiliated, non-profit organization of 132,000 engineers and natural scientists". As a "leading institution for training and technology transfer among experts, it is also a partner at the preliminary stages of the decision-making process in matters of technological policy". More concretely, the VDI serves as an administrative hub for many EU financed research projects in which German institutes participates. Therefore, it is excellently positioned to contribute to the transfer of knowledge between the security and defence domains. Given the technical orientation of the organization and background of most members, the VDI is a veritable partner for DG ENTR policies.

Regarding applied research a separation along traditional lines prevails. The Research Establishment for Applied Science (FGAN) has for 50 years carried out applied research in the field of military technology. It brought together separate university workgroups within the framework of a central establishment and took its current form in 1999. FGAN consists of three research institutes which are predominantly active in the field of Command and Control: FHR, the Research Institute for High Frequency Physics and Radar Techniques; FKIE Research Institute for Communication, Information Processing & Ergonomics; and FOM, the Research Institute for Optronics and Pattern Recognition. The research establishment supports and advises the *Bundeswehr* on "innovative strategies, processes and sourcing. In particular, the task of FGAN is to identify potential areas of utilization, so that technological advances can be optimally implemented within the specialized environment of military deployment" (FGAN, 2009).

In five areas the application of research results and new technologies supports the convergence between security and defence. While two of these areas originated in each of the defence and

security sectors, one relies in particular on generic technology, namely information and communication technology.[316]

Unmanned aerial vehicles (UAVs)

UAVs are of interest to users in the security as well as defence domain. The German MoD deploys a number of tactical drones and supports the research on a number of larger UAVs. The latter concern the EuroHawk, the Reaper, and the Fancopter. While Germany has requested to purchase five Reapers and four ground control stations, plus related support material and training from the US, the EuroHawk is developed in cooperation by EADS (Germany and Spain) and Northrop Grumman of the US.

Security customers, being they police forces, border or coast guards, fire fighters or disaster relief forces, have a considerable interest in the developments of the UAV market. In many debates it is referred to as a prime example for the convergence of security and defence with broad implications for industry. For the time being "the civilian sector, although it is 'on hold'" though. It is expected to develop only once market regulations and some fundamental legal and technical issues such as safety and responsibility for operation, collision with other aircraft have been clarified. Thus Frost & Sullivan forecast a significant number of units (20) only in 2013, rising to 100 in 2017. However, these will mainly be smaller UAVs (Frost & Sullivan, 2008).

The Commission is promoting the creation of this market with numerous activities such as research funding or conferences, where the key actors are brought together. The EDA has been supporting relating activities. Both are essential in the eyes of security and defence stakeholders, from industry and government to support the industrial and technological base for this market.

Helicopters

Helicopters is another market segment that is of interest to bother, security and defence customers, albeit with different requirements for their products. This has been the case for many years now, without helicopters being recognized as a "driver" of convergence or a dual-use product. This fact is mainly due to the fact that civil helicopters are an established strong but fragmented market and demand of security and defence customers remains uncoordinated.

Information and communication infrastructure

[316] This bottom-up analysis is complemented by a top-down analysis according to technology taxonomy in the technology chapter of the summary report.

For the military information and communication infrastructure is important in order to ensure the seamless operation of different services and weapons systems. For this purpose the military requires command, control, communication and computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) capabilities. They are of strategic importance for the transformation of the *Bundeswehr*.[317] The main procurement programmes in this segment are the establishment of a joint IT-infrastructure and communications system for all services of the military and several projects for intelligence collection and surveillance. For example, the SAR-LUPE "space-based reconnaissance system will, for the first time, provide the Bundeswehr with a worldwide imagery reconnaissance capability"; the *Herkules* project aims at the standardization of the non-military information technology of the *Bundeswehr* in a single system, including 140,000 PC workstations, 300,000 telephones, and 15,000 mobile phones at 1,500 different locations. This project is run by a joint consortium of Deutsche Telekom and IBM Deutschland. Given that the use of commercial of the shelf solutions has increased in the past years, the MoD has stepped up its effort to adapt the standardized items to the specific needs of the armed forces.

Most relevant for the issue of blurring are secure communication and data exchange equipment, as they are specifically designed to allow forces and experts of the different domains to communicate and collaborate. The German Ministry of the Interior currently introduces a single software defined radio (SDR) solution for all security actors in Germany, called "BOS". It does not only involve the Federal and *Laender* police, disaster relief forces, fire fighters and rescue services but also customs authorities and the domestic intelligence services. Allowing for 500,000 users, BOS will be the largest SDR system based on the TETRA standard, which is also used in many other European countries. A key learning from the BOS project is that it takes the Federal Level to take a conceptual, organizational, and financial lead should the introduction of a new technology be successful.

Detection and identification of dangerous substances

This segment comprises all equipment for the purpose of the detection and classification of dangerous substances. These concern in particular mobile and fixed equipment, especially sensors, for the detection of weapons, ammunition, and illegal goods in containers and vehicles;

[317] Secure command, control and communications systems include the area of IT-security. The goal is to ensure the secrecy, availability, and integrity of data. Subsegments include software, services (installation, maintenance, support), basic protection of business or administrative processes, certification.

equipment for the control of persons, luggage, and goods as they are used at airports and seaport; and the services linked to these controls, which is the fastest growing segment in this market. Especially regarding sensors it is difficult to delineate the market according to users, since they are also integrated in equipment for the process measurement, quality control, environment, and research.

The detection of explosive substance is a central topic of security research and of equal importance to the military as well as police forces, as most terrorist attacks as well as many attacks on troops used improvised explosive devises. The research task is structured by the consideration of different scenarios and various substances. While portal systems at airports allow already today for (limited) possibilities to detect explosives, the surveillance of larger spaces, and the remote sensing of explosive remains a challenge. A further miniaturization and reduction of cost can be expected in the case of applications for the surveillance of buildings and of the supply chain. Hence this segment represents not only an area of convergence between security and defence but also between security and safety.

This segment presents an extremely important field for the blurring of boundaries between security and defence for two reasons: military, police, border control forces and customs official all require equipment for the detection of dangerous substances. The equipment is used in field camps during military operations as well as at air and seaports. Moreover, the market is still in its infancy and can relatively easily be shaped.

Equipment for civil security personnel

The segment comprises all equipment for civil protection forces such as police, fire fighters, disaster relief forces, and security guards. More particularly it concerns the special attire of such forces including surveillance of their physiological state and maintenance of the gear and communication technology; and special vehicles (armoured general purpose vehicles, fire fighting vehicles, and robotic systems). In other words all ordinary professional clothing or mass produced police cars will not be considered.

In this context arises a potential for blurring, albeit in a rather unexpected way: given the quality reputation of German products abroad, many customers seek for ways to acquire German technology while still following the requirements of their governments. Here offsets, as they have for a long time been practiced (and debated) in defence might offer a solution for security

equipment suppliers. However, offsets are officially opposed by German defence companies and government.

3.2 Factors driving blurring of boundaries

Technology can be considered a key driver for the blurring of boundaries between security and defence. This concerns the application of technologies and research results more than their creation. Thus the military and security forces use applications of the same technologies, as for example in the case of UAVs, special textiles, or detection and identification of dangerous substances. We have also noted that the institutions of higher education such as the BAKS plays the role of a change agent for the conceptual and cultural change that is required should further blurring occur. The Seminar for Security Policy fosters exchange and shared understanding and provides an interesting example for the creation of an analogous course at EU level i.e. by the European Defence College.

As we have argued, application of information transfer and communication technologies is an especially important driver for the blurring of boundaries. The digitalization allows for seamless interoperability and interconnectiveness among security and defence actors and applications; so does the incremental improvement of existing technologies to new problems, which is expected to present a major growth area in coming years. Consequently, the pooling of research and procurement can lead to scale effects and to blurring of boundaries. We have stressed that public research promoted by national or EU institutions and procurement be it by military or security customers can play an important role for further convergence.

Other areas of importance for blurring are those one with applications for the detection and identification of dangerous substances and for surveillance systems. In these areas defence and security customers can be expected to have similar technical requirements. Nevertheless, active coordination at European or national levels will be necessary to translate similar needs into harmonized demand.

3.3 Factors constraining blurring of boundaries

There are important factors limiting the blurring of boundaries between security and defence, in particular in the area of technology creation. They concern specifically institutional arrangements

on the side of research and technology procurement. Such constraints to convergence include for example the continued strict separation between the financing of defence and security research by MoD and Ministry of the Economics and Technology. Similarly, the existing organizational separation within research institutes, which is partly result of separation of financial responsibility, also presents a hindrance to further blurring.

Moreover, technological innovation towards convergence is also not helped by the fact that security and defence customers are generally careful to integrate new technologies into their work practices. Reliability and fit with existing interfaces are important requirements to be met by any new equipment item.

As for the research activities, stakeholders have voice the concern that the current German security research programme is too much focused on technology development rather than systems integration, i.e. it does not particularly favour the search for synergies or networking across the boundaries of the security and defence domains. Additionally, stakeholders have pointed out that the significant administrative burden for participation in EU and national research projects is a continued deterrent for SMEs to participate in such research efforts.

4. Industry and Markets Developments

4.1 Current situation

The market for security and defence products and services remains separated. This separation is mainly a result of the different rules for the interaction of public actors with (mainly private) providers of goods and services as well as for the oversight by the government and the support it offers suppliers in their activities. The separation and fragmentation of the demand adds further to the continued existence of two separate markets. Nevertheless, there are signs that especially defence firms enter the security market and for cooperation among the firms of the separate markets. In the following we will characterize the German defence and security markets and industries. Herein we will also comment on those market segments that have been examined above as areas of technology application that promote the blurring of boundaries between security and defence.[318] Since the structure of the demand side has already been addressed in the

[318] It must be noted, however, that it has not been possible to obtain data about the market size for all technology

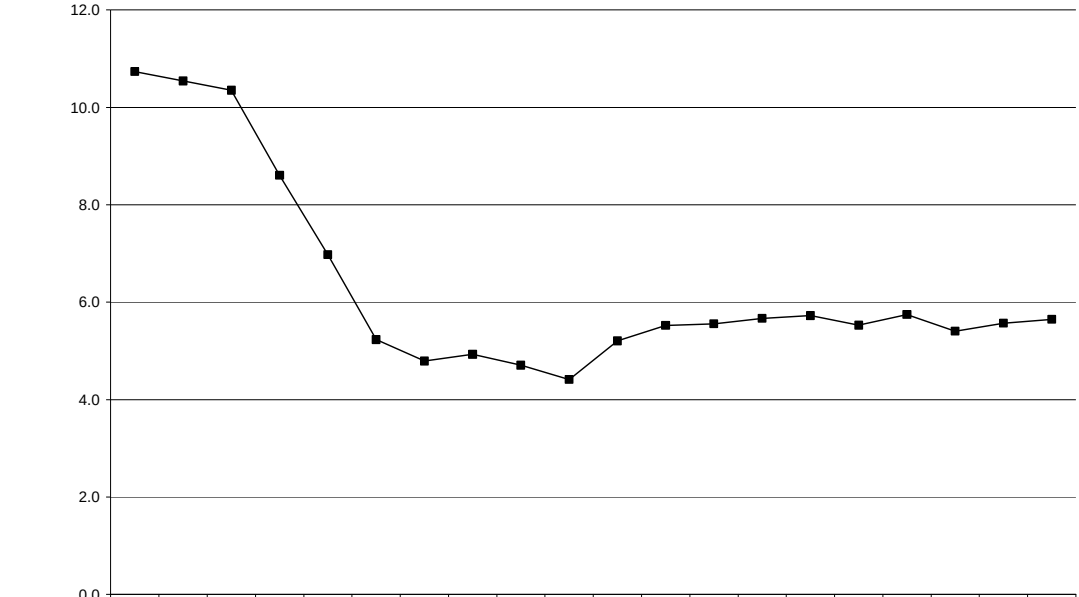
section on organizational issues, we will focus here on quantitative and industrial aspects as well as the regulatory situation.

The German defence market and industry

Military and police forces at Federal level have dedicated procurement organizations, which differ, however, starkly in the way they interact with industry. The Ministry of Defence is the single most important procurer of security and defence equipment. It oversees a budget of roughly $ 6 bn (€ 4.1 bn) per year for new equipment. In addition it funnels about € 1,2bn a year into research and development activities.

As Figure 1 shows the equipment budget has by and large remained stable over the past years. Industry experts don't expect the budget to change much in the near future.

Figure 1: German defence equipment expenditure in billion USD in constant 2005 prices (SIPRI 2008 in combination with NATO 2008)



	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Germany	10.7	10.5	10.3	8.6	7.0	5.2	4.8	4.9	4.7	4.4	5.2	5.5	5.6	5.7	5.7	5.5	5.7	5.4	5.6	5.7

The procurement is carried out by the civil administration of the MoD, the Federal Office of Defence Technology and Procurement (BWB).

In other words, no direct interface between military and industry exists, which partly restricts the direct flow of information and lessons learned back to companies and prolongs the

applications mentioned above.

implementation of innovation. Direct contacts between industry and the military are, due to historical experience, still considered problematic and restricted by laws. Recently changes to the legal situation have been adopted and the Commerzbank has set up the "Celler Trialog", a yearly meeting between business and former officers to facilitate an easier incorporation of former military personnel into the business world.

In general the supply side of the defence sectors is highly concentrated. The established defence companies form a major group of suppliers such as EADS, Diehl, Rheinmetall, or HDW. They have traditionally close relationships to the defence procurement agency and an intimate knowledge of the requirements of the procurement process. They fear a freeze or further reduction of the defence procurement budget and consider "security" as a new business opportunity that compensates for the anticipated losses. At the same time the defence industry is faced with the requirement for interoperability of the equipment, a decreasing number of procured units, and shorter time leads for the procurement or improvement of equipment.

More particularly and with regard to the major areas of technology application that drive blurring, the market segment for UAVs is one of the most dynamic. In Germany as in Europe the market for military UAVs has witnessed a considerable growth for the last two to three years, which is expected to continue for another ten years. For all EU countries a recent study estimates the market size to be just over 300 units, generating revenues of about € 1.4 billion by 2011. However, what seems to be a military market of significant size, produces modest revenues owing to the nature of the equipment, with small drones still dominating the procurement agenda (Frost & Sullivan, 2008). German firms, especially Rheinmetall DeTec, have a reasonably strong competitive position with regard to mini- and small UAVs like the KZO or the Fancopter. However, their know-how is less strong for Medium Altitude Long Endurance (MALE) UAVs.

As for helicopters German industrial and technological capabilities for rotorcraft are concentrated in Eurocopter (EADS), which is the leading helicopter company worldwide. The procurement of NH 90 transport and of the Tiger attack helicopters ensure a high utilization of industrial capacities.

The German security market

As mentioned above, the demand side of the security market is very fragmented in Germany, as it is scattered between Federal and *Laender* levels and among different organizations at each level.

While the Federal Ministry of the Interior (MoI) has a central procurement agency – *Beschaffungsamt*, it is responsible for the lesser part of the procurement budget.[319] Though the volume of its procurement budget (€ 546 bn in 2007) is only about 15% of the defence procurement budget, it has developed much more dynamically in the past years than the defence budget. The MoI has more than doubled its expenditure between 2001 and 2007 and this trend is expected to continue. The main spending items were services (36%) – mainly for airport security – telecommunication technology (25%), vehicles (15%) and information technology (12%) of the overall budget. Despite the increased procurement volume, the number of projects has remained constant, which implies rising project volumes and, hence a potential to direct industrial investment.

At *Laender* level the Conference of Interior Ministers Conference (*IMK*) plays an important role for the coordination of activities between the different *Laender* and the BMI. As a forum for policy formulation and coordination it facilitates the agreement on common standards and equipment requirements. The Ministers, including the Federal Minister, meet twice a year on a voluntary basis. Its Working Committee II is dedicated to questions of threat prevention, anti-terrorism, and police issues. Its meetings also include the Presidents of the Federal Police and of the German Police University (see below). Currently, the IMK attempts to form a position regarding the use of armed forces for particular tasks within Germany as well as with regard to the topic of security research. Both might have considerable consequences for the convergence of security and defence.

The *Laender* account for 70% of the overall public procurement in Germany, which reached € 260bn in 2008.[320] It is the Ministries of the Interior of each *Bundesland* that procures the equipment for the police forces and the fire brigades. The extent to which the *Laender* pool their procurement efforts vis-à-vis industry remains very limited (Interview DT, 2009), (Interview SQ, 2009).

The total size of this market was estimated to be € 20 billion in 2008 and to grow to € 31 billion by 2015. German companies account for about 70% of the total value added.[321] Rising crime rates, a

[319] The fact that there is no English name of the body nor an English version of the official website, goes to show that its procurement policy is still very much focused on German rather than European suppliers (Beschaffungsamt, 2009).
[320] Not known at this point how much of this sum is spent on security and defence purposes.
[321] These figures include also the segment of "investigation and phorensics" with € 800 million and € 920 million for 2008 and 2015 respectively. As it is of little relevance to the issue of blurring, this segment is not considered here.

change in the demographical situation, but also the increasing use of police and military forces in expeditionary operations drive the demand for security equipment and services.

In general, the supply side of the German security market remains fragmented, which is a stark contrast to the defence market. While companies like Bosch Security Systems and Siemens are the most important domestic suppliers and cater to the end-user preference for a one-stop shop for all their security requirements, innovation mainly comes from SMEs. Hence there is a close cooperation between large and smaller firms without the latter having lost their independence.

More particularly, as for the major areas of technology application that drive convergence, information and communication infrastructure is the most important segment.[322] In 2008 the market segment was estimated to have a size of € 6,750 million. Especially the subsegment of IT security is expected to grow dynamically in the coming years (about 12% per annum), to reach by 2015 cumulated sales of € 10,640 million (up from today's € 4,750 million). Growth will result not so much from innovative technological breakthroughs but rather from adaptations to novel problems. Such problems concern, for example, the dangers arising from an increased mobility of hardware and data; the errors due to human behaviour; the design of the interface to strike a balance between security and user friendliness. German companies are specifically strong in this subsegment for solutions that involve comprehensive enterprise services. Though the market is dominated by globally acting firms, Germany has remained quite independent due to the strong showing of its domestic firms.

The market segment for detection and identification of dangerous substances was estimated to have a size of € 830 million in 2008. In the next years it is expected to constantly grow by at least 6% per annum, so that by 2015 cumulated sales are expected to amount to € 1,280 euro. By comparison for 2010 the US market for mobile detectors of dangerous substances alone is expected to reach about € 7 billion. Successful companies in this segment is, for example the firm Robowatch, which is the world market leader for mobile detection equipment.

Finally, the market segment of Equipment for civil security personnel had a size of € 2,330 million in 2008. In the next years it is expected to constantly grow by about 3% per annum, so that by

[322] The following market estimate is based on the consolidated data provided in (Bundesministerium für Wirtschaft und Technologie, 2009) for the segments "information and communication in times of crisis" and "IT security". They refer only to the security but not to the defence market, where sales of C4ISTAR equipment would need to be considered.

2015 cumulated sales are expected to amount to € 2,860 euro. Growth is expected to be rather modest, as it is mainly dependent on the budgets of public procurers and varies among the different sub segments. For communication technology, for example, the Federal Government will spend € 15 billion over the next ten years. The market for fire fighter vehicle, however, is rather stagnant. Domestically only some 20 "heavy duty" fire fighters, i.e. at air- or seaports or large chemical companies, require specific solutions and drive innovation. They account, however, only for 5-10% of all sales. Exports don't promise increased sales either, as foreign governments insist on national supplies.

Different legislation for security and defence markets

Security and defence markets are regulated in different manners at national, European, and international levels, partly in a contradictory manner. While armaments cooperation has led to a certain joint understandings, Codes, and legislation for dual-use items, there is not even a recognized list of all legislation with relevance for the security sector.[323] A brief review of the different regulations of foreign direct investment (FDI), export controls, anti-terrorist and data protection legislation as well as norms and standards will reveal that security and defence markets continue to be governed by different rules.

Traditionally, the government has been much more sensitive with regard to foreign direct investment (FDI) in defence companies than with foreign interests in security related firms. The methods of control or protection are far ranging and include measures such as the consolidation of all sensitive assets in the aerospace sector in one major company – EADS – where German interests are represented by the industrial shareholder Daimler over the participation of German *Laender* in crucial firms to legislative instruments.

In Germany, like in other European countries, specific legislation has been adapted in the past years and is currently amended. The new law will requires any foreign investor acquiring more than 25% of the voting right in a company that concerns the "public order and security" of Germany, has to be notified to the Ministry of the Economy. The Ministry is to consult with the "Ministries concerned" and will suggest the acceptance, an amendment, or a ban of the investment, which then has to be accepted by the Federal Government.

[323] The ESRIF working group "Innovation" estimates that several man-years are required to establish such a list covering European legislation and has recommended its elaboration.

Traditionally, only different types of defence firms and satellite companies were explicitly mentioned in the legislation. Consequently, the Ministries of Defence and Finance have been heard. Given the new focus, the Ministry of Economic has to include new types of companies and industries as potentially becoming subject to scrutiny such as firms producing encrypted print equipment. Moreover, it has to get used to involving the Ministry of the Interior, which so far has neither been required nor been done in an informal manner.

Hence for further convergence of two domains it would be important to consider the specific situation of the security realm. The currently debated amendment does not list some technologies in which German firms are leading and that might have repercussions for Germany's security and commercial interests, such as image processing and biometry. Moreover, due to the different structure of the supply side in both markets (rather concentrated in defence as opposed to many SMEs in security), the protection of small and medium sized companies with security relevant know how needs to be adequately addressed too. A European control mechanism of FDI in "strategic industries" could take into account this wider circle of relevant companies and technologies as well as the authorities that need to be consulted. Alternatively, measures at the European level could focus on a harmonization of existing legislation and a common, or at least coordinated, approach with regard to future amendments.

Export controls are regulated by Article 26.2 of the Basic Law (GG), the Law on the Control of War Material (KWKG), the Foreign Trade Act (AWG), and Foreign Trade Regulation (AWV). While any activity involving defence goods require permission by the government, only few security items fall under the KWKG. Exports of defence and security goods are regulated by the aforementioned German laws and the EU dual-use regulation. They are controlled by the Federal Office for Economy and Export control (BAFA). In 2008 it took the BAFA on average five weeks to grant an export permission, which is the lower end of time required, according to information by industry stakeholders. Companies with a workforce of about 50 employ one person specifically dealing with export applications, which is a significant burden for SMEs.

Though at the European level the export of arms and dual-use items is regulated by a legally non-binding code of conduct and a legally binding EU directive on the export of dual-use items respectively, the implementation of both differs widely among EU countries affecting the conditions for competition in the Common Market. This situation is openly criticised by some

stakeholders. Some parliamentarians are afraid that a further blurring of boundaries between security and defence will be exploited by defence companies, by circumventing the existing and tough export restriction they are subject to now. At European and national levels, information on the export license requirement should be made easily accessible; for example there could be one European portal for this type of information in all countries. While defence companies have often dedicated departments dealing with these issues the many SMEs that are common in the security industry would require some specifically tailored information from the BAFA to support their application efforts. Thus it is helpful if information about the requirements for an application are made easily accessible via the internet; they should be tailored also to a readership that has a technical and engineering rather than a commercial background; and no fees should be charged for basic information material.

Given that the products and technologies developed and manufactured by defence and security companies are often of specific interests for terrorists, companies also have to follow the UN and EU Regulation imposing certain restrictive measures directed against terrorists. For this purpose companies are required to check whether their business partners appear on a list that is annexed to these documents or that can be found at the German central bank. Given that the implementation practice differs widely among EU countries, German companies are considered to run a relatively higher risk of being subject of controls and penalties in comparison to firms from other EU countries. It is urged that a common approach with a shared level of enforcement and control is implemented at the European level.

Data protection and public surveillance laws are expected to become increasingly important for defence and security firms. The most prominent example referred to are the deployment of UAVs for the surveillance of public events or of borders. Given that Germany has had strict laws that have severely limited the use of CCTV for public surveillance, which has also restricted the CCTV market, and the countries general sensitivity to issues of data protection, the upcoming change of legislation will be hotly debated.

As for standardization and norms, the defence domain is quite advanced at national level with considerable efforts for coordination within the EU and NATO. Nevertheless the MoD faces

challenges to introduce one standard in such cross-cutting technologies and applications that need to be accepted by all services (air, land, and naval forces) such as joint C2 technology. In the security domain the issue is even more daunting, given that there are so many different procurers and customers, different time schedules and no common requirements yet. However, some norms and standards have evolved in the security domain too, such as the International Ship and Port Facility Code (ISPS) and the Automatic Identification System to identify the position of ships have been established. Given the few existing norms and standards, it is expected that they will be developed for the security domain in the next few years.

Stakeholders view standards and norms mainly positively, especially when they are legally binding. Customers are offered a larger choice. For suppliers, especially for SMEs they often present an advantage as these firms can then offer their solutions also as part of comprehensive systems and can cooperate with each other. Norms, standards, and certificates increase the market volume but often imply a reduction of the rate of return, as they lead to more competition. It is mainly large firms that are able to shape standards and norms and that might therefore gain a competitive advantage. For SMEs the participation in this process is often too costly.

At the European level, the Commission together with industry has successfully elaborated and implemented common European norms and standards for “defence related industries”. This model can be adopted and emulated for the converging security and defence industry.

In sum, the legal situation for the defence and security domains is very complex. Generally, industrial stakeholders support a European rather than national solutions, since the latter tend to impact the conditions of competition in the Common Market negatively. Moreover, only a European approach can ensure that the resulting market will be large enough to allow for scale economies that are comparable to the other large markets such as the United States, India, or China. This in turn shapes the possibilities of the Commission and European governments to influence technical norms and standards agreed in international negotiations.

Industrial interest organizations

The defence industry has only in October 2009 established a dedicated industry association: the Association of the German Security and Defence Industry (Bundesverband der Deutschen Sicherheits und Verteidigungsindustrie, or BDSV). The BDSV is part of the Association of the

German Industry (BDI) and started operating in January 2010 and replaces a number of smaller associations for subsectors of the defence industry. The declared goal of the association is to improve the defence community's contacts vis-à-vis all departments of the German government and parliament as well as at European level. This concerns particularly access to the parliamentary committee addressing financial issues ("*Haushaltsausschuss*") which also concerns itself with procurement decision and export controls.

The creation of this association does not testify to the development of blurring between security and defence. On the one hand, the founding members (Krauss-Maffei Wegmann (KMW), Rheinmetall, Lürssen, Diehl, ThyssenKrupp Marine Systems, ESG and EADS) are all large defence contractors. Though the draft statute of explicitly declares the association as an interest representation of the entire German armaments industry with about 200,000 high-tech jobs open to small and medium sized businesses. Nevertheless, it remains to be seen to what extent the BDSV will be able to attract SMEs despite the current dominance of large defence firms in the constitution and management of the association's affairs.

On the other hand, though the association includes firms from *all* subsectors of the defence industry – with EADS and ESG having strong positions in the security sector too – the BDSV did not reach out to the main players in the security industry. It seems like the fortification of the German armaments interests and a protection of their home market, since even Thales Deutschland, which is with EADS a shareholder in ESG and a firm with considerable sales in security and defence markets, has not been part of the founding team.

The suppliers of the security industry, which include corporate heavyweights such as Siemens, Bosch, Thales Deutschland, IBM Deutschland, and Deutsche Telekom, are not organized in a dedicated security industry association. They have formed the Committee for Armaments Technology within the German Electrical and Electronics Industry Association (*ZVEI*). It considers itself as an "industrial forum for the dialogue with the armed forces in order to facilitate the transfer of know-how and technology from the civil to the armaments domain". However, according to one member of this Committee, the latter has been very slow in embracing the change and in adapting to new challenges.

In recent years new associations bringing together industrial manufactures of the security and defence sector have been formed at the regional level. "Regional" refers here not to the *Laender* level but rather to a "mezzo-level" above the *Laender* and below the Federal planes. The GSW-

NRW or the Initiative Security and Armament South-Germany (ISWS) are the most significant of about a handful of similar organizations. Both have very "lean" organizational structures and no administrative personnel as they rely entirely on the honorary activity of their members.

The regional associations serve as forums for the exchange of information and experience among their member companies. They regularly organize conferences and workshops to which also end users and procurers are invited. Moreover, they represent the interests of their members towards the *Laender* Governments. GSW-NRW also has a consulting arm with own personnel and supports its members in doing business with security and defence customers.

While these organizations have focused their activities purely on the regional level, they have recently also started to establish contacts to security forums in Brussels (Interview DS, 2009). Hence, we are faced with the unique situation in which a convergence between security and defence is promoted at the European plane – ASD has extended its umbrella to the security industry – as well as at the regional plane, while the national and *Laender* levels remain "stuck" in the traditional separation of both domains.

GESA – novel interface bridging security and defence, supply and demand side

The German European Security Association was found in 2007 by Members of the European Parliament with regard to the Commission's 7th Framework Programme. At the end of 2008 GESA had 80 members recruited among parliamentarians, industrialists, scientists and researchers. The main goal of GESA is to promote „investments in the civil security sector and to strengthen the related research" at national and European level. To that end the association wants to bring together Federal and *Laender* Governments, manufacturers and research institutions at an early stage of new developments. With regard to upcoming research topics it initiates research consortia, an area where the Association has proven to be particularly successful.

GESA has not been established for the purpose of interest representation of any group. It rather sees itself as an initiator and moderator of change processes in order to overcome the continued fragmentation at national level. GESA helps to identify common interests of separate actors and to bring them together in view of future European research activities. High emphasis is put on the clarification of national interests with regard to security policy.

Consequently, GESA's working method is not to advertise its services but rather to work "quietly", allowing actors to "keep face" despite acknowledging the need to change old habits. Three

Working Groups have been set up to tackle the issues of airport security, security market, and IT-security. In addition the Association organizes two conferences a year, holds workshops and seminar and publishes Position Papers on issues of national interest. GESA forms an ideal channel of communication and engagement for the Commission at national and European levels.

4.2 Factors driving blurring of boundaries

As for industry and markets development three main drivers for convergence between security and defence can be identified. The diverse development of defence and security budgets attracts business activities from defence firms in the security markets. The German defence budget is stagnating (in real terms) and there is not much public support and political will for future increases, while the procurement outlays of the Ministry of the Interior actors have risen in recent years and are expected to keep doing so.[324] Governmental departments have not yet turned to each other in order to coordinate their demand, but companies have moved into the more dynamic market segments. As they become present in more and more pockets of the market they will be able to offer more and more solutions across the entire range of the security and defence market, thereby further contributing to the convergence. EADS, Thales Deutschland and Diehl are prime examples of how defence companies attempt to systematically enter the security market, albeit with different success and determination for continuing to do so.

Moreover, many stakeholders consider an increasingly globalised industry as a driver for the convergence of security and defence. Indeed industrial consolidation as, for example, in the market for helicopters represents a blurring on the supply side. Having said this, it has to be recalled though that the demand between security and defence procurement organizations remains uncoordinated. Technical requirements continue to differ significantly and organizational change is slow. In this context we have found evidence for blurring in the adoption of defence industrial practices by the security industry. For example, offsets as a new practice that allow security companies to export their equipment. This practice has developed despite the fact that offsets are officially opposed by German companies and by the government.

[324] How the situation will develop in face of the financial crisis and the large public debts that have accumulated could not be determined at the time of writing this report. However, there are strong signs that the budgetary situation will continue to press for a blurring of lines. See for example (Brune, Dickow, Linnenkamp and Moelling, 2010).

Finally, the activities of new organizations such as GSW-NRW and even more so GESA can be considered as a second driver for convergence. The latter's executive explicitly describes the Association as a "change agent", even though it is not always perceived as such and at times seen as a competitor by the existing interest representations. As confirmed by most stakeholders the "blurring of dividing lines" is a cultural, conceptual, and organizational issue. "The walls in the heads need to be overcome". One interlocutor deliberately used this phrase that had originally been coined in the context of German unification to describe a precondition for "growing together". As for unification, convergence mainly requires the alteration of traditional ways of perceiving security issues and the answers to them.

New kind of organizations such as GESA and to a lesser extent GSW-NRW can make an effective contribution to convergence, since they enable networking between the existing actors and their associations at different levels. These looser links are not threatening to the incumbent organizations and they are not too committing for the political actors involved but enable at the same time the formation of expert and actor communities with regard to specific issues.

4.3 Factors constraining blurring of boundaries

There are two three important factors driving the blurring of boundaries between security and defence. One constraining factor for the convergence of the security and defence industry concerns the aforementioned "difference of cultures", "languages", and "thinking" between those doing business with internal security actors and those engaged in supplying the military. These notions are also reflected in the culture of the equipment suppliers. Defence contractors aiming for the "100% solution", tend to over-design their products. This is contrary to thinking of civil customers of security equipment who are content with a "fairly reliable" working solution that is more affordable. On the other hand, defence firms have the strength that they approach issues of convergence "more systematically and strategically". They are used to "translate" global political developments into threat scenarios, consequences for defence policy and equipment requirements.

In addition to the cultural differences between different manufactures, there is also a good deal of hesitation among the established players on both sides to get together. The creation of an exclusive defence industry association in 2009 is a reflection of this hesitation. The defence

industry looks at the “newcomers” from the security industry with suspicion as they are afraid that they will have to “share a shrinking cake among more guests”. In this regard the situation differs fundamentally from that in France, where such “mingling” is welcomed by companies (Interview DT, 2009). Here the Commission could provide incentives or a forum reduce mutual mistrust and to create economic win-win situations.

Another constraint is the different legislation for the two markets, for example, with regard to the control of foreign direct investment into companies of strategic interests. It is not that security firms are any less “strategically important” than defence firms, but rather that they require a slightly different protection given the structure of the industry (many SMEs) and their technology. In addition, when a law requires the involvement of relevant public authorities – in this case the Ministry of the Interior – further incentives for convergence would be put to work. The virtual non-existence of norms and standards in the security domain is considered a major impediment for the development of the market. It can also be seen as a spoiler for the convergence with the defence domain.

Annex 5.3. Blurring between security and defence in Italy

1. Conceptual changes

1.1 Current situation

The Italian concept of defence has changed in the last 20 years as much as in the other Euroatlantic countries. It should be noted, however, the lack of official publications on the subject – for example, Italy does not yet have a national security strategy. Many information contained in the report are thus inferred from direct interviews. During the Cold war, the Italian defence concept was modelled according to the main defence challenge coming from the bipolar confrontation. The menace from the Soviet empire was a clearly defined one (both geographically and quantitatively). The defence concept and doctrines, and consequently the organization of the armed forces, was focused on the possibility of an invasion from the east or on an armed confrontation between the two poles of world power. Defence, therefore, was mainly the defence of Italy's border from aggression and/or invasion.

The end of the East-West competition did not bring about the stability that was expected. On the contrary, a number of instability drivers related to the creation of a post-cold war international order forced a radical rethinking of the old defence concept and models. Menaces to the Italian defence were not coming from one single geographical direction anymore; on the contrary, they became more diffuse and coming from multiple, often unexpected directions. The events of 9/11 further destabilized and confused the situation, projecting terrorist groups in the arena of the major international players and adding an additional layer of unpredictability on the system.

The new menaces are now not exclusively based on armaments; the instruments and tools of a potential threatening entity are diversified and include phenomena such as organized crimes, money laundering, illegal trafficking of drugs, weapons, human beings, etc.

The instruments that can be used to undermine the security of the state forced a rethinking of the national defence. Today's challenges are more complex than yesterday's and require an equally

complex and diversified posture. The consequence, explicitly recognized by the 2001 White book on defence, is that the traditional defence tools (first of all the armed forces) need to acquire greater "operational flexibility": besides the traditional and constitutional missions, armed forces are asked to concur to international security and stability and to contrast violation of human rights and of peace. In this respect, armed forces will have to work side by side with civilian agencies in order to satisfy not only defence.

1.2 Factors driving blurring of boundaries

According to the 2002 White book on defence, the last of such official documents produced so far, the fall of the Berlin wall and the 9/11 attacks on the US have been the events that radically changed the global strategic scenario and pushed for a new concept of national defence. The changing strategic scenario should therefore be considered the first and most important driver responsible for the growing blurring between the concepts of security and defence in Italy[325].

This trend, moreover, has been reinforced by the need to include the defence of Italian interests and security in the wider framework of the international community, especially of the European Union. Italy fully embraced the EU security concept, which is centred on the need to answer to the challenges of failing and failed states, proliferation, regional conflict, terrorism, etc.

It should be also underlined that Italy's perception of the blurring between security and defence is heavily influenced by historical factors. The Carabinieri, a militarized police force, was founded in 1861 and represents an example of blurring *ante litteram*; or, even better, is a remnant of an age when military forces were also responsible for public order. Moreover, the Italian experience in dealings with international and internal terrorism (as, for example, the fight against radical left wings formations such as the Red Brigades) facilitated the transition from the traditional defence concept to today's more complex and blurred conception. Italian security and defence forces leaders, as well as political leaders, were forced to utilize different and combined security and defence tools in order to repress terrorist movements. The experience represented an example of blurring and paved the way for the successive conceptual development.

325 Libro bianco 2002, Ministero della difesa, pg. 14

1.3 Factors constraining blurring of boundaries

A potential driver against blurring should be considered the bureaucratic culture of division. The Italian security and defence establishment, as well as the Italian public administration in general, is highly fractionalised (see chapter on organizational issues). The structural fractionalization of institutions naturally leads to the developments of different concepts of security and defence that are typical of the individual bureaus, and practically act as a spoiler for the development of a common vision of blurred concepts of defence and security.

2. Organizational issues

2.1 Current situation

The Italian security and defence organizations are characterized by: a) a degree of blurring between security and defence functions of the armed forces, and b) a high level of fractionalisation, both at low and at high level. Different branches of the armed forces permanently perform civilian tasks, while all the armed forces are constitutionally tasked with contributing to civilian security in cases of natural or man-made disaster or emergencies. However, the fractionalization of security and defence organizations even at the command level (different forces depending from different institutions) represent a factor against the blurring of security and defence functions.

Italian Security forces
National Police
Provincial Police forces
Local (city) police
Carabinieri
Guardia di Finanza
Guardia Costiera
Vigili del Fuoco (Fire brigade)
Protezione Civile

2.2 Factors driving blurring of boundaries

The most evident example of the blurring from the organizational point of view is the Carabinieri corps, which since 1922 was defined as an "armed force in permanent public security service". The Carabinieri corps has been formally nominated as the fourth Italian armed force (after the Army, the Navy and the Air force) in March 2000, with the law n. 78. The dual nature of the current Carabinieri's role seems to be determined by historical reasons: it has to be noted, however, that the public security activity of the Carabinieri gives the corps some skills and flexibility very useful in peacekeeping and peace enforcing missions abroad.

According to the law, the Carabinieri corps shall fulfil: a) military tasks such as national defence, participation to international missions, military police functions, security service for Italian diplomatic missions: b) civilian tasks such as permanent public security service and participation to civil protection activities in the event of calamities. Because of these tasks the Carabinieri corps, while dependant from the Ministry of defence, operates under the Ministry of interiors for its civilian tasks. Moreover, Carabinieri detachments work under the authority of other ministries such as the Ministry of Health, the Ministry of the Environment, the Ministry of Labour, and others.

The Carabinieri corps is not the only armed force permanently tasked for civilian missions. The Italian Coast Guard, a corps within the Italian Navy, carries out mainly tasks connected with the civilian use of the sea, such as search and rescue, navigation security, controls on fisheries, maritime police, and environment protection. The Coast Guard is functionally dependent from the civilian ministries connected with its tasks, first of all the Ministry of Transport and Infrastructures.

Another relevant military organization with civilian tasks is the *Guardia di Finanza* (Revenue Guard Corps), founded in 1881 as an integral part of the armed forces with the task of border control and defence. Today, the Revenue Guard Corps is integral part both of the armed forces and of the public security forces. However, it is not dependant from the Ministry of Defence neither from the Ministry of Interior: it is dependant from the Ministry of Finances. It is a police force, organized

along military lines, with general responsibility over economic and financial matters, and it also has exclusive competence over financial and economic offences at sea.

However, even the other branches of the armed forces do fulfil civilian tasks, even if not on a permanent basis. The armed forces are institutionally tasked with security missions. The 2002 White Book on defence explicitly foresee the involvement of the three other armed forces in a wide range of civilian activities (the first time the armed forces were authorised for such activities was in 1978 with the law n. 382).

Under request from the competent civilian authorities, if the same authorities do not have the necessary resources for a particular intervention, military forces can be involved in: relief interventions after a natural disaster, so-called "safeguard of the free institutions" (meaning public security in major security crisis such as those provoked by organized crime or huge waves of clandestine migrations), interventions of public interest (restoration of road and railways networks, water supply to small, isolated islands, demolition of unauthorized buildings, etc.). Armed forces intervention in civilian roles is thus motivated by a lack of capabilities of civilian authorities and forces, and conversely by the high level of efficiency that the armed forces are considered to have.

Since the beginning of the 1990s, the Army has in effect been extensively used in Italy. In the first major operation, "Vespri siciliani", the Army was tasked of surveillance of public buildings in Sicily, allowing police forces to use all of their personnel for investigative actions against organized crime. Five other major public security operations followed "Vespri siciliani", involving thousands of troops. Moreover, the Army was also involved in 6 major disaster relief operations after earthquakes and floods in Abruzzo, Campania, Umbria, Calabria, Sicilia, northern Italy. In the last years, Army detachments has also been used for surveillance of waste disposal plants during the Naples' trash crisis of 2008 and the Palermo crisis in June 2009, while Navy units have been used to contrast illegal immigration at sea.

The main civil security organization in Italy is the *Protezione Civile*, which is actually a network of central, regional and local volunteers organizations. Its tasks are to protect the population, the

cities and the environment from natural or man made disasters. The role of the regions is fundamental, as according to the Constitution civil protection is considered a regional competence. [326] The *Protezione Civile* activities, however, are coordinated from the Presidency of the Council of Ministers, adding a further actor involved in security besides the Ministry of Interior and the armed forces when acting in civilian roles.

2.3 Factors constraining blurring of boundaries

Some stakeholders criticised what they perceived as an instrumental use, by the government and for mainly political reasons, of the armed forces for tasks which are not their own. Doubts were raised because of the possible degradation of the capabilities of the armed forces, forced to spend resources on missions that should be performed by others. However, the issue of capabilities degradation could in the future become a driver against the use of armed forces for security tasks (this will not be the case of those forces which have a dual nature, like the Carabinieri or *Guardia di Finanza*). The probability of resources degradation could be higher especially if coupled with a shrinking defence budget or an increase in the armed forces' missions abroad, which would put additional strain on men and equipments.

Another drivers against the blurring of security and defence at the organizational level may be the fractionalization of the different institutions which control the different branches of the armed forces and the security agencies. As it is often the case, the different ministries will probably resist, in some way, to any attempt top streamline the various organizations under the same umbrella, in order not to lose a significant asset and the consequent resources. Given the size and strength that Italian bureaucratic organizations seems to retain, the problem of fractionalization may prove to be a significant driver.

The same issue of fractionalization can be detected also at the geographical level. As already said, Italian security agencies are highly fractionalised between the national, regional, provincial and local level, with different institutions playing the leading role for different forces (for example, police forces are directed at the national level, while *Protezione Civile* at the regional one). This kind of fractionalization damages the emergence of a common culture just as much as the

326 Constitutional Law 18/10/2001, n.3.

institutional one, thus acting as a spoiler for the convergence of security and defence organizations.

3. Technological developments

3.1 Current situation

There appears to be a situation of a growing convergence between security and defence technologies in some sectors. Different factors contribute to favour the research and development of dual use technologies; however, there remain differences in requirements that limit this development.

3.2 Factors driving blurring of boundaries

Italy's shrinking defence budget represents a driver in favour of the blurring of security and defence technologies. The Army Military Staff's own R&T detachment is very often involved in the development of dual use technology projects, also because the wider dimension of the civilian market allows the possibility to create synergies with more partners (privates or Universities).

Examples of defence programs with relevant security applications
HELIOS space-based earth observation program
COSMO – SKYMED explicitly dual use earth observation program
SICRAL satellite communications program
C4I different communications and systems programs
ESSOR European security software radio program, to develop interoperability with civilian systems
WIMAX to allow civilian users access to military radio and radar systems

The defence industry (first of all, obviously, the Finmeccanica holding) also has a crucial role for development of new technologies and particularly dual use technologies. Selex Sistemi Integrati, a Finmeccanica company which develops integrated defence and security systems, invest around

20% of its production value in research and development.[327] Another Finmeccanica company, Selex Comunicazioni, had a value of production of 754 million euro in 2008, with a total R&D investment of 87.4 million (around 12.5%).[328]

Common technological requirements for security and defence missions also may be a driving factor of blurring. However, it is not clear how much the requirements are actually shared. Some areas such as communication may well be apt for a common security-defence requirement (hence the number of space-based communication systems developed by the MoD).

Another driver could be the faster rate of obsolescence of technology, which is constantly increasing. The shorter "life" of a technology is an incentive for the producing industry to maximize profits by enlarging the market, and therefore enter into different market segments. Faster rate of obsolescence also means growing sophistication of security technology, which is becoming qualitatively closer to that of the defence goods, thus providing and additional stimulus for expanding production and investments towards dual use or security technologies.

3.3 Factors constraining blurring of boundaries

A major driver against blurring, or at least a factor that does not allow the development of blurred technologies beyond a certain limit, is the difference in requirements between civilian and military technologies. While at the lowest technology readiness levels there can be minimal or no differences between civilian or military oriented technology, the final product for military use may have significantly different requirements in terms of increased performance and reliability, or smaller dimensions. These requirements may prove to be redundant for the civilian security use, adding additional costs.

A further factor may be the fact that, even in a growing technology blurring scenarios, there remains some technological areas which are of specific military interest. Technologies linked to

327 Selex Sistemi Integrati Key figures 2008
328 Selex Communications Key figures 2008

heavy weapons systems (warplanes, artillery, war vessels, armour) may find no place in a security market.

4. Industrial and market developments

4.1 Current situation

The defence market in Italy is dominated by the Finmeccanica holding, which is the third largest defence company in Europe after EADS and BAE, and the eight in the world. The company, which controls a number of Italian defence firms such as Oto Melara and WASS, boasted more than 13 billion sale proceeds in 2007 (including revenues from non-defence related sectors such as civil aviation). In the defence field, Finmeccanica is active in the defence system business (armoured vehicles, torpedoes and counter-torpedo systems, missiles).

The company, however, is also active in the security field. Selex Sistemi Integrati, a Finmeccanica company, designs complex defence systems which are mostly dual use: they include port surveillance systems to protect port infrastructures, advanced air surveillance radars, vessel traffic management systems, and C4I system facilities. Selex Sistemi Integrati was created in 2005 after Finmeccanica took over the Anglo-Italian joint venture AMS. Also other firms of the Finmeccanica holdings are very active in the security field. Selex Comunicazione develops and supplies multi-access broadband communication solutions; it produces portable satellite terminal, TETRA radios, airborne radio-communications equipment, while Elsag builds, beyond other products, mobile systems for fingerprint collection (specifically designed for police use), and an integrated system to monitor logical access to the information system.

Table 1: Italian defence companies revenues in 2007.

Company	Defence revenue	Total revenue
Elsag Datamat*		633
Alenia Aermacchi*	84	200
WASS*	105	105
Thales AS – Telespazio*	587	587
Oto Melara*	273	273
Iveco DVD	400	400
MBDA Italia*	415	415
Elettronica	291	291
Selex Sistemi Integrati*	412	571
Avio	413	1553
Fincantieri	484	2673
Selex Comunicazioni*	653	787
Alenia Aeronautica*	1298	1671
Selex S&AS*	486	550
AgustaWestland*	687	1727
Finmeccanica	7198	13429

Source: G.Gasparini, L. Marta, V. Briani. Data on defence economics and industry. *: Finmeccanica controlled company

On the defence demand side, the main and only customer is the Italian Ministry of Defence. In 2009, the Ministry budgeted 2.885 million euro for investments in equipments (which includes both financing for programs previously accepted, resources for renovations and new acquisitions). It has to be noted that some of the more expensive programs, such as the Eurofighter, FREMM frigates and some high technology aerospace and space programs, are also funded by the Ministry of Economic Development. The Ministry of Defence budget for investments appears to be constantly shrinking: from 2008 to 2009, investments were more than 20% lower. Current MoD investments are focused on the following capabilities: command, control communications, computers, intelligence-surveillance and target acquisition (C4-ISTAR); mobility and deployment; force protection and precision of engagement; logistical; scientific research. Many of those capabilities, judged by the MoD to be central for more modern Italian armed forces, are clearly

based on dual use technologies, and are developed by the MoD in partnership with civilian entities (research institutes, foundations, companies). Indeed, some of the programs aim explicitly to link military and civilian actors: for example the program ESSOR (European Security Software Radio) aims to achieve interoperability not only between European and NATO countries but also with civilian agencies.

Table 2: Italian total defence-related spending in 2009

	Defence function	Carabinieri[329]	International missions[330]	Ministry of Economy	TOTAL
Personnel	9.566	390	868		10.828
O&M	1.888	20	372		2.280
Infrastructure	324				324
Equipments	2.158[331]			888[332]	3.046
R&D	224			400	624
TOTAL	14.160	414	1.240	1.288	17.102

Source: G.Gasparini, L. Marta, V.Briani, Data on defence economics and industry, 2009.

Apart from large companies such as those of the Finmeccanica group, the Italia security sector supply side is rich with small and medium enterprises whose customers are often individuals and small industries. However, there is currently a lack of reliable and available data about the size and volume of the security industry in Italy. Security companies are not considered a category on their own, except the relatively limited sectors such as security and buildings automaton or private security agencies. For example, IT technology and informatics security companies are considered part of the informatics industry, and so on. The bulk of the companies which contributed to the security goods production are thus excluded from official statistics such as those provided by the Istututo Nazionale di Statistica (ISTAT) or from the industry associations study centres, as they probably figures in other categories (i.e. electrical engineering, electronics, constructions).

329 Estimate based on the number of Carabinieri personnel available for defence missions, military police: about 8.300 on 110.000 men total

330 Estimate based on doubling funds provided just for the first semester; historic series: personnel costs 70%, other 30%

331 Excludes 179 million euro to substitute radars due to the WIMAX frequency transfer

332 Eurofighter program

The main security companies association, *Confindustria* ANIE, is only composed by buildings automaton, private security agencies associations, and fire-fighting equipment firms. The Italian security sector seems to be in constant growth since 2006, even if 2009 may be a more difficult year because of the economic crisis. According to *Confindustria* ANIE, the security market in Italy is worth 1.8 billion in 2008 (+5.9% compared to 2007), with an aggregated output of 63 billion. Security companies seem to be very competitive on the international market: exports grew by 3.7% with 200 million euro. The access control sector is one of the most promising areas and represents 40% of the security market. Goods such as airport passenger and baggage screening equipment, scanning equipment, biometric identification and CCTV systems all have great sale performances. Other products with great potential are those connected with home security such as anti-intrusion systems, burglar alarms and other automated home protection solutions.

From the demand side, the Ministry of Interior is the main buyer of security goods (being in charge not only of the police forces but also of the Fire brigade and the civil defence). The Ministry of Interior 2009 budget (taken from the 2009 definitive state budget) includes 13.345 million euro for "technical and special instruments and material", which should include most of the security goods utilized.

The budget lists 1.830 million euro for "special-use motor vehicles", 62.961 million for normal and 19.770 for heavy motor vehicles. 7.273 million are budgeted for aerial vehicles, while 1.494 million are for maritime vehicles. Ordinary maintenance charges for all vehicles are budgeted 66.572 million euro. The budget for light arms is 2.450 million.

Regarding IT technology, the Ministry has 4.372 million euro for all-around information technology (including systems needed for administrative tasks), with 4.5 million euro for assistance and around 12 million for ordinary hardware and software maintenance. As for communications, the Ministry spends 15.127 million for communications networks.

Regarding civil security, the Ministry has a budget of 45.331 million euro, assigned to the Fire brigade, the *Soccorso Pubblico* and the *Protezione Civile*. Some of the funds are going to be used to improve the functional autonomy of the civil defence HQ trough the acquisition of better logistics, IT technology and telecommunications (also satellite communications).

4.2 Factors driving blurring of boundaries

The Italian defence market has been steadily contracting since the 1990's, after the fall of the Berlin wall. This is reflected in the constant shrinking of the MoD budget. As a stakeholder put it, "there is no war anymore", means that war in the traditional sense is not the main security challenge for a state: indeed, it can be considered, at least for Italy, not a possible event at least in the short term period. Clearly, this change of perspectives led to a contraction of orders for goods and technologies that are utilized for traditional warfare (such as armour, fighter planes, etc.). This led the MoD to maximize, when possible, the use of civilian and security products.

A further factor that may have been contributing to the decrease in volume of the market for defence goods, and thus encourage defence industry to shift or diversify into the security market, is the rising costs for modern technology. Modern warfare equipment tend to be state-of-the-art and extremely expensive, while states (the only customers for complex armaments systems) tend to have more and more limited funds to allocate to defence.

Finally, the new missions assigned to the armed forces often require a more security oriented equipment. In operations such as peacekeeping and peace enforcing missions, security equipments play a much greater role than they usually play in a pure combat environment, where the emphasis is on offensive capabilities.

4.3 Factors constraining blurring of boundaries

Regulations and rules for arms procurement represent an evident driver against the blurring of security and defence industries. On one side, security companies wishing to enter into the defence market are discouraged from doing it, because of the necessity to adapt to strict requirements; on the other side, small companies that are already into the defence market may find the existence of the very same regulations a stimulus not to expand into other market, for fear of losing the advantage of operating into a "protected" market.

Moreover, even the involvement of military actors in peacekeeping operations abroad does not seem to have the expected impact on the demand. Military actors, in fact, tend to prefer the use

of defence-origin products even in low intensity situations, as they expect to run the risk of combat.

Annex 5.4. Blurring between security and defence in the United Kingdom

1. Conceptual change

1.1 Current situation

At the conceptual level, there is a growing acceptance within the UK government of a blurring of the distinction between "defence" and "security". The UK's view of national security has broadened over recent decades to include threats to individual citizens and their way of life as well as the more traditional concerns about the integrity and interests of the state.

This view is best reflected in the UK's *National Security Strategy*. This was published in March 2008 and updated in 2009 and was the first time that the UK had published a single, overarching strategy bringing together the objectives and plans of all government departments, agencies and forces protecting national security, including both defence and security. The aim of the *National Security Strategy* was to set out how the UK government would address and manage diverse but interconnected security challenges and drivers, both immediately and in the longer term, would seek to safeguard the nation, its citizens, its prosperity and its way of life. The *National Security Strategy*, for the first time, put terrorism formally in the wider context of other threats to the UK and its people and broadened the scope of national security to look at the risks to the UK from terrorist, criminal, man-made and natural disasters.

This changed thinking about the nature of national security on the part of UK government is expressed in the following passage from the *National Security Strategy* that says:

"In the past, the state was the traditional focus of foreign, defence and security policies, and national security was understood as dealing with the protection of the state and its vital interests from attacks by other states. *Over recent decades, our view of national security has broadened to include threats to individual citizens and to our way of life, as well as to the integrity and interests of the state.* That is why this strategy deals with transnational crime, pandemics and flooding – not part of the traditional idea of national security, but clearly challenges that can affect large

numbers of our citizens, and which demand some of the same responses as more traditional security threat, including terrorism".[333]

This changed thinking recognises the need for a blurring of the defence-security distinction. A central theme of the *National Security Strategy* is that there can be no simple division between defence and wider security or domestic and international considerations. The *National Security Strategy* says:

"The distinction between 'domestic' and 'foreign' policy is unhelpful in a world where globalisation can exacerbate domestic security challenges, but also bring about new opportunities to tackle them. Similarly, *the traditional contrast between 'hard' and 'soft' power obscures recent experience of post-conflict stabilisation, which shows success in building security depends on political and economic development*".[334]

1.2 Factors driving blurring of boundaries

A number of factors can be seen to be driving this blurring of the conceptual boundaries between defence and security.

On the defence side, the experience of UK military personnel deployed in Bosnia, Kosovo and other operations during the 1990s had an important influence upon thinking within the military and the Ministry of Defence. These experiences demonstrated that post Cold War conflicts involved a complex interplay of civilian paramilitary and military groups and individuals, international organizations and the mass media. The conflicts were driven by a complex range of factors and it was recognized that military instruments alone could not effectively deal with them but that they required the engagement of other Government departments and Non-Governmental Organizations.

In this spirit, the 1998 *Strategic Defence Review* noted that this new security environment required the combined application of all the means at the disposal of the UK government. Thus, whilst military action may be one means of achieving national security objectives, it is unlikely to be sufficient on its own. Thus, the *Strategic Defence Review* argued, the UK required armed forces which could operate in support of diplomacy alongside economic, trade and developmental levers,

[333] *The National Security Strategy of the United Kingdom*, March 2008: 3-4.
[334] *The National Security Strategy of the United Kingdom*, March 2008: 8.

to strengthen security and avert conflict as well as conducting effective military operations if required.[335]

On the security side, there has been a growing recognition that the character of the international terrorism threat faced by the United Kingdom is blurring the boundary between military action and security. The UK Government has sought to justify the UK's on-going commitment in Afghanistan in terms of its importance as the "front line" in protecting the United Kingdom from international terrorism. Thus, military action against the Taliban is seen as necessary to protect UK domestic security and – at the same time - the security services and antiterrorism police are engaged in intelligence gathering activities to assess the intentions and capabilities of potential Islamic terrorist groups to attack the United Kingdom mainland.

1.3 Factors constraining blurring of boundaries

The *National Security Strategy* has been broadly welcomed within government as a necessary conceptual response to the changing security environment. During our interviews, the point was made to us that the significance of the *National Security Strategy* is that it signalled the intent at the highest political level to state a new concept of national security in which defence becomes a sub-set of a wider concept of national security. Nevertheless, it ought to be added that there are some factors that have constrained the rate at which this blurring has occurred. In particular, institutional and cultural inertia is a constraint on the rate of change. The *National Security Strategy* represents a different conceptual approach and a challenge to traditional thinking both within the defence and security communities. Whilst it has been embraced in some parts of the national security architecture it has been treated with some suspicion elsewhere not least because it challenges established ways of working and thinking about national security.

2. Organisational issues

We now turn to consider what, if any, evidence we can find for a blurring of the organisational boundaries between defence and security in the UK. This section considers three aspects of the organisation of government: the organisational structures that underpin defence and security

[335] *Modern Forces for a Modern World*, Strategic Defence Review, 1998.

policy making; the organisation of the procurement of defence and security equipment; and the organisation of government R&D for defence and security missions.

2.1 Current situation

Organisationally, there remain important distinctions between defence and security in the United Kingdom. There are different budgets, different organizational structures and different cultures. However, whilst they remain organizationally distinct, we can identify efforts to enhance organizational cooperation between defence and security.

Before considering these matters it is important to understand the complex and multi-organizational character of the governance of civil security in the UK. Placing defence to one side for a moment, it should be noted that there are a multitude of organisations and agencies that have responsibility for different aspects of UK security policy and procurement. In the United Kingdom, no single Government department or agency is responsible for national security and the following is a list of some of the most important:

- **The Home Office** is responsible for counter-terrorism policy, and the lead for domestic security lies with the civil agencies – and particularly with the police.
- The Government's Counter Terrorism Strategy (CONTEST) is led by **the Office of Security and Counter Terrorism (OSCT)** in the Home Office. OSCT was established in Spring 2007 to manage the cross-government counter-terrorism effort.
- The **Cabinet Office** provides direct counterterrorism advice to the Prime Minister, provides the secretariat for the Ministerial Committee on National Security, International Relations and Development and facilitates the coordination of the Government's response to terrorist and other national security incidents via the Cabinet Office Briefing Rooms (COBR(A)).
- The **Civil Contingencies Secretariat** of the Cabinet Office coordinates the national Resilience Programme for dealing with civil emergencies, which encompasses coordination of the *Prepare* strand of the UK counterterrorism policy CONTEST. The Civil Contingencies Secretariat was originally set up in July 2001 in response to several crises in 2000 (including

fuel protests, the outbreak of foot and mouth disease and severe flooding), but was given a new impetus after the September 11 attacks.

- **HM Revenue and Customs** which reports to the Chancellor of the Exchequer has lead responsibility for detecting prohibited and restricted goods during import and export, including those goods that may be used by terrorists.
- The Department for Transport's **Transport Security and Contingencies Directorate (TRANSEC)** is responsible for the security of the travelling public and transport facilities through regulation of the aviation, maritime and railway industries.
- The **Health Protection Agency,** a non-departmental body responsible to the Secretary of State for Health, was established in 2003 to help provide a coordinated and consistent public health response to a range of national emergencies, from a disease outbreak to a terrorist attack.

Within the machinery of government, the Ministry of Defence contributes to the cross-government and cross-agency bodies that coordinate national security matters. Those bodies include the Joint Terrorism Analysis Centre (JTAC) which was established in 2003 to bring together expertise from the police, intelligence agencies and 16 departments including the MOD. There are representatives of the MOD and the military on the COBR(A) committee which coordinates the Government's response to terrorist and other national security incidents. The Ministry of Defence and the military also provide specialist capabilities and knowledge that are used by civil security departments and agencies. For instance, the MOD's Defence Science and Technology Laboratory (DSTL) provides specialist science for policy advice in the CBRN field.

Operationally, defence plays a supporting role to the civil authorities who lead the domestic response to security issues within the UK. Any support provided by the Armed Forces, and especially the use of force, must be at the specific request of the civil authorities through the principle of Military Aid to the Civil Authorities (MACA). Defence support can be provided where the responsible civil authority lacks either the capability or the immediate capacity to deal with a situation. Defence support is normally the last resort, with mutual aid or commercial options having first been exhausted. The Ministry of Defence is also the provider of a number of specific and unique capabilities for domestic security and resilience. The MOD provides: an Explosive Ordnance "render safe" capability; a regional command and control capability to provide ability to

co-ordinate larger scale defence contributions; and Civil Contingency Reaction Forces, drawn from the reserve forces, which are potentially available if required to support the responsible authorities for dealing with civil contingencies.

Organisationally, therefore, the Ministry of Defence and the military cooperate at both the policy and operational level with government departments and agencies that are responsible for civil security. However, it ought to be stressed that defence and security remain organisationally distinct. This also holds for procurement. The procurement of equipment for the military and for civilian agencies is undertaken by different bodies with different budgets. In the case of the Ministry of Defence, procurement is undertaken by the MOD's Defence Equipment & Support organisation. On the civil security side, the situation is a great deal more complex with procurement budgets and organisation spread across a variety of organisations in both national and local government. For instance, whilst some aspects of CBRN equipment for police forces are provided centrally by the Home Office, in other cases procurement of equipment is undertaken separately by each of the 43 police forces in England and Wales. Indeed, the CBRN field is one of the only areas where there are clear efforts at coordination of development and procurement efforts between defence and civil security (the Home Office).

There is some evidence of blurring in the field of scientific and technological advice to government. Formally, the Home Office Scientific Development Branch (HOSDB) provides advice and operational support for the Home Office and its partners on any issue relating to science and technology as well as supporting the development of new technologies in counter terrorism, border security and identity management. However, the Ministry of Defence through its Defence Science and Technology Laboratory (DSTL) holds some of the UK's leading expertise in CBRN and explosive materials. Building on those capabilities, a MOD Counter Terrorism Science and Technology Centre was established and – whilst its primary mission is to support the counter terrorism technology needs of the UK armed forces – it has provided scientific and technical advice and support to the civil security department and agencies. At the same time, the DSTL's Porton Down facility has the UK's only facility for testing suspected chemical or biological weapon materials and in the area of CB terrorism DSTL supports civil security agencies through an incident support service and testing facilities for suspected CB materials.

This discussion has focused on the contribution of defence to civil security. Equally, there are organisational relationships between civil departments and agencies and defence. Thus, in line

with the Comprehensive Approach, there is close cooperation between the Ministry of Defence, the Foreign & Commonwealth Office and the Department for International Development (DFID).

2.2 Factors driving blurring of boundaries

Organisationally, defence and security remain distinct but we can see closer organisational cooperation and increasingly intense working relationships in some areas. A number of factors can be seen as driving that closer cooperation.

On the one hand, the Ministry of Defence has specialist knowledge and capabilities that are needed to tackle civil security challenges within the UK. In the previous section, we noted that the MOD's Defence Security and Technology Laboratory possesses unique capabilities in the chemical and biological field that are used extensively by the Home Office. It also provides scientific advice and assessments to the security policy making process.

On the other hand, the new concepts used in overseas operations – and especially the Comprehensive Approach – are driving closer cooperation between defence and security organisations with the police and the Department for International Development (DFID) providing specialist knowledge and capabilities needed for operations abroad.

2.3 Factors constraining blurring of boundaries

The new concepts of operations signalled by the Comprehensive Approach as well as the capabilities required to meet civil security missions within the UK may be leading towards closer cooperation but this closer cooperation has presented significant challenges. There are a number of factors that are constraining this form of organizational blurring.

The organizations have different missions and different priorities and are experiencing overstretch. A particular problem is that the UK's commitments in Afghanistan are placing an enormous strain on the Ministry of Defence and the military in some areas. For instance, the MOD has become increasingly concerned about the use of the Counter Terrorism Science and Technology Centre as a cross-government resource. In part this because it is anxious about cross-government sharing of knowledge and capabilities with respect to CBRN but it is also increasingly concerned to ensure that the efforts of the CT Centre are focused on operational requirements in Afghanistan and the support of troops in the field.

Organisations operate with different budgets. The Ministry of Defence has a separate budget from the Home Office and other departments and agencies with civil security responsibilities. Consequently, budget considerations can act as a constraint on closer organisational cooperation. A single security budget has been introduced by the Government but at the time of writing it was unclear as to the impact of this development. It appears as if the single security budget represents little more than the identification of total budgets across government for national security. However, there is no central allocation of resources for national security. Consequently, this acts as a constraint on closer cooperation.

Bureaucratic politics and inter-departmental rivalries also act as a constraint on blurring. Greater involvement of the Ministry of Defence in domestic security missions has always been resisted by some civil security agencies (not least the police). Equally, efforts to promote greater cooperation by the Home Office's Office of Security and Counter Terrorism (OSCT) have been viewed with suspicion within parts of the Ministry of Defence who have seen as an attempt at "centralization" of powers within the Home Office.

A final important constraint is legal and political. The role of the military in domestic security missions has always been tightly specified and is governed by the principle of Military Aid to the Civil Authorities (MACA). Equally, there are political sensitivities about the appropriate use of the military within the UK.

3. Technological developments

In the Chapter on technology in our report, we have pointed to technology as one of the main drivers of the blurring of the dividing lines between security and defence. In this section, we examine technology developments in the United Kingdom and note that there is evidence of a blurring between defence and security in some technologies and in particular some common applications of technologies in fields such as CBRN and Information and Communication Technologies.

3.1 Current situation

In August 2009, the UK government published *The United Kingdom's Science and Technology Strategy for Countering International Terrorism*. This provides a great deal more information on

the UK's strategy and research priorities than was previously available. The document explains that the strategy has three principle objectives:

- To use horizon scanning to understand future scientific and technical threats and opportunities and inform our decision making on counter-terrorism.
- To ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority science and technology requirements.
- To enhance international collaboration on counter-terrorism related science and technology.

The strategy also identifies some of the key counter-terrorist challenges that the UK will need to address in the next few years and where science and technology are likely to be vital. The challenges set out in the document are:

- Understanding the causes of radicalisation;
- Protecting the national infrastructure;
- Reducing the vulnerability of crowded places;
- Protecting against cyber terrorism;
- Improving analytical tools;
- Identifying, detecting and countering novel and improvised explosives;
- Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) threats.

Although there is still no publicly available statement of UK central government budgets for security science and technology, the document does reveal that the UK's cross department science and technology programme to strengthen the UK's ability to respond to a CBRN attack has a budget of around £10 million a year and includes more than 50 projects.

CBRN is one field in which there is a clear blurring of the dividing lines between security and defence. We have already noted how there is some evidence of blurring in the field of scientific and technological advice to government on CBRN matters. The cross department science and technology programme on response to a CBRN attack is further evidence of some blurring. Information and communication technologies (ICTs) are another area of blurring. The growing emphasis on military transformation through Network Enabled Capability means that information and communication technologies (ICTs) are increasingly critical to the UK military. The security of those ICT systems is becoming a critical concern for the Ministry of Defence and as a consequence

civil-security origin technologies and enterprise security-origin technologies have growing defence applications. These include information security technologies. [336]

3.2 Factors driving blurring of boundaries

A first point to make is that generic technologies are increasingly critical to most defence and civil security products and systems. Since the 1980s, dual-use and civil origin technologies have assumed growing importance in the defence sector, reflecting the growing size and increasingly technologically sophisticated demand of consumer in the electronics and industrial goods markets.[337]

The fact that both defence and civil security products rely heavily on generic and globally available technologies, not least information and communications technologies (ICTs), can be seen as a powerful driver of "blurring". ICTs in particular are increasingly pervasive and are revolutionising the manner in which organisations (both public and private) are able to address their security needs.[338] Thus, both defence and civil security in the UK have common technology interests in enhanced communications, situational awareness, data collection, analysis and storage and so forth.[339] Concerns about CBRN terrorism mean that the security sector requires CBRN detection equipment, protective clothing and decontamination equipment.

There are increasing efforts to promote synergies between defence and security research in some technology areas with CBRN leading these developments. The MoD's Counter-Terrorism Science and Technology Centre plays an important role in ensuring MoD investment in a range of research and technologies assist wider counter-terrorism requirements although – as will be noted – there have been some MOD sensitivities to the role of the CT Centre in supporting civilian security requirements. In the CBRN field, the UK Ministry of Defence and the UK Home Office are engaged in deepening cooperation. This is seen as a mean of transferring technological knowledge from the MoD's Defence Science & Technology Laboratory to the civil security sector. Sensitivities over the transfer of knowledge in this field mean that developments have been cautious, but CBRN is seen

[336] *Defence Technology Strategy*, 2006, Ministry of Defence: London.
[337] John A Alic, Lewis M Branscomb, Harvey Brooks, Ashton B Carter and Gerald L Epstein (1992) Beyond Spin-Off: Military and Commercial technologies in a Changing World, Boston: Harvard Business School Press.
[338] ESRAB, *Meeting the Challenge: the European Security Research Agenda*, Brussels, 2006.
[339] *Defence Technology Strategy*, 2006, Ministry of Defence: London.

as a lead-area that may be used as a model for broader technology cooperation between MoD and the Home Office.

The defence technology strategy of the UK Ministry of Defence has increasingly sought to find ways of accessing civil origin technologies and spinning-in technologies from these increasingly globalised markets. There is an acceptance by the Ministry of Defence of the considerable advantages in integrating technologies from the civil and enterprise security sectors into current and future programmes. This is seen as providing a mean of spinning-in technologies and systems engineering experience developed by the enterprise security sector from working on large private sector projects in the financial sector, retail sector and elsewhere. [340]

3.3 Factors constraining blurring of boundaries

There are, however, a number of factors that are constraining the blurring of boundaries between defence and security technologies.

Much of the enterprise security sector is characterised by an "open innovation" approach where companies source technologies in global markets based on their cost and performance. These technologies are sourced in what are in effect open and global markets from companies who are not under the same controls and scrutiny of Ministries of Defence as are traditional defence contractors.

Thus, concerns from defence and high-end security users about security of supply and technology integrity have constrained the rate at which some enterprise security technologies have been adopted. Specific technology solutions are still required in some areas. The most important of these areas is software, particularly for safety critical and other high integrity applications, and information management and information assurance.[341] Thus, defence-specific development programmes and suppliers remain in some areas.

There have also been Ministry of Defence concerns over the transfer of CBRN technological knowledge to non-defence agencies as well as tensions over the role of the MOD's Counter Terrorism Science and Technology Centre in civil security activities.

[340] *Defence Technology Strategy*, 2006, Ministry of Defence: London.
[341] *Defence Technology Strategy*, 2006, Ministry of Defence: London.

In addition, the rate and character of the transfer of technology between defence and security and vice versa is influenced by a variety of adoption factors related to the character of the market and industry. It is to these matters that we now turn.

4. Industry and market developments

We now turn to consider the extent to which we are observing a blurring of the defence and security industries and markets in the United Kingdom.

4.1 Current situation

By way of background, UK defence procurement spending amounts to around £16 billion a year of which £7 billion is spent on military equipment and R&D and £9 billion on maintenance, spares and upgrades, IT and communications and facilities management.[342] The UK public security market was estimated to be worth around £800 million in 2008 and one market research report estimates that what it calls the UK homeland security market is likely to be worth £5.4 billion in total between 2008-2016.[343] As such, the UK homeland security market whilst sizeable is considerably smaller than the UK defence procurement market.[344]

We have already noted that the procurement of equipment for the military and for civilian agencies is undertaken by different bodies with different budgets. We reiterate here that on the defence side, procurement is undertaken by the MOD's Defence Equipment & Support organisation. We also emphasise again that, on the civil security side, the situation is a great deal more complex with procurement budgets and organisation spread across a variety of organisations in both national and local government. The only area in which there have been some moves towards a blurring of the procurement process is the CBRN field where there are efforts underway by the MOD and the Home Office to coordinate their procurement efforts. However, these efforts are at a relatively early stage.

---

[342] Figures are for 2004/05 and are taken from the MOD *Defence Industrial Strategy*

[343] The figures are for operational spending and equipment spending combined and it should be noted that in some segments operational spending represents a considerably greater share of spending than does equipment (for instance, airport security, where operational spending accounts for 80% of security spending). Frost & Sullivan, *UK Homeland Security Market*, July 2007.

[344] Considerable caution is needed with these figures since it is unclear whether they are like-for-like comparisons. Nevertheless, the key point, namely that the security market is much smaller than defence market, holds true.

Industry structure reflects the structure of the markets. There are some companies who – by the nature of their technologies and products – have always operated in both the defence and security markets. In the CBRNE field, Smiths Detection has long sold equipment to detect and analyse CBRNE materials to both defence and civil security customers. In information and communications technologies, companies like Fujitsu Defence & Security have sold similar information technology systems to defence and "High-end" security customers. Fujitsu Defence & Security is one of the largest suppliers of IT systems to both government and the private sector; with installations in the Home Office, Cabinet Office, MOD, Her Majesty's Revenue and Customs and Security Agencies. Fujitsu Defence & Security is one of the UK's leading IT Systems Integrators and sees the security market as an opportunity to enlarge demand for ICT and its services.

Some UK defence companies are actively seeking to diversify into the security market. For instance, BAE Systems has identified the security market as an evolving and growing sector and emphasises its capabilities that it sees as applicable to security including secure computer systems, information and network technologies, C4ISTAR, situational awareness and surveillance and intelligence and systems integration. BAE Systems is also exploring the potential of the use of UAVs for civilian security applications. Significantly, after attempting to grow these capabilities organically, it made the decision in 2008 to acquire DETICA (a specialist "High-end" security company) in part as a way of strengthening its marketing capabilities in the security field. This shows how possession of distinction technological capabilities may be a necessary but not sufficient condition for successful market entry by defence companies. Another example is SERCO, an international services company with experience in the defence and home affairs sector as well as in IT, education and other government services. VT Group - a leading UK defence and support services contractor – has established VT "Homeland Security" to bring together expertise in the provision of communications infrastructure, nuclear engineering and technical services, fire fighting training facilities, military training, aircraft and ships.

Equally, some security companies have moved into the defence sector. Companies with a strong position in civil-security origin and enterprise-origin information and communication technologies have entered (or strengthened) their position in the defence market; these companies include the likes of Cisco Systems, Sun Microsystems and Fujitsu Defence & Security.

4.2 Factors driving blurring of boundaries

A number of factors can be identified as drivers of blurring between the defence and security markets and industries.

One driver is common technology requirements. Thus, we have noted how there are some technology requirements that are increasingly common to the defence and security sectors. There is a common demand for CBRN detection, protection and decontamination equipment. Equally, we have already noted how Information and Communications Technologies are increasingly generic and pervasive. Accordingly, there is a growing blurring of the market for products and systems based upon such technologies.

In some fields, this blurring is being encouraged by government which recognizes the potential benefits in terms of economies of scale and the encouragement of innovation through creating common demand opportunities. Thus, in the CBRN equipment field, the MOD is exploring synergies with the Home Office and other government departments to develop a common market. The MOD's *Defence Industrial Strategy* illustrates MOD thinking about the potential benefits of a growing blurring between defence and security in the UK CBRN industry when it states:

"The supplier base within the UK is strong and growing due in part to increased focus on the homeland defence market. This is attracting suppliers who have not previously shown a defence interest, which should benefit us by facilitating access to innovative solutions and technologies…. The UK's commercial CBRN sector is buoyant. To manage effectively both MOD's and industry's aspirations the following strategy will be followed…. *Maximise the economies of scale from effective cross Government working*".[345]

We have noted how large defence contractors are paying increasing attention to the security market by seeking security applications for defence technologies and in some instances acquiring security companies as a means of gaining access to their knowledge of the market. This is another factor driving blurring and the anticipated decline in UK defence budgets is likely to encourage further efforts by defence contractors to enter the "High-end" security market. The security market is seen by defence companies as an opportunity for adjacent diversification since they

[345] *UK Defence Industrial Strategy*, 2005, p.119 (emphasis added).

perceive themselves as having technologies and systems integration capabilities that are applicable to “High-end” security requirements.

A further blurring of the distinction between the defence and security industries can seen to be a consequence of teaming between defence companies and security companies on large security programmes. In this way, a defence company’s technological capabilities can be complemented with the knowledge of the security customer possessed by other companies. Equally, since defence companies perceive themselves to have strong systems engineering capabilities, we observe teaming between defence companies (as systems integrators) and other (non-defence) suppliers of systems and sub-systems. For example, the successful bidding consortium for the UK eBorders programme was led by the defence contractor Raytheon Systems Limited and other members of the consortium include Serco (a services company), Accenture (IT and consulting), DETICA (a company focused on the security and intelligence sectors recently acquired by BAE Systems), QinetiQ (the privatized UK government defence research agency), Capgemini (the IT services and consultancy company) and Steria (an IT services provider).

We have already noted the role of ICTs in the transformation of the UK military. The growing emphasis on Network Enabled Capability and the security of that network means that the capabilities of security companies are of increasing importance to defence procurement programmes although it should be noted that they have rarely sought prime contractor status on defence programmes for reasons that we will discuss below.

4.3 Factors constraining blurring of boundaries

We have noted that there is some evidence of a blurring of boundary between the markets for CBRN and ICTs. However, in other areas differences in buyer values and requirements represent powerful barriers to blurring. These differences present major challenges to defence companies seeking to diversify into civil security markets and vice versa.

The defence and security markets have very different structures. The UK defence market has a single easily identifiable buyer (the Ministry of Defence) and a single set of clearly defined procurement processes (managed by the MOD’s Defence Equipment and Support organization). In contrast, the security sector is characterized by a large number of relatively small customers with very different procurement practices. Large procurement programmes in the security sector are

relatively rare. The AirWave programme for a first responder communication system (£2.5 billion over 19 years) and the eBorders border control information technology programme (£650 million) are relatively rare examples of very large civil security programmes.

Another constraint on blurring is that security customers are very different to defence customers and their buyer values are not necessarily receptive to product offerings from defence companies. Defence technology and defence-like solutions to security challenges may not necessarily be attractive to security customers. For instance, police forces in the UK tend to be relatively conservative with respect to their use of new technology. Equally, new technologies (like UAVs) may require changes in operating procedures and training and civilian security agencies may prefer manpower intensive solutions over complex, costly and untried technological approaches. A challenge for defence companies has been to develop business models (like pay-as-you-use) to encourage adoption of some technologies like UAVs that may be regarded by many civilian agencies as too expensive and complex to operate. At the same time, defence companies are seeking to enter a market that already has incumbent security companies with niche capabilities and strong reputations amongst security customers.

Thus, diversification has not moved as far or as fast as they may have expected. Differences in buyer values and requirements between the defence and security markets mean that defence companies have to develop an understanding of the market and this has taken time. The rate at which defence companies have been able to diversify into the security market has depended – in part – on the speed at which they have been able to understand the security market either through organic developments or through acquisition of businesses with knowledge of the security market (for example, BAE System's acquisition of DETICA).

Equally, defence companies have found that competitive conditions in the security market can be challenging. On the one hand, there are powerful incumbents in some parts of the market. On the other hand, there are new entrants from the civilian ICT sector who are drawing on civil origin technologies and applications drawn from the dynamic retail, banking and telecommunications sectors. There are examples of defence companies losing out to such companies in head-to-head competitions for security programmes. One example of a defence company losing out to a telecommunications company is provided by the 2005 procurement competition in the UK to supply a UK national radio system for first responders. The programme was won by O2 Airwave – a consortium led by the telecommunications company BT – at the expense of a consortium led by

EADS Defence and Security. Equally, however, examples of the reverse can also be identified. For example, a consortium led by defence contractor Raytheon Systems Limited won the UK eBorders programme against competition from a BT led consortium.

Equally, enterprise and civil security companies have faced challenges in moving into the defence market. They too have found that buyer values differ between the security and defence markets and some have found defence procurement practices and processes complex and security controls off putting. The paradox is that whilst the technologies that these companies possess such as ICT security systems are clearly of growing importance to the Ministry of Defence it is the case that security companies have rarely established themselves as prime contractors on defence programmes. Commercial technologies may be at the heart of the military network but established defence companies remain the prime contractors on most communications and network infrastructure programmes. In most cases, security companies – whilst interested in the business opportunities emerging – remain subcontractors and suppliers and this is likely to remain the pattern for the foreseeable future. One example is the UK MOD's Falcon communications infrastructure programme where BAE Systems acts as prime contractor with technology partners that include CISCO Systems.

Security companies have therefore mainly entered large defence programmes as sub-system suppliers, with established large defence contractors playing a crucial role as intermediaries integrating technologies developed in the civil and enterprise security sectors and translating them into military applications. However, in the United Kingdom at least, there is a strong sense that defence contractors have by-and-large not been particularly good at maximising the benefits of working with civil and enterprise security companies. Fixed-price procurement contracts have made it difficult for them to develop true partnerships. Thus, they generally not use the systems engineering and integration experience of security ICT companies because the day-rates of engineers in commercial companies tend to be regarded as relatively expensive. In part this is because the security sector companies can gain high rates working for clients in other sectors (until the financial crisis, the banking and financial services sector were a key and profitable market for their IT security services) but it is also because they also tend to quote risk-adjusted prices. Instead, the role of commercial companies has been primarily as the suppliers of "black box" sub-systems rather than systems integrators.

Annex 6. The United States and the issue of blurring boundaries between security and defence

An analysis of the situation in the United States shows remarkable differences in comparison to the EU but also similarities. Generally there is much less concern with the issue of blurring and its industrial implication in the US American debate. Like in the EU the demand side of the security market is much more fragmented than that of the defence market, albeit with the marked difference that there is a single defence equipment purchaser and that there is no equivalent to the Department of Homeland Security (DHS) in the EU. At federal level the DHS is a significant procurer of research services as well as equipment and considers the industrial and technological base in its entirety as a source for the goods and services it requires. This has made the newly created homeland security an attractive source of revenue also for defence contractors. It will be argued that they have followed different strategies in entering this market. Finally, we will point to a number of practices known from defence market that the DHS emulates and that have consequences for European firms.

Clearer separation of missions let's the US be less concerned with "blurring"

A review of publicly available sources that are concerned with the industrial implication of the blurring of boundaries between security and defence in the US shows little concern with the industrial implications that might result from a blurring of the boundaries between security and defence, as both, the Department of Defence (DoD) and the Department of Homeland Security (DHS) seek to satisfy their individual needs with the best possible (American) supplier. Thus the founding documents of the DHS make explicit reference to the industrial and technology base, however, herein the private sector at large is addressed and the activation or use of the defence sector is not singled out.[346]

The reasons for this separation are at least twofold: First, after its establishment in 2002 the DHS had to seek to position itself as an independent organization with an own mission and strategy vis-à-vis existing security agencies. As the only institution responsible for overall public (or

[346] George W. Bush. The Department of Homeland Security, Washington D.C., The White House, Office of Homeland Security, 2002, Office of Homeland Security, National Strategy for Homeland Security,, http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf

"homeland") security[347] at federal level the DHS established a clear profile in relation to the Pentagon. This was the more necessary, as the legislation creating the DHS was silent on this issue and as the DoD had activated NORTHCOM (Northern Command) in response to the increased concern for homeland security without specifying the exact focus and limits of its activities.[348] The DHS has, for example, insisted that as a security agency it has different buyer values in comparison to the defence sector as they relate to operational requirement, the procurement approach, the operating environment, issues of privacy, data protection, aspects of training, and the security of supply. To satisfy its demands for goods and services the DHS considers the entire US scientific, technological and industrial base as its source.

In addition, The Federal States and the wider public are wary of a greater involvement of the Pentagon in homeland security;[349] so is the Pentagon itself. The Department of Defence has traditionally focused on expeditionary warfare overseas and before 9/11 its participation in domestic operations has been sporadic and generally in response to natural disasters. For its operations abroad and at home it could always draw on the National Guard and the activation of policemen from Federal States presents an exception. Moreover, the Pentagon guards its focus on war fighting, its budget and tries to get involved as little as possible in homeland security tasks such as border security.[350] At the same time the Pentagon's intelligence collection and analysis capabilities represent "a substantial portion of the United States' national intelligence assets" and it "remains the greatest federal repository of resources for responding to a chemical, biological, radiological, or nuclear (CBRN) incident", despite the expectation that civilian authorities will eventually develop better capabilities.[351]

In face of these two factors – the clear separation of responsibility for security and defence missions and the insistence of the DHS to use the entire industrial and technological base for its

[347] In our understanding the American term "homeland security" corresponds largely to the notion of "public security" more prevalent in the European context. Both will be used interchangeably.

[348] Steve Bowman. Homeland Security: The Department of Defense's Role, Washington, Congressional Research Service, 2002.

[349] See, for example, the discussion in The Westerner, Pentagon & Homeland Security to Work with Local Police, http://thewesterner.blogspot.com/2009/06/pentagon-homeland-security-to-work-with.html as well as the sources provided there.

[350] Spencer S. Hsu. Agencies Clash on Military's Border Role. At Issue: Which One Directs Troops in Anti-Drug Mission, Washington, The Washington Post, 2009.

[351] Bowman. Homeland Security: The Department of Defense's Role.

newly defined but still evolving mission – it comes as no surprise that there is little discussion about a blurring of lines and its industrial implications.

Department of Homeland Security promotes wide range of technologies

The Department of Homeland Security promotes a wide range of technologies, among them also those that foster the interoperability between different users. The DHS spends its money mainly on six "macro-priorities":[352]

- Comprehensive Immigration Reform with the Secure Border Initiative (SBI) representing the largest spending item in 2008;
- Biometrics and ID programmes;
- Transportation security with a focus on air cargo, where Congress demands an inspection/screening of 100% of all passenger planes
- BioBio--security and Public Health Emergencies Health Emergencies;
- Nuclear detection and chemical facility security with the goal of deploying technology in order to scan 99% of containerised cargo; and
- Federal response to hazards and disasters.

In face of these priorities, information technologies receive a specific attention. This is not only expressed in the fact that the Secure Border Initiative is the single most important and financially the largest project but also in the entire strategy of the DHS. Thus information technologies are a central part of most of the 13 Capstone Integrated Product Teams, which were set up to meet the "high-priority technology needs" of the DHS.[353]

The importance given to information technology is due to the fact that the US government considers information sharing among the different security providers as an essential means to enable overlap on the user side. Information sharing and systems are considered one of four "foundations" of HS and the National Strategy sets out an ambitious programme for the use of IT and communications technologies to have "complete and common awareness of threats and

[352] Christina Balis and Tim Garnett, Homeland Security Opportunity Analysis: An Assessment of Dhs Budget and Contracting Trends, Presentation at the Ndia 2007 Heartland Security Conference, 11 July, http://www.dtic.mil/ndia/2007heartland/Wednesday/BalisandGarnettPresentation.pdf.

[353] Department of Homeland Security - Science and Technology, 2009.

vulnerabilities" among all government entities of every state. A cultural as much as a technological change is required to achieve this goal: thus the National Security sets out to create "a Collaborative Classified Enterprise environment to share sensitive information securely among all relevant government entities," and the establishment of "a secure video conferencing capability connecting officials in Washington, DC with all government entities in every state".[354] This technological emphasis has played to the strength of the major defence contractors when attempting to enter the homeland security market, as the brief analysis of US industry will show further below.

As a major federal procurer the DHS's emulates defence business practices

As in Europe, the demand side of the US American defence and security market differ considerably. The demand side of the public security market is very fragment, as the Federal states have major responsibilities for homeland security. The Pentagon is the single most important buyer not only in the defence market but in the US American public arena in general. Of its overall budget of roughly $ 616 billion it spent about $ 104 billion on procurement and $ 73 billion on research and development. Though the Pentagon dwarfs the Department of Homeland Security in terms of budget, the DHS is at federal level a significant buyer. It has a yearly budget of about $ 50 billion of which it spends about $ 15 billion on the procurement of equipment. It hands out about $ 1 billion for research and development activities. As in many European countries these figures represent about 10% of the size of military procurement.[355]

In its pursuit to establish a public security market at the federal level the Department of Homeland Security introduces practices that are partly know from defence markets and that might influence the chances of European companies to compete successfully. Three examples shall suffice here to support our point. First, the DHS has introduced procedures that strengthen "buy America"

[354] Bush. The Department of Homeland Security.

[355] For defence data see EDA, European - United States Defence Expenditure in 2006, http://www.eda.europa.eu/genericitem.aspx?area=Facts&id=310; for homeland security see Procurement Watch, Role of Homeland Security Contractros Is Questioned, http://www.encyclopedia.com/doc/1G1-170731070.html; U.S. Department of Homeland Security, Closed Session of the Homeland Security Science and Technology Advisory Committee (Hsstac), February 23-24, Arlington, Va, http://www.dhs.gov/xlibrary/assets/HSSTAC_MtgMinutes_23-24Feb05.pdf; Government Computer News (GCN), Dhs to Hire More Procurement Officers, http://gcn.com/articles/2006/08/04/dhs-to-hire-more-procurement-officers.aspx. All figures are 2006 data in order to allow comparison with the corresponding publicly available figures for the Department of Homeland Security.

provisions.[356] This might have two negative consequences for European firms. On the one hand, they might be put at a disadvantage vis-à-vis their US American competitors as it is the case in defence markets. On the other, there might be longer term implications. In the future the US market is likely to become even more attractive than it is now, especially in comparison to the fragmented EU markets. European companies might therefore tend to shift some of their research as well as production facilities to the US instead of retaining them in Europe, which could have negative consequence on the European technological and competitive position in general.

Moreover, the DHS decisions have procedural and economic effects beyond the borders of the United States. The forward screening of containers in European port is the most obvious example. More important, however, are the attempts to establish international standards and norms favouring US companies but based on a security argument. The current struggle over the standards in container security backed by strong interests of IBM and other computing companies that seek to exploit the vast amount of data to be collected has already pitted European against American interests, with the potential of a US-Chinese cooperation on this issue. Cases like this pose a specific challenge to the EU given that economic interests are advanced with a security argumentation.

Finally, the DHS has established a Homeland Security Advanced Research Projects Agency (HSARPA) and three other organizations to mobilize the research and technology base of the country for its mission. Like the Defence Advanced Research Project Agency (DARPA) HSARPA has been created to foster research activities, especially of the private sector. It is an interface to with private industry. In contrast to its famous “defence sibling”, however, HSARPA focuses mainly on research for the solution of current rather than long-term problems. Thus Under Secretary for Science and Technology, Charles E. McQueary, stated in 2004:

“But at least today, about 90 to 95 percent of the emphasis is on things that can be done now. And what I mean by "now" I mean tomorrow, six months from now, a year from now. By near-term I mean a couple of years. They're working on near-term with only about five to ten percent of their budget dealing with what I'll call forward-looking science.”[357]

---

[356] Alane Kochems, "Buy America" Provision Don't Help Homeland Security or National Defence. Web-Memo of the Heritage Foundation, http://www.heritage.org/research/homelandsecurity/wm769.cfm.

[357] U.S. Department of Homeland Security, Closed Session of the Homeland Security Science and Technology Advisory Committee (Hsstac), February 26, Potomac, Maryland, http://www.dhs.gov/xlibrary/assets/HSSTACOpenSessionMinutesFeb2604.pdf.

This focus on short-term projects might be subject of change in the future.[358] The main "mission of HSARPA is to engage the private sector in R&D in order to satisfy DHS operational requirements, conduct rapid prototyping and commercial adaptation, and conduct research and development of revolutionary options." [359] Stakeholders have pointed out that HSARPA thereby fulfils a function that still needs to be filled in many European countries.

Defence companies have entered security market with different strategies

In response to the significant sums spent by the Department of Homeland security all main US defence companies entered the homeland security market, but have followed markedly different strategies. Defence firms entered the security market mainly in the expectation that defence budgets won't keep rising and to open up new sources of revenues. While past experiences to diversify into the commercial sector have not been particularly successful the homeland security market is thought to be similar to the defence market in that it involves selling to the federal government.[360]

In entering the homeland security market the major defence contractors have followed clearly different strategies. Thus Lockheed Martin and Northrop Grumman, the first and third largest defence contractors respectively, have both built on their expertise in information technology and services. Lockheed is the largest federal information technology contractor and secured a number of contracts from the DHS. In July 2008 the company was awarded a $1.2 billion contract from the Transportation Security Administration (TSA) to manage its Integrated Hiring Operations and Personnel Program for up to eight years. Since 2002 Lockheed has provided the TSA with new training and screening procedures at 429 airports in the United States. In 2009 Lockheed Martin won a 10-year, $1 billion contract from the FBI to develop the Next Generation Identification system. It will double the size of the existing database for fingerprints and will add palm prints, iris and facial recognition. Moreover Lockheed Martin provides US maritime port workers with biometric smart cards for their secure identification badges. The company is also the prime

[358] U.S. Department of Homeland Security, Closed Session of the Homeland Security Science and Technology Advisory Committee, May 20-21, New York, Ny, http://www.dhs.gov/xlibrary/assets/HSSTAC_MtgMinutes_20-21May04.pdf.
[359] U.S. Department of Homeland Security, Closed Session of the Homeland Security Science and Technology Advisory Committee (Hsstac), February 23-24, Arlington, Va,
[360] Philip Finnegan, Defence Companies Pursue Homeland Security Growth, http://www.hstoday.us/content/view/4926/201/.

contractor for the New York Metropolitan Transportation Authority's comprehensive upgrade of its electronic security operation infrastructure. The company intends to build on its edge in nuclear, biological and chemical sensors and cyber security to offer further goods and services to the DHS.[361]

Northrop Grumman equally focuses its strategy on information technology, putting a high priority on winning contracts for TSA information infrastructure development and Department of Homeland Security (DHS) network support under the Enterprise Acquisition Gateway for Leading Edge (EAGLE) contract for information technology. Thus it was one of 25 companies awarded the indefinite delivery/indefinite quantity (IDIQ), five-year EAGLE contract with two one-year options. In 2006 the company won a $357 million IDIQ contract to assist the DHS' Citizen and Immigration Services Support Application Centres. Northrop Grumman Technical Services provides the labour that inputs the biometric data needed to support the centres. Based on its expertise as a defence contractor Northrop Grumman offers services in four functional categories: infrastructure engineering design, development, implementation and integration; operations and maintenance; software development; and management support services. In 2006 the company won two other critical contracts: under a five-year agreement with the DHS it was to provide support engineering to improve first responder communications; in the area of port security the company's system will among others help to identify potential threats at and to ports of entry, collect information through preventive measures and interdiction of cross-border violations.[362]

Boeing, the second largest defence contractor, has followed a markedly different strategy. Building on its edge in quickly bringing together diverse technologies, the company has built its strategy around systems integration rather than information technology. Thus the company's first major success in homeland security was a $508 million contract to install more than 1,000 X-ray explosives detection machines and 4,500 explosive trace detection machines at more than 400 airports in the United States. The work on this contract was completed by the end of 2002. In 2006 Boeing became the prime contractor for the Secure Border Initiative Network (SBInet), a comprehensive border protection program using advanced technology. Under this three-year

[361] Frost & Sullivan, "U.S. Federal Homeland Security and Defence Markets," (London: 2004); Jane's Defence Weekly, Homeland Security, http://jdw.janes.com/public/jdw/security.shtml ; Finnegan, Defence Companies Pursue Homeland Security Growth, ; Lockheed Martin, Center for Innovation, http://www.lockheedmartin.com/innovation.

[362] Jane's Defence Weekly, Homeland Security, ; Finnegan, Defence Companies Pursue Homeland Security Growth, ; Northrop Grumman, Our Capabilities, http://www.northropgrumman.com/capabilities/index.html.

contract – three one year extensions are possible – the company has already received approximately $1.15 billion, including a $773 million award for supply chain management, a $136 million contract for program management and $122 million to build 32 miles of fencing.[363]

[363] GAO. Secure Border Initiative. Observations on the Importance of Applying Lessons Learned to Future Projects (Gao-08-508t), 27 February, Washington, United States Government Accountability Office, 2008; Finnegan, Defence Companies Pursue Homeland Security Growth, ; Alice Lipowicz, "Gao: Sbi So Far Nets Boeing More Than $1b," Washington Technology 2008; CBP.gov, Security Border Initiative (Sbi), Available at: http://www.cbp.gov/xp/cgov/border_security/sbi/