Study on pre-commercial procurement in the field of Security

Within the Framework Contract of Security Studies – ENTR/09/050

Final report

Client: European Commission DG Enterprise and Industry

November 2011

Consortium partners:

DECISION Etudes & Conseil

ECORYS Research and Consulting

TNO

In collaboration with:

Manchester Institute of Innovation Research

Corvers Procurement Services

Study on pre-commercial procurement in the field of Security
Within the Framework Contract of Security Studies – ENTR/09/050

Final report

Client: European Commission DG Enterprise and Industry

November 2011

ECORYS

About Ecorys

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

Ecorys Netherlands has an active CSR policy and is ISO14001 certified (the internationally recognized quality standard for environmental management systems). Our sustainability goals translate into our company policy and practical measures, such as printing our documents on FSC certified paper and compensating our carbon footprint.

ECORYS Nederland BV
Watermanweg 44
3067 GG Rotterdam

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

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

W www.ecorys.nl

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

Outline

Preface

This document constitutes the Final Report for the “Study on pre-commercial procurement in the field of Security” undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland BV.

The main elements of this Report concern the overview of the EU security R&D environment, and of the already existing PCP schemes. National surveys for 5 EU Member States are provided in an accompanying report (Part II). Drawing on the findings from the EU and national surveys, the Report identifies and assesses potential EU-level policy options that could help the implementation of PCP in Europe.

The organisations that have contributed to this report are:

- DECISION
- Ecorys
- MIoIR (Manchester Institute of Innovation Research)
- Corvers

The individual contributors to the study (including the national surveys) are as follows:

- Sébastien Rospide, Gerard Briard, Laurent Marragou, and Thibault Montoroi (DECISION)
- Robert Piers, Dick Mans, Koen Berden (Ecorys)
- Thomas Teichler, and John Rigby (MIoIR)
- Stephan Corvers, Ramona Apostol (Corvers)

Team Leader and Coordinator:

- Sébastien Rospide (DECISION)

Executive Summary

General context to the introduction of PCP

Security has increasingly become a critical concern both for political authorities and citizens. In 2009 the European security industry had a turnover of more than 20 billion €, with 130 000 employees, or even 255 000 including equipment related service employees.

According to EOS, the European Security Trade Organisation, public spending in security R&D is ten times lower in Europe than in the USA. This represents a potential threat to the competitiveness of the European security industry, in a time when world markets are expected to grow significantly faster than European or US markets.

Moreover several security market weaknesses were identified in the ECORYS 2009 study. These weaknesses consisted for a large part in lack of coordination within the supply chain, insufficient transparency, difficulties with intellectual property rights, and absence of international standards in the security field.

Lack of coordination within the supply chain, between research organisations, prescribers, manufacturers and suppliers, and end-users has led to difficulties in succeeding the transition of an innovation from the research stage to the commercial development stage. It has made the transition from research activities to commercial development difficult.

The question of Intellectual property rights has been a source of concern. It is necessary both to ensure adequate protection, and at the same time to find acceptable modalities for sharing rights when investment in R&D is shared between public funders and suppliers.

The insufficient transparency of the public procurement systems has sometimes been used to limit the access to markets of potential suppliers, for example through preference for local suppliers. This has contributed to market fragmentation, as does the absence of common European and international standards in the security field. This is a serious disadvantage for the European security industry, faced with problems due to diverse specifications and limited inter-operability.

In order to preserve the future positions of European industry, reinforcing both the amount and efficiency of European R&D seems essential, as well as striving to correct these weaknesses. Pre-Commercial Procurement (PCP), a procedure for the public procurement of R&D services, covering the exploration and definition of different competing solutions, down to test-series production and field testing, seems able to provide some answers to these difficulties.

In the first place, PCP is a demand based innovation scheme. A fundamental aspect of this is the expression of needs by the end-users, who are involved as well as all the other stakeholders in the supply chain from the very start of the innovation process. Security prescribers, equipment suppliers, and end-users cooperate in defining common needs and corresponding specifications in order to optimise the fit between user needs and the solutions developed.

Splitting the R&D procurement process into phases down to pre-commercial products enables fine-tuning of the competitive selection of the most promising of different competing solutions. This can

function as a learning process, and the breakdown into distinct phases enables the gradual participation of SMEs.

Competitive development through the different phases of the R&D process, together with the increased transparency of procurement procedures should contribute to greater efficiency, and lesser fragmentation.

The status of intellectual property rights could enable different configurations of sharing of funding risks and commercial benefits of R&D and innovation between public or private funders and suppliers of security solutions.

Security is a major concern for public authorities and citizens in general, and security needs are generally publicly driven. An important advantage of PCP schemes in the security field is that public procurers could thereby exert an important leverage on the market.

A distinction should be made between 'individual' PCP programmes led by a single entity whether it is national or sub-national and 'joint' PCP programmes that bundle together several potential procurers or parties involved. The fragmentation of the security market is considered as the most limiting factor for the competitiveness of the EU security industry. In that respect, 'joint' PCP programmes could provide a relevant vehicle for bringing together user demand, and the Commission has recently introduced in the last FP7-Security Research Call 5 published in July 2010 the concept of POV (pre-operational validation), which is similar to the PCP scheme but with a different project phasing.

Key findings from country and sectorial analysis

Procurement organisation: cooperation a key factor in all sectors

In the sectors we have analysed in this study, security is generally not the operators' core business. It is however the direct concern of the political authorities and the citizens of the EU. For the operators on the other hand security is often experienced as a burden.

Responsibilities are generally split between public bodies tasked with prescribing security measures, and operators (generally private) who are tasked with implementing them and procuring the equipment. As a consequence, prescription and procurement are often dissociated in the security field. Greater efficiency requires greater cooperation.

In sectors that are transnational in their nature (airport security, maritime borders), international structures have been established in order to facilitate cooperation. This is less the case for sectors such as urban transport or critical infrastructures. Sector configurations differ as to relative public-private involvement but all of them require a large measure of coordination between stakeholders and of cooperation between the public and private sectors.

A critical issue is the commitment to purchase in the sectors covered by this study. The procurers of the R&D services are public authorities, who will not usually procure the resulting equipment. This will be purchased by the end-users generally as a result of functional regulation by public authorities, who will not specify a particular supplier. This makes the link between R&D procurement and commercial procurement more complex than in Defence industry programmes.

Security is a priority, and PCP is seen as a useful innovation

Security is a priority in all the countries we studied, and coordination between the public bodies is a necessary first step towards more efficient security. Such a process has started in most countries.

However the involvement of the whole supply chain in the cooperation process remains to be achieved. This is where PCP as an essentially cooperative R&D procedure can bring a valuable contribution.

Governments that have already introduced PCP are favourable to the principle, but have not yet been able to assess its efficiency because its introduction is still very recent, and the others consider that if PCP-POV proves to be a useful tool, then it should be developed, but again there is not yet much European experience in the field.

The positions that have been expressed by European governments on PCP are not specific to the security field. So far, existing PCP schemes in Europe are only implemented in a few Member States (Belgium, the Netherlands, the UK and Spain[1]) and they mostly address R&D in other fields than security.

Industry positions are more operational, and look at the results industrialists can expect in terms of markets, costs and delays... Weighing the pros and cons is still difficult due to the lack of sufficient experience of the new procedure, its results, and the difficulties it may create.

PCP could boost the growth of the European security industry

It is very difficult to assess the impact of PCP-POV, as such procedures are still very little used in Europe. However similar schemes have been implemented elsewhere, and in particular the US SBIR programme, which was launched in 1983.

Various studies have attempted to measure the impact of SBIR on sales, employment, growth, R&D and innovation, or project costs.

These studies are unanimous in considering the SBIR programme has had positive results. Several of them succeeded in measuring a quantifiable impact on sales and employment. 30 to 40% of SBIR projects generated products that have reached the market, and that would not have existed without it. One study found that sales growth for companies that received SBIR contracts, compared to ones that didn't, was twice as fast, and employment growth three times as fast.

SBIR awards add to these companies' growth capabilities, in an almost Darwinian policy of facilitating the "survival and development of the fittest", thus improving the competitiveness of the industry, as well as benefiting the whole community by aiding innovation and, in this particular case, security.

The implementation of a European PCP programme should bring at least equivalent benefits in terms of sales and employment growth. The difficulty is of course to extrapolate the benefits to the recipient companies to the whole industry. Looking at the present situation of the world security markets, and the relative position of the European security industry, we can explore some

[1] Spain launched a new funding instrument in September 2011, the Innodemanda programme, oriented towards public procurement of innovative technologies and offering good perspectives for the implementation of PCP procedures

possibilities of impact of a successful PCP scheme. We have attempted to show what the effect of an increased growth rate could be on the sales and employment of the European security industry. Increased and more efficient European security R&D can be expected to boost the European market growth and at the same time to improve the competitiveness of European supply, thus giving production and employment in Europe an extra impetus.

A tentative assumption of a 1% increase in the annual growth rate of the European security markets due to R&D support through a PCP scheme would lead to extra annual sales on the European market by 2020 of more than 2 billion € compared to the baseline situation, and to an increase in annual production in Europe of 6 billion €, leading to around 40 000 new jobs in the industry, and maybe another 40 000 new jobs in the related services.

Major challenges raised by PCP/POV in the field of Security

Mobilising resources

Today awareness of security stakeholders concerning the PCP innovative R&D procedure is very low in most EU countries, and at present only four countries (Belgium, the Netherlands, the UK and Spain) have actually embarked on PCP pilot schemes with only few funded security programmes identified under the UK SBRI programme or the Dutch SBIR programme.

Promoting and implementing international cooperation, but also coordination inside the EU countries between diverse national stakeholders in security R&D, is a challenging task.

A first difficulty is that technical expertise and resources are unequal in the different security sectors. In sectors such as urban transport or critical infrastructures these resources need to be built up.

Moreover international cooperation and also national coordination are seen as time consuming in the present, for uncertain future benefits. Mobilising operator resources to participate in security R&D programmes would therefore require that the projects to be implemented should address clear operational issues.

Organizing cooperation

PCP involves multi-level cooperation between all stakeholders in the innovation and procurement process, from the common expression of needs, both functional and technical, to the review of results and their validation procedures.

A difficulty in achieving the common expression of functional and technical needs is that the fine expression of such needs may differ from one security procurer to another inside a same country, and even more so in different countries. And as coordination and cooperation imply the exchange of information, confidentiality can be a problem, given the sensitive character of information on security issues and solutions.

This is all the more true as the assessment and validation of the results of a PCP R&D programme requires a high degree of transparency. A consensus between stakeholders is essential to guarantee the acceptance of the R&D programme and its results.

An issue not to be neglected is the geographical scope of PCP R&D programmes. Some stakeholders argue that non-EU countries should not participate in PCP/POV programmes that are in particular designed to improve the competitive position of the EU security industry on European and world markets.

Intellectual Property Rights (IPR) management

The general principle in PCP schemes for IPR management is that the Intellectual Property is owned by the supplier, and the procurer (who has funded the R&D) receives a user right or a royalty-bearing license, which can be exclusive or not.

However the IPR question may become a complex issue due to several factors. A first difficulty concerns the scope and definition of the IP generated during the project, and its distinction from the IP held by the stakeholders (supplier or procurer) before the start of the project.

A second difficulty resides in the evaluation of the value of the IPR generated during the project. This may be a complex task in the security market, due in particular to the influence of the regulatory environment in shaping the security market.

The question of sharing information and exploitation can be problematic when critical or restricted information needs to be disclosed in association with the IPR. This is particularly an issue when the PCP project involves cooperation between several Member States.

The purpose of this study is not to provide answers to these complex issues. However, in spite of these possible difficulties, most of the stakeholders interviewed felt the IPR question should not be a major obstacle to the development of PCP.

Legal basis of PCP in the Security field

The PCP concept has originally been developed by the European Commission on the basis of the EU Directives regulating the procurement procedures of public authorities and public entities. However the application of PCP in the Security field falls under the scope of another Directive regulating public procurement in the fields of defence and security. This last Directive provides for the procurement of R&D services awarded through a shared risk-benefit approach (i.e. PCP) and contains a few differences with the equivalent provisions in the first Directives. The object of this legal analysis is to assess the potential adaptation to the original PCP concept that may be required to implement such scheme in the security field.

Firstly, the concept of R&D services under Directive 2009/81 covers fundamental research and excludes the making and qualification of pre-production prototypes, tools and industrial engineering, industrial design or manufacture. Fundamental research is though excluded from the concept of PCP as developed by the European Commission within the context of Directives 2004/17/EC and 2004/18/EC, while the pre-production prototyping phase is included.
This difference entails that contracting authorities/entities may in principle follow the procedural steps described in the PCP procedure - as outlined by the European Commission within the context of Directives 2004/17/EC and 2004/18/EC - when they procure R&D services with a shared risk-benefit approach, if they limit its application to Phase 0, Phase 1 and Phase 2 of the PCP (see Fig.1). Phase 3 Field Test could not be procured outside the scope of application of Directive 2009/81/EC.

Secondly, Directive 2009/81 expressly provides that the contracting authority/entity may buy the product developed within an R&D contract (with shared risk-benefit approach) without having to organise a separate procurement procedure if the contract which covers the research activities already includes an option for those phases and was awarded through a restricted procedure or a negotiated procedure with the publication of a contract notice, or, where applicable, a competitive dialogue.

Thirdly, all contracts awarded within the framework of a cooperative programme based on research and development, conducted jointly by at least two Member States for the development of a new product are excluded from the scope of application of Directive 2009/81.

The above mentioned differences in the scope of the R&D concept do not affect the possibilities for contracting authorities/entities from different Member States to initiate a bottom-up procurement of R&D services with a shared risk-benefit approach, unless there is national legislation which constitute a barrier to collaboration. The provisions of Directive 2009/81/EC do not limit the potential of the EU to finance cross-border procurements of R&D services with a shared risk-benefit approach.

Attractiveness of PCP/POV in the security field

European PCP schemes are attractive in the security field both for general reasons common to all sectors, and for reasons that are specific to the security field. These are summarised in the table below:

Attractiveness of PCP/POV in the security field

	Generic to PCP	Specific to security of countries
Pros	- General need in Europe to better align R&D projects with security requirements and end-user needs - Similarity of security needs between public procurers in different countries - The phasing could represent an opportunity to develop SME participation in larger R&D programmes	- PCP is attractive in the maritime borders and airport security sectors (high international organisation, public involvement, security awareness) - Smaller countries generally have few R&D structures of their own, and may welcome European initiatives as a possible way to improve their R&D activities
Cons	- Procurers have often limited capabilities to create specifications corresponding to operational needs - Phasing seen as an additional delay in bringing innovation to market - Cooperation between public procurers may be restricted due to sovereignty and/or IPR issues	- PCP may be less attractive in the urban transport and critical infrastructure sectors (low international organisation, lesser public involvement, lesser security sensitivity) - Larger countries have their own R&D structures, and may be wary of new organisations creating new burdens and constraints

Policy options and assessment of their impact

Different policy options can be considered for different sectors

Ad-hoc sectorial initiatives may facilitate the European cooperation that is crucial for the survival and development of the European security industry. This rests on the fact that country specificities are probably secondary to the specificities of the different sectors in the security field. Addressing these sectorial specificities may help recognition of the benefits of cooperation.

Such a sectorial approach should also facilitate the bottom-up approach, between players « speaking the same language » in their sector.

In this perspective, two different policy options may be adopted, keeping in mind that they are not necessarily mutually exclusive:

Option 1 consists in the support of the European Commission to centralised PCP schemes engaged through existing European sectoral structures. This option corresponds to security domains where such agencies exist, such as maritime borders or airport security.

Option 2 consists in the EC funding decentralized PCP/POV programmes jointly with several Member States through Framework Programme 7 and 8 projects. This option would best correspond to security domains where there are yet no European agencies or structures, such as urban transport or critical infrastructures

Both options result in positive impacts

Both options considered (centralised or decentralised EU-PCP schemes) bring about a broad set of impacts, which are to a large extent positive, although in many cases the positive impact is stronger with the first option.

Key in the differentiation of the impacts between the options, is the difference in the number of procurers that together set-up a PCP scheme. This number will be larger in the first option with the European agencies running PCP schemes, than in the second option with PCP applied via a Framework Programme scheme. The European agencies generally represent procurers or users from the 27 member states who will thus be involved in their PCP schemes.

The second option generally applies to those sectors in which there is no EU coordination body, such as urban transport and critical infrastructures. This means that the cooperation should come from the procurers or users themselves, and given the character of the FP programme, such a PCP scheme will only involve a selected number of procurers or users and not all users from the 27 member states. The consequence is that any impacts that are dependent on the existence of a coordination body or on the number of procurers or users in a PCP scheme score better in the first option than in the second. For all other impacts the two options score equally good or bad.

Thus the first option involving EU agency coordinated PCP schemes scores higher for a selected number of impacts where a larger number of procurers / users involved contribute to increase the

benefit while the second option scores better on some impacts especially related to the time to market.

Positive impact is greater in the first option in security sectors where the validation of R&D results is strongly connected to national interests and sovereignty. In these cases starting out with a consensus on these issues is a key to the full exploitation of the results.

However one should note that both options are not mutually exclusive as already mentioned. This means that if existing agencies in some security sectors are not willing, authorized or capable to run a centralized EU PCP scheme, option2 could well be applicable to these sectors with positive impacts. The 'best' option may be indeed a combination of option 1 and option 2, tailored to the situation of different sectors.

Recommendations

The study proposes some recommendations to the European Commission for supporting the development and implementation of PCP in the Security field. These recommendations provide a set of measures and support actions that can be implemented before, during and after a PCP project.

Preparatory actions

The first action consists in **educating the market**. Public and private players need to be made aware of the need for PCP, of the difference between PCP and conventional R&D grants and conventional procurement, of the reasons for additional instruments beyond those provided by the existing procurement legislation, as well as of the challenges, pitfalls, and solutions related to operating PCP schemes, and of the possibilities for EU support (from other member states and from EU institutions).

The second action should be to **give priorities to any PCP action** engaged in the field of security.

An **EU sectoral approach** should focus on those cases in which EU institutions or agencies with security tasks intend to procure security equipment, or to coordinate procurement-related activities.

An **EU technological approach** should focus on those technical fields offering the most cross-fertilization potential across security domains and beyond.

Programme implementation

The European Commission should privilege the **financial involvement of all stakeholders**. This could include an ex-ante IPR agreement (licensing terms, royalties, free license to use, etc.)

The Commission should require the **involvement of the end-users** in the PCP programmes. In this respect PCP in the security field is a potential area for Public Private Partnership initiatives. Such PPPs should be designed as a continuum, from the expression of needs down to the solution validation stage.

The Commission should encourage the **involvement of authoritative third parties** to translate operational needs into technical specifications, and to evaluate and validate R&D results. This is

crucial where such a capability is not available within public procurers, and it is crucial also to confer confidence in the programme, both internally and externally.

The Commission should ask for **clear project phasing and deliverables**, to reduce the risk of declining involvement due to the programme length, and to encourage SME participation, which is an important objective of the PCP concept.

Market take-up actions

The Commission should take measures to facilitate the **transition from PCP R&D to commercial procurement**. This could be achieved by the dissemination and promotion of PCP results towards potential investors concerned with the business model and business plan, towards public procurers wanting answers to their security needs, and towards private operators worried about their return on investment.

Social acceptance is identified as a major factor to consider in Europe for the security market development and the Commission could therefore leverage the cooperation on security research undertaken in PCP to **raise the social acceptance level** of commercial products and solutions.

Integrated approach to security innovation policy

The Commission should link its PCP policies with other activities related to innovation in the field of security like **standardisation and conformity assessment** of security products, systems and services. This is crucial considering the fact that PCP is initiated at the beginning of the market cycle with the first expression of operational security needs.

This also means that the range of interested parties could go beyond national authorities as security prescribers and public or private operators as end-users, to involve all that may be concerned.

Structure of the report and approach

This Report describes the findings from the study on “PCP in the field of Security”, which is the second study undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland BV.

The content of the study consists of five segments:

- **Pre-Commercial Procurement (PCP) definition and existing programmes**: this segment provides an overview of the general background context and key characteristics of PCP as an innovative procurement scheme for R&D services and innovation, and describes similar existing schemes and programmes.
- **Security sector and country overview**: this segment gives a picture of the present state and organisation of security R&D and equipment procurement in selected domains and countries, and concludes on the attractiveness of the PCP approach in the security field. It also contains lessons learnt from the US SBIR experience, and an analysis of the quantitative impact of PCP/POV on industry.
- **Major challenges raised by PCP in the security field:** this segment discusses the specific challenges and issues to take into account in organizing PCP in the field of security.

- **Policy options and assessment of the impact of implementing PCP in the security field:** this segment defines different possible policy options to encourage the development of PCP in the security field, and assesses the impact of such actions. It concludes with recommendations to facilitate the acceptation and successful implementation of a European PCP scheme. This segment also analyses the legal basis and specific characteristics of PCP in the security field based on the Directive 2009/81 regulating public procurement in the fields of defence and security.
- **Recommendations:** this segment puts forward some possible policy recommendations for the European Commission, to facilitate the development of PCP in the field of Security.

The analysis of the overall EU situation (as documented in this Main Report) has been supported through national surveys conducted in 5 Member States

- France
- Germany
- Hungary
- the Netherlands
- the United Kingdom

The findings from the national surveys are documented in an accompanying Report to this Main Report.

Several particular sectors were selected inside the security field because of their size, their growth potential and their importance as market drivers. In particular they were chosen to represent different configurations with respect to international or local involvement, or to the public or private character of the stakeholders. These particular security sectors were:

- Urban transportation;
- Airport security;
- Maritime borders;
- Critical infrastructures.

1 The study

1.1 Presentation

The aim of this paper is to study the potential application of Pre-Commercial Procurement (PCP), which is a procedure for the public procurement of R&D services. Before doing so and presenting a more comprehensive definition of PCP, it is important to first present the link between public procurement and innovation…

1.1.1 Procurement typologies

According to the Study "Innovation and Public Procurement. Review of Issues at Stake » (Study for the European Commission No ENTR/03/24), two levels can be distinguished in the organisation and administration of innovative public procurement: general and strategic public procurement.

General Procurement. Government procurement can generally be so organised, that innovation can become an essential criterion in the tender and assessment of tender documents. As a rule, central procurement offices are responsible for procurement in general.

Strategic Procurement. Strategic procurement occurs when the demand for certain technologies, products or services is encouraged in order to stimulate a certain market. Strategic procurement is as a rule associated with sectorial policy, and therefore to a large extent neither initiated nor coordinated by the ministries responsible for innovation policy. It is more likely to be located in ministries associated with specific sectors – for example, the various public utilities (or infrastructure branches), and the few remaining "natural monopolies" controlled by the state, such as national defence.

A systematic utilisation of both forms of government procurement calls for coordinated action, i.e. coordination between various ministries and authorities and their admittedly widely different targets and incentive structures. Ministries responsible for innovation policy might, with appropriate mandates, play an important role in bringing about such co-ordination.

Nevertheless, there are also instances of procurement cases where purchasing by state or public sector actors is directed not only towards fulfilling their own (original) tasks, but also aims to influence and support certain patterns of demand on the part of private consumers. On this basis, we can distinguish three main varieties of public procurement: **direct**, **co-operative**, and **catalytic** procurement.

Essentially, these distinctions refer to different types of end-users and corresponding categories of societal need. The theoretical foundation for these distinctions was established in an earlier dichotomy between "direct" and "catalytic" procurement[2]. In direct public procurement, the public agency or authority that carries out the procurement is the primary end-user of the product in question, and the needs that motivate the procurement are thus intrinsic to this procurer.

In catalytic public procurement, the procurement is conducted on behalf of end-users other than the

[2] Edquist & Hommen, 2000

public agency or authority that carries out the procurement, and the societal needs that motivate the procurement can thus be said to be extrinsic to the procurer and located primarily within the private sector, among firms or individual consumers. It is also possible to refer to a third, “mixed” type of case, where the public agency or authority that carries out the procurement is one, but not the only, intended end-user of the product in question, and the needs that motivate the procurement are thus con- generic - i.e., shared by the procurer and other intended end-users. This type of public procurement can be called “cooperative” public procurement.

1.1.2 What is Pre-Commercial Procurement?

From an official point of view, the EU definition as stated in its official 2007 Communication on PCP[3] is reported hereafter:
“For the purpose of this communication "pre-commercial procurement" is intended to describe an approach to procuring R&D services other than those where "the benefits accrue exclusively to the contracting authority for its use in the conduct of its own affairs, on condition that the service provided is wholly remunerated by the contracting authority" and that does not constitute State aid. More specifically in pre-commercial procurement:

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

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

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

However, it is crucial to note that so far, the existing PCP programmes do not fully meet the aforementioned requirements. Indeed, the existing PCP projects are going to be described below, and all of them differ to some extent from the theoretical definition of PCP.

A more pragmatic approach to the definition and scope of PCP is provided hereafter for the sake of clarity.

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

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

provides a link between the PCP R&D scope and the commonly accepted Technology Readiness Level used to assess the maturity of evolving technologies.

Link between innovation phases and Technology Readiness Levels

Innovation Phase	*Technology Readiness Level*	*Description*
	1. Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Example might include paper studies of a technology's basic properties.
Phase I	2. Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.
	3. Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
Phase II	4. Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that the pieces will work together. This is "low fidelity" compared to the eventual system. Examples include integration of 'ad hoc' hardware in a laboratory.
	5. Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include 'high fidelity' laboratory integration of components.
Phase III	6. System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond the breadboard tested for TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in simulated operational environment.
	7. System prototype demonstration in an operational environment	Prototype near or at planned operational system. Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, vehicle or space. Examples include testing the prototype in a test bed aircraft.
	8. Actual system completed and 'flight qualified' through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.

	9. Actual system 'flight proven' through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. In almost all cases, this is the end of the last "bug fixing" aspects of true system development. Examples include using the system under operational mission conditions.

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

The answer to this dilemma is to leave the IPR to the supplier, who in return must concede some advantage to the public procurer, either a price discount on the resulting product, or some modality of IPR sharing or royalty or licensing agreement. This amounts to an overall sharing of the risks and benefits of the project between the public authorities and the private suppliers[4].

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

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

- Integrate the end-users in the R&D process (creating a link between R&D support programmes and procurement needs, coordinating funders, prescribers, procurers and end-users)
- Initiate demand-driven R&D procurement rather than supply-driven R&D procurement

Secondary objectives of PCP are those intending to maximise the efficiency and effectiveness of the programme such as:

- Bring R&D concepts that are promising for the public sector quicker to the market
- Increase SME involvement in innovation
- Develop higher quality and better prices products thanks to competitive development
- Increase the degree of interoperability between participants. The desired degree of interoperability needs to be integrated as a key objective from the start. Indeed, efforts after each R&D phase to achieve interoperability and product inter-changeability between the alternative solutions being developed pave the way for open standards.

With regard to the scope of the PCP programme, a final distinction should be made between:

- 'individual' PCP programmes led by a single entity whether it is national or sub-national one

[4] For a more complete definition of PCP schemes and risk-benefit sharing principles, please refer to §4.4 (Legal analysis)

- 'joint' PCP programmes that bundle together several potential procurers or interested parties

1.1.3 Rationale for PCP in the field of security

In the security sector, studies commissioned at EU level[5,6] identified PCP as an alternative means to bridge the gap from technology development to commercial production.

The European Security Research and Innovation Forum final report (hereafter: ESRIF) underlined the need to ensure maximum take-up of research effort, in order to lead to more efficient and effective operational capabilities in security-related tasks and missions, and in order to enhance the competitiveness of the European security-related industry. To this end, it appeared necessary to consider research activities and their related technological solutions in a system of operational requirements and user needs. Moreover, it seemed necessary to employ the entire pallet of innovation tools, including the involvement of public and private end-users, and the interaction and integration of supply and demand. ESRIF dedicated working group on Innovation (WG 9)[7] emphasized that pre-commercial procurement of innovative security solutions should be promoted and the potential role of the EU as a "first buyer" explored.

Within this context and based on the above-mentioned characteristics, PCP could indeed be well adapted to address some of the identified market failures in the EU security market (ECORYS, 2009):

- Market asymmetry between supply and demand (threats, policies, solutions)
- Difficulty of transitioning from research activities to commercial development of products, particularly for SMEs
- Insufficiency of current security R&D, often not aligned with the immediate security capability requirements
- Insufficient transparency of public procurement systems, which may be used to limit markets access
- IPR concerns (e.g. the discouragement of investments when IPR protection is inadequate)
- Absence of European and common international standards for security

Pre-commercial procurement aims to bring answers to some of these problems with:

- Demand-based innovation schemes
- Procurement from Phase 1 up to Phase 3 of the innovation cycle, from the proof of concept up to the pre-commercial stage[8]
- Competitive development and increased transparency of procurement procedures
- IPR left to the industry based on risk/benefit sharing principles
- Development in distinct phases allowing gradual participation of SMEs

[5] European Security, Research and Innovation Forum (ESRIF) Final Report, December 2009, p.200-201

[6] Ecorys, Decision and TNO, Study on the Competitiveness of the EU security industry within the Framework Contract for Sectorial Competitiveness Studies – ENTR/06/054, Final Report, 15 November 2009, p.32, 110, 118

[7] ESRIF WG9 addressed several issues related to innovation in the security field including: Legal framework, standardisation, specificity of the security market, business model, innovation policy, education and training

[8] Please refer to table "Link between innovation phases and Technology Readiness Levels" (§1.1.2) for a detailed description of the innovation cycle phases

PCP would particularly benefit small and medium sized suppliers of security equipment and systems, who encounter difficulties in transitioning from technology development (research) to the full commercial development of products.

'Joint' PCP programmes as described above could therefore provide a relevant solution for gathering user demand, and thus reduce the European security market fragmentation. As a reaction, the Commission announced its intention to speed up the application of PCP in the security domain, in order to bring results obtained in other research programmes closer to the market. It has recently introduced[9] the concept of POV (pre-operational validation), which is similar to the PCP scheme but with a different project phasing.

1.1.4 Study analytical framework

So far existing PCP schemes in Europe are only implemented in few Member States, and they mostly address R&D in other fields than Security, despite the fact that the Security field is largely publicly driven, thus giving to public procurement a high leverage on the market.

The general aim of this study as set out in the Task Specifications is:

- Analyse the feasibility and the potential impact of pre-commercial procurement measures/systems in order to reduce the fragmentation of the security market in Europe for the benefit of a better EU industry efficiency, cost-effectiveness and security of the European Citizens.

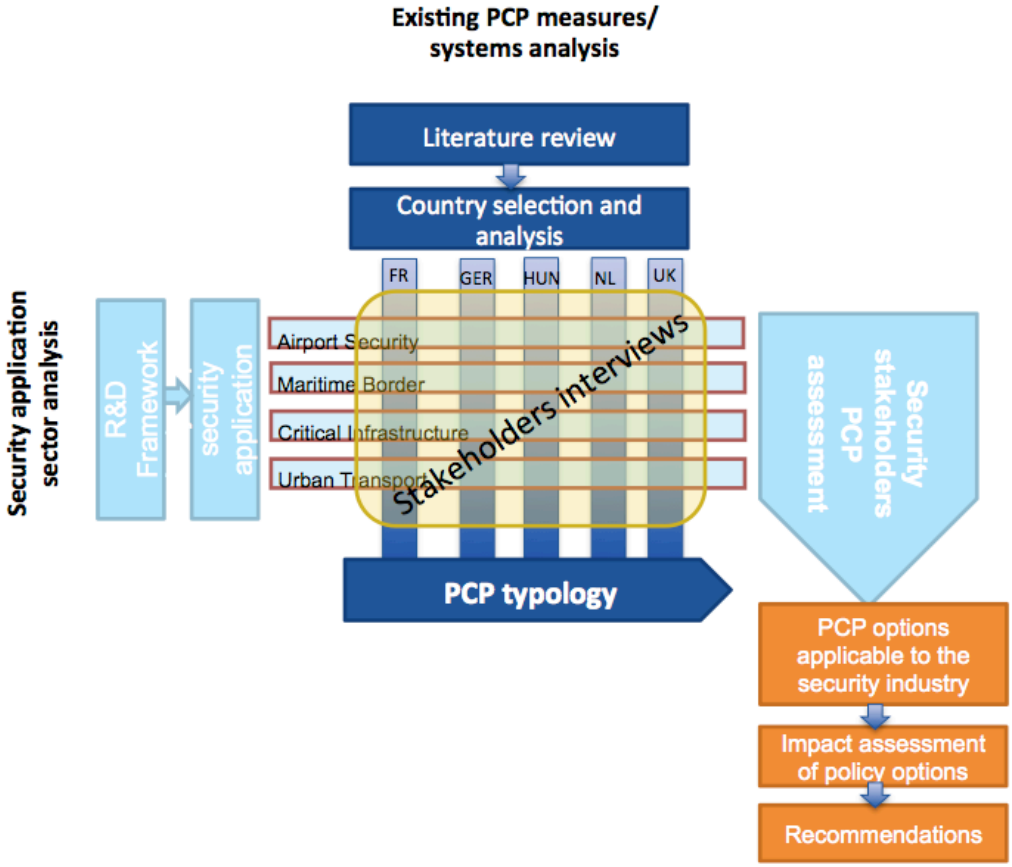
More precisely, the Task Specifications set out the following objectives for this study:

- To bring together available information on pre-commercial procurement and innovative aspects for public procurement applicable to the field of the security sector;
- To evaluate available information and analyse the different existing PCP measures/systems;
- To identify PCP measures/systems best suited to enhance the European competitiveness in the field of security.

In order to ensure adequate coverage to answer these objectives and take into account the specificities of the security field, both in terms of national organization and sectorial specificities, the study was carried out on the basis of 5 country case studies each analysing 4 application domains in the security field with the following analytical approach.

[9] last FP7-Security Research Call 5 published in July 2010

Overall approach to the study



1.2 Sectors selected and rationale

In order to respect the limited time-schedule for the study, it was decided, inside the security field, to focus on selected sectors that would cover a representative set of security issues, stakeholders and markets, leading to different attitudes towards PCP-POV.

The sectors were selected because of their size, their growth potential and their importance as market drivers, and for their particular configuration as to international or local involvement, and as to public or private stakeholders.

This is why the four following sectors were selected:

- Urban transportation;
- Airport security;
- Maritime borders;
- Critical infrastructures.

1.2.1 Urban transportation

Sector coverage

- the sector covers public transportation only (rail and buses), excluding private cars, taxis, professional transportation, delivery, etc. In the study on France, only transportation in the Paris region (Ile de France) was covered;
- security in urban transports covers both attack prevention and petty crime and European citizens could be sensitive to such issues.

Sector characteristics

- this sector lies within the responsibility of municipal or local authorities. Operators are rail and bus companies, which may in some cases be public (often municipal) bodies (in particular in Germany, the Netherlands and the UK);
- in the same locality, different types of players (police, transport operators, local authorities, etc.) are present

1.2.2 Airport security

Sector coverage

- the sector covers mainly the airport and passenger/baggage traffic, rather than the border aspect;
- the sector covers specific security aspects such as threat elimination mainly through baggage and passenger control. It does not cover safety aspects, air traffic control;
- the sector does not include customs, contraband and drug detection, immigration controls.

Sector characteristics

- this sector lies within the scope of European Commission, which contributes to the harmonization of European regulation;
- trans-national issues are at stake in airport security, because the countries of departure and arrival are both concerned, as well as each country that is flown over;
- this is reflected in the importance of international bodies in this sector (ICAO, ECAC and EU)

- air transportation still has an important development potential;
- competitiveness of European industry has to be improved against mostly American suppliers;
- this sector drives technology in the fields of ID control, biometry, baggage and passenger screening;
- airport operators are often private companies, but can also sometimes be publicly owned (as Manchester Airports in the UK). The airline operators are less involved in the airports;
- in security enforcement the main players are private security companies, as well as the police forces or dedicated border agencies

1.2.3 Maritime borders

Sector coverage

- in this sector the study focuses on the *borders* rather than the *harbours*, unlike airport security where the opposite option was chosen;
- in this case the distinction between security, safety, and contraband or immigration control is not so strict;
- the activities covered are marine approaches and borders control, rescue and safety, pollution prevention and control, immigration, contraband and illegal traffic.

Sector characteristics

- at the European level, the Commission outlines a common framework for setting up a "European border surveillance system" (EUROSUR).
- the study focuses on the activities covered by public bodies such as the Navy, Coast Guard, Customs, Sea Rescue, Border Control;
- the other players, harbour operators or shipping operators, are involved in activities such as freight handling and control that are not covered.

1.2.4 Critical infrastructures

Sector coverage

- for the EU, critical infrastructures are the physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU countries;
- the European Critical Infrastructure Directive[10]'s scope concentrates on the energy and transport sectors and their subsectors:
  - Energy:
    - Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity security systems and procedures
    - Oil: Oil production, refining, treatment, storage and transmission by pipelines
    - Gas: Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
  - Transport: Road, rail, air, inland waterways, ocean and short-sea shipping and ports

[10] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Additional sectors might be added with the review of the Directive.

- the different types of critical infrastructures raise different issues. We chose to cover selected aspects in different countries, because of our very tight time-schedule.

Coverage of critical infrastructures

	Electricity		Water
	Production	Transport	
France	X		
Germany	X	X	
Netherlands			X
The UK	X	X	

Sector characteristics

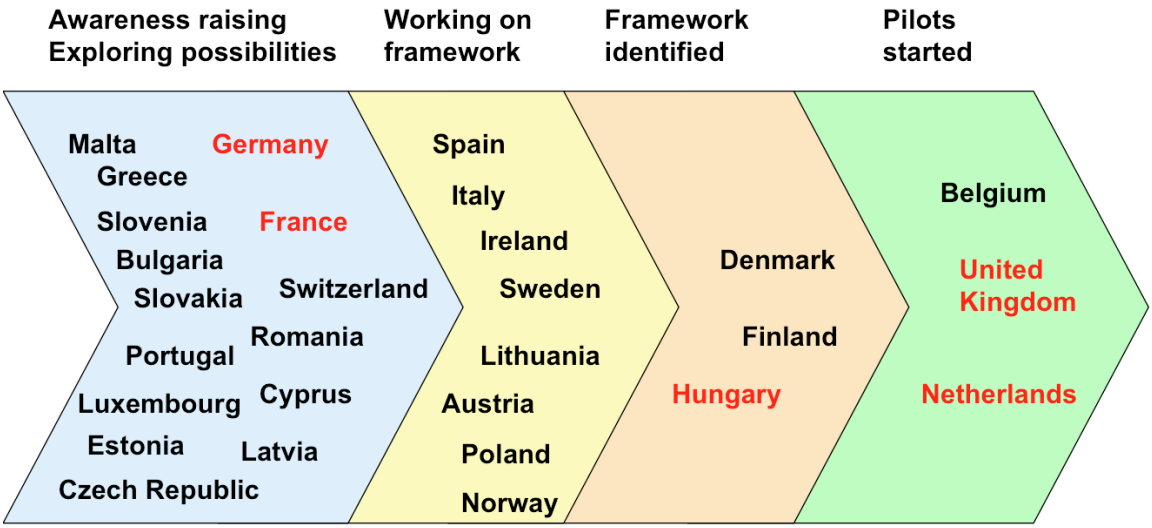
- the international and external dimension of critical infrastructure protection is important. Disruption or destruction of a particular infrastructure may have consequences for countries inside and outside the Union and vice versa;
- power availability is an important European issue, given the interconnection of networks. An attack on a nuclear power plant can also have consequences for the population of several European countries;
- in the water sector security R&D has become a topic after 9/11. The water companies realised that they had to take action to increase security;
- players are both public and private, and local or transnational.

1.3 Selected countries and consultation of stakeholders

When it comes to security, investments are to be done on a large scale. Therefore, we chose to focus our analysis on countries with a significant organization and activity in terms of R&D, more particularly in the field of security:

- Germany;
- France;
- The UK;
- The Netherlands.

Countries covered in the national case studies (in red)



Source: European Commission

The degree of awareness and implementation of PCP in the European Member States is fairly limited so far and this country selection has also been guided by the fact that we wanted to integrate both countries with existing experiences of PCP either in the field of security or elsewhere (UK and Netherlands), but also countries with no existing PCP programmes (Germany or France).

Moreover, we wanted to broaden our analysis to Hungary, a smaller East-European country that is particularly active and motivated in PCP (through pilots like the RAPID Project). However it was not possible to gather information consistent with the other countries studied, in particular because the country is in the process of restructuring its organisation.

Stakeholders per country and sector

Country	*Maritime Border*	*Airport Security*	*Urban Transport*	*Critical Infrastructure*	*Other transversal stakeholders*
France	Cassidian, DCNS.	Morpho, DGAC/STAC, EADS/Sodern, MultiX.	PPSL, Thales Security Solutions & Services, Ministry of Transport, SNCF, RATP.	EDF*, GDF*	ANR/DGA, Ministry of Interior, SGDSN.
Germany		Smith Detection Germany.			Cassidian Germany, VDI, BMBF**, BMWi**, BMVg**, BMI**.
Netherlands	Koninklijke Marechaussee, Thales Nederland BV, Ministry of Defence Procurement department.	NCTb, Schiphol Airport.	NCTb.	Rijkswaterstaat, Vitens.	Ministry of Economic Affairs, Agentschap NL.
Hungary* **					RAPIDE Project
United Kingdom	British Ports Association, UK Border Agency.		UITP, BAE Systems, Transport for London.		ADS-Aerospace Defence Security Industry Association, Technology Strategy Board (TSB – Trade Ministry), Centre for Applied Science and Technology (CAST), Science and Technology Unit Office for Security and Counter-Terrorism UK (Home Office).

* Contact request only

** Conference held with DECISION and Manchester Institute on July 14th 2011

*** About Hungary, we contacted GDF-Suez Hungary, but we could not get any answers. The Hungarian Ministry of National Development, for which the authority of the RAPIDE Project had given us contacts, also did not answer us. Eventually, it was also impossible to get valuable security information from the Hungarian security industrials.

2 Sector and country overview

2.1 Sector overview

We shall first review the organisation of the four sectors in each country, before looking at the different forms of procurement organisation or typologies that can be seen, and the different characteristics of each sector.

2.1.1 Sectorial organization at the country level

2.1.1.1 Urban transportation

- the operators are mostly local;
- there is as yet little cooperation between players, except on a national level;
- video-surveillance is the main security measure, and is transverse to public transportation and urban environment in general.

France:

Regional local authorities are the organising authorities for rail transport, with state-granted operating budgets. They sign conventions with the operators. The regional and the departemental local authorities in Ile de France have created the STIF, which is in charge of organising, co-ordinating and financing public passenger transport in Ile de France. Funding is dealt with in contracts between STIF and operators. The prescriber is always the Ministry of the Interior. There is no funding mechanism for R&D specific to urban transport.

Germany:

Urban transport is in charge of the Länder, and security in this sector is a regional police (*Länderpolizei*) matter, whereas the national railway system is under State responsibility, and is protected by the federal police (*Bundespolizei*)).

Netherlands:

The three largest cities Amsterdam, Rotterdam and The Hague have a municipal public transport company offering bus, tramway and metro services (GVB, RET, HTM). All other cities have public transport services offered by private operators. The main stakeholders in the area of security are the National Coordinator for Counterterrorism (NCTB), the Urban transport companies, the municipalities, the Police.

United Kingdom:

Local and regional transport executive bodies commission transport services from private operators, bus companies and train operating companies or TOCs. In the London area, the operators are mostly publicly owned, in this case by Transport for London. Security within transport systems is addressed by operators of the service and the infrastructure providers jointly and by law enforcement agencies, including the Police and a dedicated railway police force (the British Transport Police).

The Transport Security and Contingencies Directorate (TRANSEC) was set up as a separate unit within the Department for Transport (DfT) following the Lockerbie bombing of 1988. It regulates security issues for the transport industries i.e. aviation, maritime, channel tunnel, heavy rail, London underground, light rail (DLR in London and the subway in Glasgow only), road (transportation of dangerous goods only). TRANSEC devises and enforces security measures with due regard to their deliverability and proportionality, based on the nature and scale of the prevailing.

Private security services are also provided at certain times with the forthcoming Olympics likely to lead to extensive use of private security services to ensure the safety of the public using urban transportation system to attend the games.

Regarding urban transportation, central Government supports security through its own PCP scheme within the urban environment through one competition funded by the Home Office.

Urban transportation: the players

Country	*Functional prescribers*	*Technical prescribers*	*R&D funding*	*Equipment Procurement*	*Users*
France (Ile de France region)	Police forces	SNCF, RATP	ANR, companies	STIF, FIPD, SNCF, RATP	STIF, SNCF, RATP, CNIL
Germany	Public & private operators, local authorities, police	Public & private operators, local authorities, police	BMBF	Operators	Regional police forces
Netherlands	Public & private operators, local authorities, police	Public & private operators, local authorities, police	Public & private operators, local authorities	Public & private operators	NCTB, public & private operators, local authorities, police
United Kingdom	Police, Transport Police, DfT-TRANSEC	Private operators	Home Office	Private operators	Private operators, police, security forces

2.1.1.2 Airport security

- the operators are mostly local, although larger groups exist;
- there is strong international cooperation, through European and international bodies;
- baggage and passenger screening and control are the main security measures, which are specific to the sector, although they may find some markets elsewhere.

France:

There are two different players, the State whose objective is to reinforce security, and the airport operators whose objectives are mainly profitability. The police forces, the customs, the Civil Aviation authority and its technical service (STAC) are prescribers (approval of security schemes, elaboration of technical specifications), but the airport operators purchase the security equipment.

Germany:

Airport security is run by the federal police (*Bundespolizei*). People working at the various checkpoints are employed by private security companies, but are overseen by the federal police. Customs are also responsible for some security aspects (control of transported goods.

Netherlands:

The main stakeholder in the area of airport security in the Netherlands is the ministry of Justice, overall responsible for the security of airports in the Netherlands, who delegates the execution of this responsibility to:

- the National Coordinator for Counterterrorism (NCTB), directorate Airport Security, also responsible for the monitoring of the airport security system and the quality of airport security.
- the ministry of Transport, co-responsible for airport security, who must approve security plans
- the airport operators and the airlines, responsible for the operational execution of security measures
- the Koninklijke Marechaussee (Military police), responsible for overseeing the security tasks of the airport operator and airlines.

The main private operators are the airlines. Schiphol airport is a public company (shares owned by the national, regional and local government). Schiphol airport Group owns the regional airports of Rotterdam, Eindhoven and Lelystad. There are two other small regional airports, Maastricht and Groningen Eelde. The latter is owned by regional/local government, while the former is owned by private investor Omniport from the UK.

United Kingdom:

The Department for Transport (DfT) and a number of airport groups are the main actors for security research. The airports have the major responsibility for security arrangements. Each airport has to procure the security equipment individually, and is not financed by central government. TRANSEC, a body of the Department for Transport, regulates security issues for the transport industries i.e. aviation, maritime, channel tunnel, heavy rail, London underground, light rail, road, and has an R&D programme.

Airport security: the players

Country	*Functional prescribers*	*Technical prescribers*	*R&D funding*	*Procurement*	*Users*
France	ICAO, ECAC DGAC, SGDSN	DGAC-STAC	ANR, SGDSN	Airport operators	Airport operators
Germany	Conference of the Ministers of Interior of the Länder	Länder	BMBF	Federal Police	Federal police, private security companies, customs
Netherlands	NCTB, Min of Justice & of Transport, Operators	NCTB, Min of Justice & of Transport, Operators	Airport operators (some public)	Airport operators (some public)	NCTB, Min of Justice & of Transport, Koninklijke Marechaussee (Military police) Operators
United Kingdom	DfT-TRANSEC, Airport groups	DfT, Airport groups	DfT, Airport groups	Airport groups	Airport groups

2.1.1.3 Maritime borders

- the security players are national, operators of ports and shipping can be local or international;
- there is strong international cooperation, in particular through the EU agency Frontex;
- there is a strong link between security and defence, in particular through players like the navies or coast guards;
- vessel and personnel surveillance, identification and tracking, are the main measures, and they are specific to the sector.

France:

The public players (navy, maritime police, maritime affairs…) are locally under a single authority, the Marine Prefect, which facilitates the expression of needs and synergies; in maritime surveillance needs are practically identical in the security or military fields

Germany:

A special branch of the federal police is in charge of the protection of the maritime borders: the police for water protection (*Wasserschutzpolizei*). The responsibility is also shared with the concerned Länder, through the regional police

Netherlands:

The main stakeholders are the Coast guard, responsible for providing the required equipment, such as vessels, the Koninklijke Marechaussee (part of the Dutch army), responsible for border control related to persons, the Customs, responsible for border control related to goods; the Defence procurement department, responsible for procuring expensive equipment for the army, such as vessels

United Kingdom:

For maritime border security the UK Border Agency and UK ports are the main actors. The Border Agency is tasked with protecting the UK border (not only maritime), and is one of the largest law enforcement agencies in the UK. Most British ports are either under private ownership, municipal control, or are run by a trust. They operate as commercial entities and do not receive systematic financial support from the UK Government. They compete with each other and are keen to protect their independence

Maritime borders: the players

Country	*Functional prescribers*	*Technical prescribers*	*R&D funding*	*Procurement*	*Users*
France	Navy, DAM, Maritime police, Customs	DGA, DAM-SDSIS, CROSS	ANR, DGA	Navy, Customs, police, CROSS, operators	Navy, Customs, police, CROSS, operators
Germany	Conference of the Ministers of Interior of the Länder	Coastal Länder	BMBF	Coastal Länder	Special branch of the Federal Police, Coastal Länder
Netherlands	Coast Guard, Army/Navy, Defence, Customs	Coast Guard, Army/Navy, Defence Customs	Defence	Defence, Army/Navy	Coast Guard, Koninklijke Marechaussee (Military police), Army/Navy, Defence, Customs
United Kingdom	Navy, Border Agency, Coast Guard, port operators	Navy, Border Agency, CAST	Navy, Border Agency	Navy, Border Agency, port operators	Navy, Border Agency, port operators

2.1.1.4 Critical infrastructures

- the operators are local, national or multinational;
- there is little cooperation;
- the main security measures are site, grid and network protection in diverse technical environme nts (electricity, water);
- different infrastructures were studied in different countries.

France:

The infrastructure studied was electricity production.

The MEDDTL (ministry of ecology, sustainable development, transport and housing) is in charge of risk prevention. Security in the field of electric energy is organised through the vitally important sectors (SAIV) security action directed by the SGDSN.

Germany:

Critical infrastructures (here electricity production and transport) are the responsibility of the private sector, and also of the Länder. The Ministry of the Interior (BMI) is also involved through the BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), the Federal Office for Civil Protection and Disaster Assistance.

Netherlands:

For the Netherlands the study covers the water distribution sector. The Ministry of Infrastructure and Environment and RWS are responsible for the main water infrastructure in the Netherlands. Other players are the water companies (public companies), VEWIN, branch organisation of water companies; KIWA, branch organisation of engineering companies (active among others in the water sector), WETSUS, centre of excellence for sustainable water technology, Reststoffen Unie, branch organisation

responsible for processing residue in the water. The main responsibilities for security in the drinking water sector are with the drinkable water suppliers.

United Kingdom:

The Department of Energy and Climate Change (DECC) is the policy-maker for the issues concerning the security of electricity generation and transmission. The regulation of all the energy markets is in the hands of the Gas and Electricity Markets Authority, supported by the Office for Gas and Electricity Markets (Ofgem). Ofgem is independent in its decisions from the ministry. There is a fragmented market in terms of generation, transmission, distribution and supply. The Centre of for the Protection of National Infrastructure (CPNI) provides protective security advice to businesses across the national infrastructure.

Critical infrastructures: the players

Country	*Functional prescribers*	*Technical prescribers*	*R&D funding*	*Procurement*	*Users*
France	MEDDTL, SGDSN, operators	MEDDTL, SGDSN, operators	ANR, SGDSN	Operators	Operators
Germany	*	*	BMBF, BBK (BMI)	Operators	Operators
Netherlands	RWS, water companies, KIWA	RWS, water companies, KIWA	RWS, water companies	RWS, water companies	RWS, water companies
United Kingdom	DECC	DECC, CPNI, operators	TSB	Operators	Operators

** it has not been possible to identify the corresponding stakeholders based on consultations and desk-research*

2.1.2 Procurement issues

In the sectors studied, security is generally not the operators' core business (except to some extent for maritime borders), but it is more directly the concern of the political authorities and the citizens.

Responsibilities are generally split between public bodies tasked with prescribing security measures, and operators (generally private) who are tasked with implementing them and procuring the equipment. For private operators, security is often a necessary burden although some threats can also affect them directly (vandalism, piracy…).

As a consequence, prescription and procurement are often dissociated. According to the respective roles of the players, different procurement configurations or typologies can be distinguished, that can have different implications as to policies that can be implemented.

2.1.2.1 Procurement typologies in the security field

A general typology for public procurement has already been described (see 1.1.1). Let us develop this typology for the specific field of security.

Indeed we have seen how Edquist and Hommen have made the distinction between direct and "catalytic" public procurement:

- The State procures technology (public technology procurement)
  - the State procures technology because it needs it for its own markets (e.g. defence, ICT...). This is direct public technology procurement

- the State procures technology, although it has no internal market for it, because it "needs" it for societal reasons (e.g. environmental friendly refrigerators, or security...). This is catalytic public technology procurement.

- Technology procurement is dealt with by the private sector. In this case one may have cooperative technology procurement. But not necessarily, there can also be direct technological procurement if a single player wishes to and is in a position to do so.
- A fourth, mixed, category can be added, where the public body that carries out the procurement is one, but not the only, intended end-user of the product in question. This is another form of cooperative technology procurement, and it can occur between several public procurers across sectors or countries, or between public and private procurement.

Configurations in the field of security vary according to the particular sector (and to a certain degree, according to the country):

Three of the studied sectors (airport security, urban transportation, critical infrastructures) fall into a category where catalytic procurement is more the rule, since public bodies drive and fund R&D but the procurement of the final equipment is (mostly) by the private operators. In some countries the operators sometimes remain public bodies, but they are distinct from those in charge of security as such.

In these sectors, in order to develop efficient security R&D, national public body involvement could take the form of PCP-POV in the future. This has already begun in the UK. Although according to the Home Office, as well as the Aerospace Defence and Security Industry Association (ADS), pre-commercial procurement is not extensively used in the field of security, to date we could identify several application of PCP in the area of security (INSTINCT, Intent in Crowded Places and Hot Products). They are all competitions run under the UK Government's SBRI scheme i.e. through the Technology Strategy Board, with the involvement of the Home Office (see UK country study for more details). However, for the moment public body involvement in the EU is still mostly through national programmes or EU FP7 projects.

For maritime borders, the public bodies will also be involved in the actual equipment procurement (direct procurement) resulting from the R&D programmes. Moreover there is call for a POV project in WP2012 for maritime border surveillance tools.

2.1.2.2 Sectors show different procurement configurations

Sector configurations differ as to relative public-private involvement, and in the various countries the status of operators can be either public or private, or frequently a mix of the two. It is likely that in most cases bundling of operator demand should bring benefits (market scale effect, interoperability, standardisation, improved cost efficiency of security).

Procurement according to sectors: a varying mix of public and private players

Sector	*Functional prescribers*	*Technical prescribers*	*R&D funding*	*Procurement of final equipment*	*Users*
Urban transport	Police & security forces	Local operators, RTOs	Local operators	Local operators	Police & security forces
Airports	ICAO, ECAC, EU, State	State RTOs	State	Airport operators	Airport security
Maritime borders	Border authorities, Navy, Customs	Border authorities, Navy, Customs	Border authorities, Navy, Customs	Navy, Customs, Border auth., port operators	Shipping operators, Navy, Customs Border Auth.
Critical infra-structures	State	State, operators	State	Operators	Operators

Dark grey zone: public bodies
Light grey zone: private and public mix
White zone: private players

Prescriber characteristics

- Security needs are specific to each sector rather than to each country;
- Public bodies are generally in charge of security issues, which are a transverse societal need, and often not a vital preoccupation for the operators;
- They also generally are in charge of R&D programme definition and funding;
- They often cooperate on the European and international level (airport security, maritime borders, water).

Procurer characteristics

- Procurers of R&D services are often the public bodies involved in prescribing;
- Procurers of equipment are generally different from prescribers and R&D service procurers;
- Except in the specific case of maritime borders, procurers of equipment are generally the operators (private companies or in some cases public bodies).

Operator characteristics

- Private companies, or, in some cases, public bodies (national or local);
- Their needs are generally similar or identical in each sector;
- They are dispersed, but do not generally compete on security issues;
- They tend to become international (acquisitions)

2.1.2.3 Sectorial coordination, international cooperation are key

National coordination and international cooperation are key conditions for the development of efficient security and innovation in the field, but they are unequal in the four sectors studied.

State and private operator involvement (in R&D activities, security R&D, security procurement) vary considerably from one sector to another but in every case a number of different players (both public and private) are involved, and it is essential that they are coordinated in order to harmonise expression of

needs, specifications, R&D and procurement. Bodies in charge of coordination in the security field have been instituted in the countries selected.

Security strategies require international cooperation, in particular because threats are largely international. International cooperation (ECAC, EU, ICAO, Frontex…) is very important in airport security and maritime borders, which are by nature cross-border activities. These are also the sectors where State involvement is greatest (for strategic and historical reasons).

Other transverse European or international bodies may play a part in innovative security procurement procedures in all sectors. Europol (police), Enisa (Information Society Security), or W-SMART (water utilities), and ERA for railways (which touch urban transportation), are organisations of this kind.

The existence of such international structures can be a precious help in facilitating discussion, harmonisation, and the emergence and management of cooperative projects

All these sectors, where public involvement is more or less direct, require a large measure of cooperation between the public and private sectors, which may take the form of public-private partnerships. PCP-POV procedures can contribute to this, and could also contribute to resolving acceptability issues, by involving all players throughout the supply chain.

Involving all the players throughout the supply chain is important if innovative solutions that effectively answer the needs of the market and of the prescribers are to be found. This requires the involvement and coordination of prescribers, procurers, suppliers and users, from the very beginning of the project.

International involvement is different according to sectors

Sector	*European structures*	*International structures*
Urban transportation		
Airport security	ECAC, EU	ICAO
Maritime borders	Frontex, EU	
Critical infra-structures	W-smart	

2.2 Country overview

2.2.1 General approach to security

2.2.1.1 Security: a priority for each country

First of all, it is important to note that security is a priority in all the countries we studied. Most of them have made security into a national priority issue, often linking it with defence.

They have formalised this in security master plans:

- France: White book on “Defence and Security”, and COSG (Concepts and Tools for Global Security) an R&D programme in cooperation with Germany
- Germany: “Research Programme for Civil Security”, driven by the BMBF (Ministry for Education & Research)
- Netherlands: A national R&D program for the field of societal security has been developed, under the coordination of the Ministry of Interior Affairs
- UK: “National Security Strategy” (2009), the counter-terrorist strategy CONTEST outlines the assumptions, priorities and the approach, and a specific Science and Technology Strategy for Countering International Terrorism states the research priorities until 2012.

2.2.1.2 Coordination, cooperation, and market unification

Coordination at the national level and international cooperation are crucial both for efficient security and for unifying the European market and promoting innovation and the competitiveness or the European security industry.

Coordination in each country between the public bodies concerned is a necessary first step, if efficient, harmonised measures are to be implemented, and if innovative solutions to be found and brought to the market. This coordination process has been started in most countries.

At the national level, bodies or structures have been established to better coordinate actions between the involved ministries:

- France: the SGDSN, reporting to the Prime Minister, coordinates government action, and the GTN Security is a forum grouping the technical ministries concerned and public and private research bodies.

- Germany: the four concerned ministries ((BMBF-Education & Research, BMWi-Economy, BMVg-Defence, and BMI-Interior) coordinate their actions towards the Research Programme for Civil Security. An independent expert group, the “Scientific Board Security Research Programme”, advises the Federal Government in matters concerning security research.

- Netherlands: in the societal security field the Ministry of Interior Affairs coordinates the other involved ministries and takes care of the connection with European R&D programmes like FP7.

- UK: OSCT and cross-Government CONTEST board and CONTEST Science and Technology Board.

These coordinating bodies are also natural contact points for the necessary international cooperation. This cooperation aims to coordinate and harmonise the various national topics and the European topics, and to promote a transverse vision of the importance of technologies, with the potentialities of dual cross-fertilisation

International cooperation ranges from structured sectorial bodies or agencies (ICAO, ECAC, Frontex, W-SMART…) through multi or bilateral structures or agreements (mostly with non-EU countries), to case-by-case consortia for European R&D Framework Programmes.

However the involvement of the whole supply chain, from prescriber to end-user, remains to be achieved. This is where PCP-POV can bring a valuable contribution, and at the same time improve cooperation inside the European Union.

2.2.2 Specific approach to security R&D and PCP per country

All governments consider security as a strategic domain, and that the competitiveness of the security industry in Europe should be reinforced. Governments that have already introduced PCP are favourable to the principle, but have not yet been able to assess its efficiency, and the others consider that if PCP-POV proves to be a useful tool, then it should be developed. However positions on PCP remain on a general level and are not specific to the security field.

Government positions.

- France: wishes to remain heavily involved in the European programmes. If these programmes are to be implemented in the form of POV or PCP, this will not affect French interest, but only if public authorities are somewhat encouraged to procure the final equipment. But presently there is no PCP scheme at the national level. There is a degree of coordination in the expression of needs for security R&D (capability driven), in particular via the meetings of the security GTN (national thematic group);
- Germany: the German Federal Government considers the security industry an important sector of innovation; it made safety and security of citizens one of the four priorities of its “High-Tech Strategy for Germany”. So far there is no official public German point of view on PCP/POV, although the answer to the EC Consultation on an Industrial Policy for the Security Industry (April-May 2011) was negative.
- Hungary: PCP and commercial procurement can reinforce the innovation capacities of Europe. The Hungarian Government has decided to put PCP (and more generally R&D) among its priorities;
- The Netherlands: A national R&D programme for the field of societal security has been developed. In the Netherlands. PCP has been introduced in 2005, using the already existing American SBIR programme as a starting point. Three programmes have been identified in the field of security.
- The United Kingdom: the UK has been one of the first EU countries to apply PCP as a policy tool. Some programmes in the field of security have been identified.

I**ndustry** positions are more operational, looking at what the results are for industrialists in terms of markets, costs and delays... Weighing the pros and cons is still difficult due to the lack of sufficient experience of the new procedure and its results.

Pros of PCP in civil security:

- Involving the end-user and end-market early in the R&D process

- Acceptance by national or supra-national authorities of a security product implies that the product meets its goals
- Enabling a shift from pure R&D to capacity development with the involvement of the end-users

Cons of PCP in civil security:

- Industrialists supplying equipment and systems criticise the fact that POV and PCP schemes do not solve the problem of the link between support to R&D and equipment acquisition. They consider the proper scheme is the “programme” concept used in the armament field. However that cannot be applied in the security field, because R&D funders, prescribers and operators are often three distinct entities. Public bodies should give assurance of acquisition at the end if they want to make PCP/POV attractive.
- The time to market in security: PCP/POV schemes might be too lengthy because of the iterative process.
- Development, validation and testing of a product through the mid to upper TRLs (Technology Readiness Levels) is more costly compared to low TRL research. Thus industrialists would like the final procurers to fully fund the programme.

Finally, industry is in favour of the availability of a whole range of instruments and procedures to be applied selectively on a case-by-case basis.

2.2.2.1 France: a defence-based approach

In France security was recognised as a strategic issue in 2008 and added to Defence in the SGDSN. Security is dealt with in the concerned Ministries, as well as the SGDSN, the GTN Security, the ANR (CSOSG global security programme in cooperation with Germany).
The GTN Security is a forum bringing together public bodies and private research. The elaboration of road maps is a major objective.

However, no PCP-POV projects have yet been launched in France. Specific security R&D funding including both national and EU funding is in the average of 30 million € per year.

In France manufacturers believe that the best arrangement would be that the operators commit themselves to purchase the equipment resulting from the development. This is the “programme” concept, with the contractual automatic succession of R&D stages and acquisitions, as is practised in armament programmes.

However armament and security are two different worlds. In the former there is only one buyer and prescriber, whereas in the latter R&D funding, prescription, acquisition and implementation are often done by different entities. In armament there is a programme approach with a global commitment linking R&D investment and acquisitions, and this is not the case in security.

Possible recommendations for PCP (based on conducted interviews):

- Propose projects with well-defined objectives, and clearly identified deliverables, whose added value for the user is easy to appreciate. At the end of a project, providing a prototype or a mock-up enables a real feed-back on the implicit specifications of the user;
- It is not possible to task private third parties with defining specifications for matters of security concerning the State, nor even with validation. The public users do not have the necessary

competencies, so an authoritative public third party would be needed, i.e. a public procurement agency tasked with specification and validation;
- the succession of contracts may cause delays to accumulate unless it is possible to negotiate the contracts all together;
- design projects with detailed stage points, corresponding to real evolutions. This will enable the user, who always finds delays too lengthy, wait in patience until the project is completed
- A PCP or POV is not of the same nature as a research programme. There should be a rule restricting such projects to the 27 member states, excluding « associated » countries (Turkey, Israel, Russia) and other countries.

2.2.2.2 Germany: European and bilateral programmes

Germany is among the countries that benefit most from European fundings. The FP7 SEC 2011-1 call shows Germany's position improving to become the top beneficiary of European funds, with 36 million euros compared to 20 million euros in average for the period 2007-2011.

German national funds are mainly provided through the Forschungsprogramm für die zivile Sicherheit (research programme for civil security), which is driven by the BMBF.
All the concerned ministries are involved to set objectives (economy, defence, health, transport).

It consists of two programme lines:
- The first programme line refers to scenario-based security research. This means that research considers the needs of users from the outset. The focus is thus not on solutions to individual problems but on suitable system innovations;
- The second programme line aims at studying the generic technologies within the framework of mixed-technology networks, which are needed in many scenarios. These networks combine the technologies for quick and reliable identification of people, quick and mobile identification of hazardous substances, pattern recognition and security and rescue capacity building.

Cooperation between the Research Ministry and the other government departments is an important part of the programme. Research, legislation, regulatory support, international cooperation and procurement in the area of civil security are considered to form an integrated whole.

Another objective of this strategy is to increase the competitiveness of security companies and to achieve technological leadership in specific security technologies

The decision-making process also relies on independent experts (academia, industry, end-users, etc.). To date, the Federal Ministry of Education and Research has published twelve calls for proposals within this programme. Such projects are partly funded by the BMBF (up to 50%), and the consortia bring the rest of the funds.

There are also a number of bilateral programmes, for which each country funds its own partners, with Germany coordinating the whole process in the end:
- Cooperation between Germany and France
  - A BMBF call on Cooperation in Civil Security Research between Germany and France within the Framework of the Federal Government's "Research for Civil Security" Programme. French funding will be provided by the ANR "Concepts Systems and Tools for Global Security CSOSG 2011".

- funding can also be granted to independent projects dealing with overarching societal policy and cross-cutting issues. For this coordinated call a Partnering Platform and a Partnering Event support French and German potential applicants in forming joint consortia

- Cooperation between Germany and Israel:
  - In 2008, the BMBF, the MOST (the Israeli Ministry of Science, Culture and Sport) and MOITAL (the Israeli Ministry of Industry, Trade and Labour) signed a Joint Declaration to start collaboration in the area of civil security research.
- Cooperation between Germany and the United States:
  - An intergovernmental agreement between Germany and the USA on cooperation in the field of civil security research was signed in 2009. Germany and the USA also signed a Preventing and Combating Serious Crime (PCSC) Agreement in 2008 to allow information sharing of fingerprints on suspected criminals and terrorists. In addition, Germany plays an important leadership role in advancing counterterrorism cooperation between the United States and the European Union.

2.2.2.3 Hungary: PCP as a means to structure R&D policy

Low quality of its business environment is one of the most important structural weaknesses of the Hungarian economy. A new public procurement law was adopted in July 2011, and a comprehensive programme has been launched, in order to:

- reduce the administrative burden on enterprises;
- improve the regulatory-institutional elements of competitiveness, of quality of public services, of domestic capital market:
- achieve an increase in the level of research and development expenditures up to 1.8 per cent of GDP by 2020.

Other initiatives include the establishment of the National Research, Innovation and Science Policy Council, and the creation of the unified institutional system of development policy.

Under the umbrella of the New Széchenyi Plan – Science and Innovation Programme - the Hungarian Government has decided to put pre-commercial procurement (PCP) among its priorities and the Észak-Alföld Regional Development Agency currently leads a PCP pilot project.
This project was realized under the umbrella of the RAPIDE programme. The aim of the programme was to help businesses, mainly SMEs, and to bring innovative products and services to the market in a reduce timeframe.
The Agency is funded by the Hungarian State (through the Hungarian Innovation Fund), and by other sources (public owners, universities...). The budget might be quite small (300 000 euros), but the programme respects the 3 PCP phases with a competitive development process. The project is still in progress, but does not target security.

2.2.2.4 Netherlands: the SBIR approach

There is experience of cooperative R&D related to security in the domain of critical infrastructures (water), and indirectly in the maritime border security domain, where many actors are linked or even part of the Defence industry.

In both of these sectors, water and maritime border security, the advantages of cooperative procurement are recognised and also both indicate their interest in PCP schemes.

The R&D budgets in the Netherlands, mainly based on labour fees, are estimated at around 10 million Euro per year for the security industry (0.5% of total turnover in labour fees of WBSO (Fiscal stimulation arrangement for R&D) of 2.1 Billion Euro), and around 40 million Euro for the Defence related industry (about 1.9 % of WBSO).

The Dutch SBIR programme

In the Netherlands PCP has been introduced in 2005, using the existing US SBIR program as a starting point. SBIR has not been applied to the security domains covered by this study, although some projects related to security in other fields have recently been awarded (see chapter 3.1):

The SBIR program in the Netherlands consists of the following three phases:

- Feasibility, technical, market, organisation; time schedule
- Research, development, prototyping, test series or demonstration;
- Product ready for the market, lancing of the product; phase 3 is the responsibility of the companies themselves and is not financed by the government.

The Dutch government bodies are satisfied that the programme results in actual products that are provided to them, in other words that a SBIR tender always results in an actual innovative product.

SBIR fits very well with the current policy ideas in the Netherlands. Companies, including SME's are working together to provide actual innovative products, which are intended to solve current societal problems. SBIR offers an opportunity to have a real influence on the part that SME's can play in the market.

For a lot of companies, SBIR projects lead to new activities, which they otherwise would not have started. The SBIR process with its fixed price and its obligation to provide actual tangible results is positive for the business environment.

Some recommendations on the evaluation of SBIR programme based on interviews conducted:

- The government should follow the companies, including in phase 3. Although the financing is ended after phase 2, an SBIR project is only completed after a successful phase 3;
- The ministry of EL&I (Ministry of Economic affairs, agriculture and innovation) is advised to investigate what role the government could play in the third phase of SBIR. This could be for example non-financial support to companies and stimulation of new markets;
- In cases where the government is an important potential client, it should start from the beginning to think about the role of the government as first buyer;
- The ministry of EL&I is advised to keep flexibility in the program, which results in each SBIR call for tender remaing tailor-made. The ministry is also advised to keep one organisation responsible for the execution of SBIR, preferably AgentschapNL. In this way all parties can learn from experience in the different SBIR calls for tender.
- focus on interoperability in Dutch SBIR programs is an efficient way to promote more cooperation within industry, and it also supports the standardization process in Europe in this area.

2.2.2.5 United Kingdom: concern about industry fragmentation

The Government's Consultation Paper on Equipment Support and Technology for UK Defence and Security expressed the concern that the fragmented structure of the UK security market may place UK companies at a competitive disadvantage

The UK's National Security Strategy was published in 2008, updated in 2009 and 2010: it is a single strategy bringing together the objectives and plans of all Government departments, agencies and forces protecting national security, including both defence and security.

The UK Government conducts security research and development work mainly as part of the fight against international terrorism (CONTEST counter-terrorist strategy).

The main bodies in security research are the Office for Security and Counter-Terrorism (OSCT) with its CONTEST Science and Technology Board and CAST Centre for Applied Science and Technology (Home Office), and the Counter-Terrorism Science and Technology Centre (Ministry of Defence)

TRANSEC is a body that regulates security issues for the transport industries i.e. aviation, maritime, channel tunnel, heavy rail, London underground, light rail (DLR in London and the subway in Glasgow only), road (transportation of dangerous goods only).

The UK pioneer in PCP

The UK was one of the first EU countries to apply PCP as a policy tool:

- The Technology Strategy Board, which operates under the wing of the UK's trade ministry, BIS, runs the UK's flagship PCP scheme, the UK SBRI or Small Business Research Initiative. It should be noted however that this scheme is not the only part of Government, which undertakes PCP activities. The Department of Health's National Innovation Centre has also undertaken on its own account important procurement of innovation activities including PCPs since 2006. Current changes in Government in the UK make it difficult to know how future UK PCP activity will be progressed and under which scheme such activity will take place. The UK SBRI was launched in 2001 but was not generally a success in that user departments did not engage with it. A re-launched scheme in 2004 where user departments were compelled to use the scheme for a proportion of expenditure saw more engagement.
- The Energy Technologies Institute (ETI) operates a pre-commercial procurement scheme in the area of energy. The UK Energy Technologies Institute was set up in 2006 as a private company, made up of global energy companies and the UK Government.
- TSB runs R&D competitions on behalf of user departments in the UK. Competitions normally extend through phases 1 and 2 of the innovation cycle but use of all stages for a competition is not essential. Test series of pre-commercial products are not funded in the UK's TSB. IPR is left with the company in nearly all cases by default. However, the UK Government normally retains rights to use the technology

Industry wishes use of PCP in security

According to the Home Office, as well as the Aerospace Defence and Security Industry Association (ADS) pre-commercial procurement is not yet extensively used in the field of security.
ADS would welcome the extension of PCP to civil security, as it is seen as a valuable route to product for end users and companies. A stronger link is required between the research programme and the end-user.

Opinion of the Aerospace & Defence Industry on PCP:

- There cannot be protectionism at the level of research procurement;
- There would have to be some mechanism so that there will be an element of competition among the prime contractors;
- If PCP is about an integration project, then the Commission might not take it in-house but prime contract it to some contractor with experience in a pre-commercial environment;
- There are mechanisms through which the Commission could mandate involvement of SMEs
- Transparency is key;
- Involvement of the entire supply chain is called for.

Some recommendations on PCP based on conducted interviews:

- EU level action to support PCP might be most suitable for those cases in which EU institutions or agencies exist and could address security issues. Examples are ICAO, FRONTEX or EUROPOL, whose role, can go from organising cooperation to recommending or even procuring technologies.
- The Commission should link its PCP policies with activities on standardisation and conformity assessment of security products, systems and services to pursue a comprehensive approach for the promotion of innovation in the field of security.
- The EU should take active measures to **'educate the market'**. Even in countries with running PCP schemes like the UK knowledge of PCP is still confined to certain public sector organisations. The situation is even more challenging in countries without such schemes. Public authorities as well as private actors need to be made aware, for example, of
  - The need for pre-commercial procurement;
  - The difference of between PCP, R&D grants and 'normal' procurement;
  - The reasons for additional instruments beyond those of the existing procurement legislation;
  - Challenges, pitfalls, solutions related to operating PCP;
  - Possibilities for EU support (from other Member States and from EU institutions).
- Finally, the Commission should pursue a **comprehensive approach** to promote innovation in the field of security. PCP is one element that could be fruitfully combined with standardisation and conformity assessment. The latter two are important instruments to opening markets both within the EU and in export markets. The EU is particularly well placed to set international standards. In this context specific attention should be paid to equipment that is developed in response to newly arising threats or where security functions are automated, as in the case of biometric identity cards and eGates at airports.

2.3 The US SBIR experience

2.3.1 SBIR and PCP similarities and differences

The Small Business Innovation Research (or SBIR) program is a United States Government program established under the Small Business Innovation Development Act of 1982 (P.L. 97-219) with the purpose of strengthening the role of innovative small business concerns in Federally-funded research and development (R&D).
The program mandated that all federal agencies spending more than $100 million annually on external research set aside 1.25% of these funds for awards to small businesses. In 1992, the Congress increased the size of the set-aside to 2.5%, which today represents an annual funding of about $2 billion.

The three key characteristics of the SBIR programme implementation are:
- Competitive development in phases;
- Assignment of IPR ownership with companies not with procurers;
- Separation of R&D phase from commercial deployment phase.

To that respect SBIR shares some fundamental similarities with Pre-Commercial Procurement as described by the European Commission although both programmes do not pursue entirely the same objectives. In addition, differences in the US versus the European legal context generate some differences in the implementations of both programmes:

The European Commission FAQ on PCP provides the following list of important differences between SBIR and the EU approach to PCP:

- Whereas participation in the US SBIR program is strictly limited to Small Businesses only, this is not what is proposed in the PCP Communication in compliance with the EU Treaty principle of non-discrimination. Indeed, early customer feedback on new product developments can be beneficial for companies of all sizes.

- Participation in the US SBIR program is limited to companies that are at least 51% US-owned and whose operated principal place of business is located in the US. The PCP Communication does not advise to use similar conditions in a systematic way; it suggests that public purchasers decide on a case-by-case basis on the openness to worldwide offers and on the relevant contract conditions, taking into account the full potential of the European Research Area.

- Some US federal government agencies organise the SBIR program mainly as a grant scheme (so-called "granting" agencies). Other US federal government agencies - mainly those with large operational responsibilities and thus large procurement needs - implement the SBIR program as a procurement scheme (so-called "contracting" agencies). The granting agencies let companies make the specifications for concrete project proposals in broadly defined areas of interest to the agencies. The contracting agencies define more concrete problems to be addressed and performance targets to be met. The PCP approach as described in the Communication is purely a procurement, which does not involve any grant or State aid element.

2.3.2 SBIR implementation

11 federal departments and agencies are required by SBIR to reserve a portion of their R&D funds for award to small business.

- Department of Agriculture
- Department of Commerce
- Department of Defence
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Transportation
- Environmental Protection Agency
- National Aeronautics and Space Administration
- National Science Foundation

SBIR is coordinated by the Small Business Administration (SBA, through its Office of Technology), which directs the 11 agencies' implementation of SBIR, reviews their progress, and reports annually to Congress on its operation. SBA is also the information link to SBIR. SBA collects solicitation information from all participating agencies and publishes it quarterly in a Pre-Solicitation Announcement (PSA). The PSA is a single source for the topics and anticipated release and closing dates for each agency's solicitations.
It is the responsibility of the 11 federal agencies participating to the SBIR programme to designate R&D topics and accept proposals.

Small businesses must meet certain eligibility criteria to participate in the SBIR program:

- American-owned and independently operated
- For-profit
- Principal researcher employed by business
- Company size limited to 500 employees

Following submission of proposals, agencies make SBIR awards based on small business qualification, degree of innovation, technical merit, and future market potential. Small businesses that receive awards then begin a three-phase program with the following definition as stated in the SBIR programme policy directive[11].

- Phase I: Phase I involves a solicitation of contract proposals or grant applications (hereinafter referred to as proposals) to conduct feasibility- related experimental or theoretical R/R&D related to described agency requirements. These requirements, as defined by agency topics contained in a solicitation, may be general or narrow in scope, depending on the needs of the agency. The object of this phase is to determine the scientific and technical merit and feasibility of the proposed effort and the quality of performance of the SBC (Small Business Concerns) with a relatively small agency investment before consideration of further Federal support in Phase II.

- Phase II: The object of Phase II is to continue the R/R&D effort from the completed Phase I. Only SBIR awardees in Phase I are eligible to participate in Phases II and III. This includes those awardees

[11] Small Business Reauthorization Act of 2000 (Reauthorization Act) Amendments to the Small Business Innovation Research Program, chapter 4, http://archive.sba.gov/idc/groups/public/documents/sba_program_office/sbir_policy_directive.pdf

identified via a "novated" or "successor in interest" or similarly-revised funding agreement, or those that have reorganized with the same key staff, regardless of whether they have been assigned a different tax identification number. Agencies may require the original awardee to relinquish its rights and interests in an SBIR project in favour of another applicant as a condition for that applicant's eligibility to participate in the SBIR Program for that project.

- Phase III: SBIR Phase III refers to work that derives from, extends, or logically concludes effort(s) performed under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. Phase III work is typically oriented towards commercialization of SBIR research or technology.

2.4 Quantitative impact of PCP-POV on industry: US SBIR experience and its potential implication for Europe

2.4.1 Quantitative impact – evaluation of SBIR programme

It is naturally very difficult to assess the impact of PCP-POV, innovative R&D service procurement procedures that are still very little used in Europe. A way round this difficulty is to look at assessments of the SBIR programme in the USA, a programme which now benefits from 30 years of experience.

2.4.2 The SBIR (Small Business Innovation and Research) programme metrics

Today, the SBIR programme represents annual funding of about $2 billion.

Phase I allows a business to provide proof of concept or to prove the feasibility of its idea. Awards usually hover around $100,000. Phase II takes that feasible idea into a demonstrative prototype and awards can be upwards of $1 million. Phase III is an "unofficial" phase as it does not include SBIR Programme funding, however it can include internal funding and perhaps outside source investment to bring the prototype into commercialization.

In total there were more than 23 000 SBIR applications annually for Phase I, during the period 2000 to 2009, amounting to a total of more than 232 000 applications. Out of this number of applications almost 32 000 were awarded (over 3 000 on annual average). The ratio of awards to applications for Phase I was about 14%.

In Phase II, in most cases, there are two companies competing for the award and the awarding rate is in most cases around 50%. On average each year, more than 3 000 applications for SBIR Phase II are received; and the total number for 2001-2009 was over 32 000.

The $2 billion spent annually through the SBIR programme is divided between Phase I and Phase II at roughly 25% and 75%.

2.4.3 Assessments of SBIR programme

The National Research Council in the USA carried out a substantial assessment survey of the Small Business Innovation and Research (SBIR) programme from 2001 to 2009. This comprised a general survey, and particular surveys by the five government departments that account for 96% of SBIR programme expenditures. In decreasing order of programme size, they are the Department of Defence (DoD), the National Institutes of Health (NIH), the National Aeronautics and Space Administration (NASA), the Department of Energy (DoE), and the National Science Foundation (NSF). The SBIR programme at DoD is the largest of all the SBIR programmes, and accounts for over half the programme's funding.

Concerning the NIH more particularly, Metin Ege wrote a thesis on "How do grants influence firm performance? An econometric evaluation of the SBIR programmes at NIH", which concludes that the programme had a measurable impact on sales and employment growth for the companies involved.
In the Netherlands, André Roos, SBIR programme manager at the Ministry of Economic Affairs, Agriculture and Innovation, states that PCP-SBIR in the Netherlands is used by 7 ministries with €69 million spending, on over 370 contracts, and 65% of companies involved making business from their

SBIR development within 1 year. He concludes that if the American SBIR investments led to 1800 new products yearly, PCP in Europe could, with an EU annual investment of €1 billion, lead to 2000 new products every year. A full evaluation of SBIR outcome in the Netherlands is scheduled for 2015.

2.4.4 Conclusions of SBIR assessments

From these sources, and others, the impact of SBIR was measured on several levels:

- impact on sales;
- impact on employment;
- impact on growth;
- impact on R&D and innovation;
- impact on project costs.

2.4.4.1 Impact on sales

On the question of commercialization, the NRC assessment concludes that the SBIR programme has a strong commercial focus, with considerable efforts to bring projects to market, which has known some success. The number of major commercial successes has been small, but that is normal for early stage high-risk projects, and the overall commercialization effort is substantial.

Products are coming to market quickly, significant licensing and marketing efforts are under way for many projects, and approximately 30-40% of projects generate products that do reach the marketplace. These data all paint a picture of a programme that is successful in commercializing innovative technologies in a variety of ways.

65% of companies involved make business from their SBIR development within 1 year.

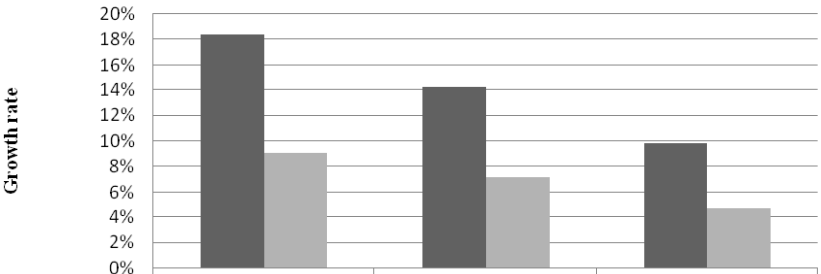
Audretsch et al. (2001) estimated the expected sales for each SBIR project on the basis of actual sales realised until 1999 from 112 DoD-funded Phase II SBIR projects. Average actual sales were $175 021 per project, which reflected the large number of firms with no actual sales (78 out of 112 made no sales of their product). However, when the sample was limited to the 34 projects reporting sales, the average increased to $575 539 per project.

The study concluded that if the SBIR programme did not exist, the probability of these projects reaching the Second Phase would be very limited, showing the strong positive impact of the SBIR programme.

An NAS survey of 790 Phase II projects with commercial sales showed average sales per project of about $2.4 million. The results were bifurcated. There were a handful of outsized successes, but more than half of the projects examined had sales of less than $1M. Of the sales studied, 35% were to the private sector, 32% to DOD, 10% to DOD prime contractors, and the rest to other public sector purchasers. About 14% of sales were exports.

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

Three Five and Eight year sales growth rate of the SBIR firms



	3-year sales growth	5-year sales growth	8-years sale growth
Phase II	18.40%	14.27%	9.84%
Control Group	9.06%	7.22%	4.69%

source Metin Ege

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

2.4.4.2 Impact on employment

The NRC assessment of the SBIR programme found that the median size of a company receiving SBIR awards is relatively small (far lower than the 500-employee limit imposed by the SBA).

The programme focuses the bulk of its awards on very small companies. More than a third of awardees had between one and five employees at the time of award. A very substantial number (70%) of respondent companies had 20 employees or fewer at the time of the Phase II award.

The NRC Survey sought detailed information about the number of employees at the time of the award and at the time of the survey and about the direct impact of the award on employment.

Overall, the survey data showed that the average employment gain at each responding firm from the date of the SBIR award to the time of the survey was 29.9 full-time equivalent employees. Of course, very few of the companies that went out of business responded to the survey, so this question is particularly skewed toward firms that have been at least somewhat successful.

Most responding companies have expanded since the date of the Phase II award. The NRC Phase II Survey also shows that respondents enjoyed strongly positive employment growth after receiving a Phase II award. The percentage of companies with at least 50 employees more than doubled, from 16.5 % to 35.4 % of all respondents.

Overall, survey respondents reported gains of 57,808 full time equivalent employees, with the top five respondents accounting for 18.4 % of the overall net gain.

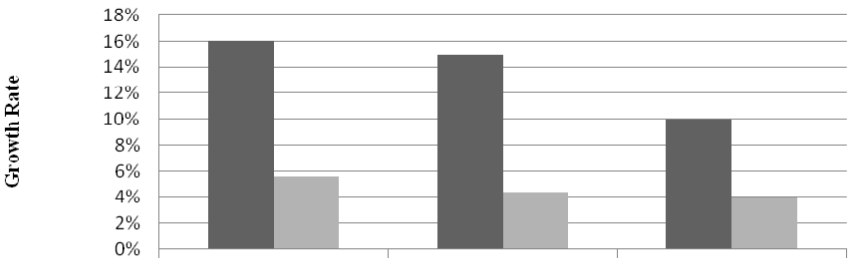
The NRC survey also sought to directly identify employment gains that were the direct result of the award. Respondents estimated that specifically as a result of the SBIR project, their firm was able to hire an average of 2.4 employees, and to retain 2.1 more

Overall, 40% of all projects retained zero employees after completion and over one-third retained only one to two employees, and about one quarter retained more than two. Thus the direct impact of SBIR funded projects on employment is small, especially when compared to the total number of employees in the firms. However, there are substantial cross-project differences in the number of retained employees that are explained by differences in the firms and their SBIR projects:

- funding agencies that funded projects creating intellectual property for the developer (patents, copyrights, trademarks, or publications) caused more employees to be retained after completion of the project;
- public funding of research by the SBIR programme was more likely to stimulate employment when the government created a market for the products, processes, or services developed by the research projects.

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

Three Five and Eight year employment growth rate of the SBIR firms



	3-year employment growth	5-year employment growth	8-year employment growth
Phase II	16.08%	14.95%	10.04%
Control Group	5.58%	4.38%	4.06%

source Metin Ege

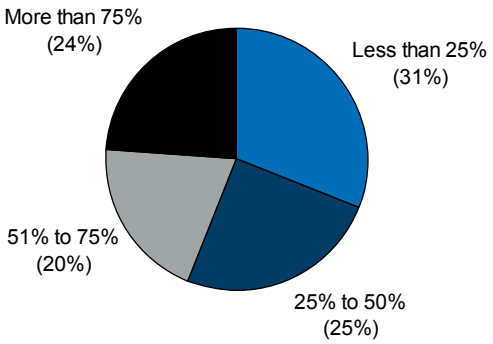
Results were similar when all recipients (Phase I and Phase II) were compared to all non-recipient applicants.

2.4.4.3 Impact on growth

The NRC assessment of the SBIR programme measured the impact of the programme on the growth of the companies that were awarded SBIR contracts.

All the respondents to the survey declared that a large share of their company growth was attributable to their SBIR awards. **In 44% of cases SBIR awards were credited with over 50% of company growth.**

SBIR impacts on company growth: Percent of company growth attributable to SBIR awards



source NRC

Metin Ege in his thesis quoted above states that “the main finding from the thesis is that the NIH SBIR programme stimulates both sales and employment growth.”

“Firms that received any number of Phase I and/or Phase II awards experienced 6.82% greater sales growth, and 6.90% greater employment growth over the three years following the first year they received an award compared to firms that applied to the program but were rejected, controlling for other factors.”

“Firms that received one or more Phase II awards experienced 6.13% greater sales growth and 7.86% greater employment growth over the three years following the first year they received an award compared to those that applied but were rejected.”

Josh Lerner (The Long-Run Impact of the SBIR Program, 1999) comes to a similar conclusion when he examines interactions between government and firms through the public subsidisation of small firms by the Small Business Innovation Research (SBIR) programme.

He compares the SBIR awardees with matching firms, and he shows that the mean sales increase from the end of 1985 to the end of 1995 was greater for the awardees ($4.0 million vs. $1.1 million, both in constant 1995 dollars). There was a similar employment increase (a boost of 26 employees vs. six). For the mean SBIR awardee, this represented a 98% boost in sales (in inflation-adjusted dollars) and a 56% increase in employment. In both cases, the differences in means were statistically significant.

Moreover, while the awardees and matching firms did not differ significantly in the likelihood of receiving venture capital in the years prior to the awards, in subsequent years the awardees were significantly more likely to receive such financing

Numerous studies have suggested that, because of knowledge spill-over, social rates of return to R & D are often much higher than the private returns that the firms performing the research enjoy. Lerner’s analysis does not seek to assess the social benefits of the programme, and focuses exclusively on private returns, as roughly measured through sales and employment growth. The differentials between the private and social benefits of the SBIR awards might be particularly large because many projects involve very early-stage technologies (where spill-over to other firms may be more frequent) or those important to national defence or public health

2.4.4.4 *Impact on R&D and innovation*

Subsidies are potentially effective in inducing firms to invest. Xulia Gonzfilez, Jordi Jaumandreu, and Consuelo Paz (Barriers to innovation and subsidy effectiveness, 2005) estimate that almost half of large nonperforming firms could be induced to perform innovative activities by financing less than 10% of their R&D, and one out of three small nonperforming firms by financing up to 40% of their expenses. They obtain evidence that actual subsidies do, in fact, play a part, even if a modest one. Some small firms' R&D performing observations are estimated to depend on the (expected) subsidy, in the sense that no R&D would be observed in its absence.

André Roos, SBIR programme manager at the Ministry of Economic Affairs, Agriculture and Innovation, states that PCP-SBIR in the Netherlands is used by 7 ministries with €69 million spending, on over 370 contracts.

65% of companies involved make business from their SBIR development within 1 year.

He concludes that if the American SBIR investments led to 1800 new products yearly, PCP in Europe could, with an EU annual investment of €1 billion, lead to 2000 new products every year.

2.4.4.5 *Impact on project costs*

There is little quantitative information available on the advantages of cooperative R&D programmes with regard to project costs. This is due to two difficulties:

- a methodological difficulty: how can one quantify the advantage of an explored cooperative solution compared to a non-explored non-cooperative solution?;
- a communication difficulty: if there is an added cost, there is a strong tendency not to say so.

In the absence of a real quantification of the costs of the cooperative approach, one may apply an old empirical rule used in the armament field to estimate the extra R&D cost of a cooperative programme, using the formula $\sqrt{N-1}$ where N is the number of participants.

According to this rule, for two participants the extra cost is 41.4%, representing the following added costs:

- technical extra costs due to the superposition of functional specifications of the various participants;
- loss of efficiency in the management of the programme;
- possible duplication of production facilities.

However each participant only supports half the extra costs, in this example 20.5%.
Moreover the customer may benefit from a larger scale production, which will normally impact the unit price and more globally the life cycle cost. This effect will also benefit the manufacturers.

Impact of cooperation on the cost of R&D based on the number of participants

Number of participants	R&D added cost
2	21%
3	24%
4	25%
5	25%

Number of participants	R&D added cost
6	24%
7	24%
8	23%
9	22%
10	22%

This formula shows a maximum added cost for 4 participants.

As an example, the added cost for the A400M was 50% above the initial estimate. In March 2010 the head of the French Defence Procurement Agency (DGA) stated:
"I believe we must definitely eliminate commercial contracts. Of course we could also discuss the issues of cooperation, the difficulty to align the positions of the participants, the relations between customer countries and manufacturers via the OCCAR, but we must remain lucid and face the fact that the manufacturer was not able to carry out the contract as it had been signed. There clearly has been a problem with the organisation and the industrial steering of the programme. EADS and Airbus have drawn the consequences concerning their organisation, but they must launch a more radical review of their capability to manage programmes"

"The A400M programme is a programme managed under the responsibility of the OCCAR, and it complies with commercial rules. The result proves that this sort of contract must be avoided in the future because it does not enable the States to check that the various stages are completed in time."

This question of costs was discussed with the manufacturers. Most of them think that PCP schemes may lead to longer delays and higher costs compared with conventional programme solutions (a single funder and purchaser). One should note however that industrial stakeholders in the security field we have consulted have no experience from PCP. Their opinion is therefore essentially based on their experience of cooperative and competitive procurement schemes in the Defence sector.

The manufacturers feel the old formula used in armament fits reality quite well. Some of them add that in European programmes 33% of the funds are absorbed by the administrative complexity of the contracts and the management of co-operation between participants (travel, exchanges). However, they also say that it has the advantage:

- of making companies work together;
- of contributing to the creation of a European market.

2.4.5 Impact of PCP in the security field in Europe

2.4.5.1 The approach

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

The difficulty is of course to extrapolate the benefits to the recipient companies to the whole industry. Assessing the effect on growth or employment of a given investment in R&D is not possible in a deterministic way. There is no mechanical link between R&D spending and future sales or employment, and it is probably not possible to state that when one invests, say, 100 million € in a PCP scheme, the

result will necessarily be extra industry sales of a given amount. The commercial outcome of R&D projects is never fully predictable, The only thing that can be stated with some degree of confidence, is that R&D spending does have a positive impact on sales globally and in the long term, and that measures to improve the efficiency of R&D, as in PCP, must also have a positive impact. But again, this cannot be directly related to the actual amount of spending, as a number of other less quantifiable factors must be taken into account.

Keeping this in mind, we can look at the present situation of the world security markets, and at the relative position of the European security industry, and we can explore some possibilities of impact of a successful PCP scheme. We can attempt to show what the effect of an increased growth rate could be on the sales and employment of the European security industry. Increased and more efficient European security R&D can be expected to boost the European market growth and at the same time to improve the competitiveness of European supply, thus giving production and employment in Europe an extra impetus.

This could be translated in terms of a differential of growth for the European security industry over the next ten years. A PCP scheme would have both an effect on the European market (by facilitating the introduction of new innovative products in Europe), and consequently on EU production, since it is expected that these new products will be developed by the EU security industry.

2.4.5.2 The security industry and market

EOS, the European Organisation for Security, has published in March 2011 a survey that gives an estimate of the size of the European security industry and market. These figures differ from those given in the previous Ecorys study (2009), mainly because of a difference in coverage.

The EOS study estimates the world security market in 2009 at 45 billion €, whereas Ecorys had found 103 billion €. The difference seems mainly due to “physical security protection”, including CCTV, access control equipment, intrusion and detection systems, etc., for private and commercial premises, and protective clothing, which together amount to 49.2 billion € according to Ecorys. After this correction the Ecorys world market figure is reduced to 53.8 billion €, which seems acceptably close to the 45 billion € shown in the EOS study.

The EOS study also gives forecasts to 2020, with two scenarios, a stable scenario and a “major security event” scenario. The following are a few key figures from this survey:

Stable scenario (relatively constant evolution of the security market)

– The world market for security solutions is growing rapidly, and even more so in emerging countries, and is worth 45 billion € in 2009 and over 87 billion € in 2020. The average growth rate should be over 6 % per year during the next 10 years.
– The corresponding EU security market is worth about 7.7 billion € in 2009 rising to 11,3 billion € in 2020, with an average growth of about 3,6% per year up to 2020.
– The EU security market is second behind the US in 2009 (17% of the world total) but should regress to 13% in 2020 behind the US, China, India and maybe even the Middle East. This is significantly below the lower limit for the European share estimated by Ecorys (25 to 35% of the world total).

Major event scenario

– Market evolution is driven by a large security related "event" happening, for example beginning 2013, and impacting all security sectors across the world
– The worldwide security market would in this case grow to more than 120 billion € in 2020 (growth of nearly 10 % per year).
– The corresponding EU security market would rise to more than 16 billion € in 2020 (growth of nearly 7% per year).

2009-2020 security market

	2009 (bn €)	% share	2020 stable (bn €)	% share	annual growth (%)	2020 major event (bn €)	annual growth (%)
World total	*45.0*	*100*	*87.5*	*100*	*6.2*	*123.6*	*9.6*
USA	*17.6*	*39*	*26.2*	*30*	*3.7*		
EU	*7.7*	*17*	*11.3*	*13*	*3.5*	*16.0*	*6.9*
MEAST	*3.6*	*8*	*9.1*	*10*	*8.8*		
China	*6.0*	*11*	*14.9*	*17*	*8.6*		
ROW	*11.3*	*25*	*26.0*	*30*	*7.9*		

source EOS *Security Market Evaluation and Recommendations for Funding Future EU Security Activities*, March 2011

European security market and industry 2009-2020

	2009	2020 stable (bn €)	annual growth (%)	2020 major event (bn €)	annual growth (%)
EU market	*7.7*	*11.3*	*3.5*	*16.0*	*6.9*
EU industry	*10.5*	*14.0*	*2.6*		
Net EU export	*2.8*	*2.7*			

source EOS *Security Market Evaluation and Recommendations for Funding Future EU Security Activities*, March 2011

Relative size of security markets in 2009 (Ecorys)

Sectors	EU (in billion €)	World (in billion €)
Aviation security	*2.0*	*5.2*
Maritime security	*2.0*	*6.7*
Border security	*5.0*	*9.9*
Critical infrastructure protection	*3.0*	*12.6*
Counter-terror intelligence	*5.0*	*19.4*
Sub-total	***17***	***53.8***
*Physical security protection**	*13.0*	*39.2*
Protective clothing (first responders)	*2.0*	*10.0*
Total security market	***32.0***	***103.0***

** includes CCTV, access control equipment, intrusion and detection systems, etc.*

Source: ECORYS (2009)

2.4.6 Security employees

The EOS study gives employment figures for the security industry:

- Employment in the security solutions industry is about 250 000 at world level and about 50 000 in Europe. In companies working in both the defence and security fields it is often difficult to clearly differentiate personnel employed between the two fields, and to give precise figures.
- Induced or secondary markets (e.g. subcontractors) for the security solution industry would account for some 15 000 more employees in Europe
- Complementary to this market, the EU security (manned) services market is constituted by more than 1 700 000 private guards (figures from CoESS – 2008).
- In connection with the security market, there are more than 4.2 million civil servants across Europe's national public administrations involved in security duties

EOS gives a breakdown of industry and service employment for Europe, which is the following:

Security employees in 2009

	Worldwide	*EU*
Security solutions industry	*250 000*	*50 000*
Induced secondary employment		*15 000*
Industry sub-total		***65 000***
Security services		*1 700 000*
Total private industry and services		***1 765 000***
Security civil servants		*4 200 000*

source EOS *Security Market Evaluation and Recommendations for Funding Future EU Security Activities*, March 2011

The Ecorys study gives a worldwide employment of 2 million. This figure includes employment in the security fields not covered by the EOS study (physical security, protective clothing), which can be estimated at roughly the same as the fields covered by EOS, i.e. another 250 000 worldwide, giving a total for the "security solutions" industry of 500 000 worldwide (and a total of around 100 000 in Europe, plus around 30 000 induced employment). The remaining 1 500 000 in the Ecorys figure may be considered as the part of the service employees more directly connected with the solutions and equipment deployed (this could be 255 000 for Europe, using the 17% share of EU in the world security market).

2.4.7 Security R&D

EOS also gives figures for R&D in the EU compared to the US, which show a level of public funding of security R&D in Europe that is ten times lower than in the USA, a ratio that is worrying for the future of the EU industry.

Security R&D investment

	EU (in billion €)	*USA (in billion €)*
Security industries turnover	*10.5*	
Public & private R&D	*0.66*	
R&D as % of turnover	*6.3%*	
of which public funding	***0.36***	***3.5***

source EOS *Security Market Evaluation and Recommendations for Funding Future EU Security Activities*, March 2011

2.4.8 Measuring the possible impact of a PCP scheme

Increasing the amount of public aid to security R&D, and increasing its efficiency through the implementation of a PCP scheme, should improve the competitiveness of the European security industry on European and world markets.

This is an absolute necessity, as public funding of security R&D is ten times lower in the EU than in the USA, according to EOS. And EOS foresees that in the coming years the European market will grow significantly faster than European production, reflecting a loss of competitiveness and leading to a decreasing share of world markets. This loss of world market shares is shown by the approximately 1% per year slower growth of production of security equipment in Europe compared to the market growth.

If nothing is done, and in particular if no PCP scheme is deployed in the R&D field, security industry growth in Europe until 2020 could be around 2.6% per year, compared to 3.5% for the European market.

The studies on the impact of SBIR mentioned above show a significant impact on growth of sales and employment. Companies receiving R&D support through SBIR or PCP programmes have shown faster growth than the others. There is no easy way to quantify the increase in growth for the whole industry caused by this faster growth of recipient companies.

But the effect of a PCP scheme would be felt at two levels at least:

- on the level of market growth, new products leading to improved security service and new markets.
- on the level of industry competitiveness, improving the position of the European security industry on European and world markets, contributing to maintain the ratio of EU production on EU markets.

A tentative assumption of a 1% increase in the annual growth rate of the European security industry market due to innovation from R&D support through a PCP scheme would lead to a growth rate of 4.5% per year on the period 2009-2020.

This could induce a growth of production of 4.5% over the same period, assuming that the PCP scheme would maintain at least a constant share of European industry on world markets due to the scheme.

This could give a significant impact on sales, production and employment in the security industry and services. Production of the European security industry could be higher by 6 billion €, inducing nearly 40 000 extra jobs in production, and the increased market could induce another 40 000 new jobs related to new equipment in services.

Possible impact of a PCP scheme on the European security industry

	2009	2020 no PCP		2020 with PCP		PCP impact
		growth (%)	amount	growth (%)	amount	
European security market value (billion €)	15.5	3.5	22.7	4.5	25.2	+2.5
European security industry production (billion €)	21*	2.6	27.9	4.5	34.1	+6.2
European security industry employment (thousands)	130	2.6	172.4	4.5	211.0	+38.6
European security service employment (equipment related) (thousands)	255	3.5	372.3	4.5	413.8	+41.5

* using EOS European production/market ratio

3 Major challenges raised by PCP in the security field

3.1 Current state of implementation

PCP is designed as a cooperative demand-based innovation process that is based on the involvement of public prescribers and end-users in the early stages of R&D projects. Efficient PCP could therefore contribute to address key market failures of the security market such as reducing market fragmentation, bridging the gap from R&D to market and eventually increasing the competitiveness of the EU security industry.

So far existing PCP schemes in Europe are only implemented at national level in few Member States, and they address R&D mostly in other fields than security, except for some projects funded under the UK SBRI programme or the Dutch SBIR programme.
It should be mentioned that there are no ministries for security and therefore, various kinds of public authorities can be concerned when it comes to public procurement procedures (e.g. defence, transportation, Interior, etc.) increasing the complexity of such programmes in the security field.

UK experience of PCP and R&D procurement in the field of security:

- There are several applications of PCP in the area of security: INSTINCT, Intent in Crowded Places and Hot Products, competitions run under the SBRI scheme through the Technology Strategy Board
- The Government also procures research and development services with framework contracts in the policing sector or the Home Office procures through its technology demonstrator programme
- Regarding urban transportation, central Government activity to support security through its own PCP scheme within the urban environment is limited to one competition supported by the Home Office.

NL PCP projects in the field of security:

- Physical protection (phase 1, closed 2 December 2010, budget 2.85 Meuro. Preliminary decision to start phase 2 has been taken in October 2011)
- Simulation and serious gaming for better training operational public security services (phase 1, closed 2 December 2010, budget 2.85 Meuro. Preliminary decision to start phase 2 has been taken in October 2011)
- Secure land operations (phase 1, closed 20th October 2011, budget 1.9 Meuro)

With regard to international cooperation, sectorial security needs are fairly similar between countries, and trans-national R&D cooperation in this field is still to be developed on a larger scale than traditional FP7 bilateral cooperation.

In its COM(2009)691 final Communication, "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations", the European

Commission indicated its intention to speed up the application of PCP in the security domain, in order to bring research results obtained in other research programmes closer to the market. Following this objective, the European Commission introduced the POV (Pre-Operational Validation) scheme in the 5th FP7 call for security research released in July 2011. This POV scheme, dedicated to maritime border surveillance, intends to provide a support framework for National Authorities to elaborate joint specifications and validation of integrated border surveillance systems. The POV scheme is also based on a competitive development principle where at least 2 companies or consortia will be funded to develop competing solutions.

The POV scheme could therefore be considered as a first attempt by the EU to organize PCP in the security field although the POV differs from the theoretical concept of PCP in some ways:

- The project R&D phasing does not strictly correspond in both schemes. Border surveillance systems consist in complex integration of existing technologies and platforms and are therefore principally focused on phase 2 of the innovation cycle (prototype demonstration) whereas a theoretical PCP starts from the proof of concept (phase 1) down to the production of a test-series to prove industrial feasibility (phase 3),
- The funding principle in the POV scheme is based on a mix of existing funding sources i.e. CSA – Coordinating and Support Action (funding the expression of needs and validation steps) and CP – Collaborative Projects (for the R&D investment itself). While CSA allows for 100% funding, CP only allows up to 75% funding and the POV scheme foresees that the rest will be paid by the Member States, therefore making POV a form of procurement..

While the success of the POV procedure is still to be confirmed, PCP/POV schemes in the security field represent a new approach to R&D for security stakeholders, and several challenges related to their implementation have been identified throughout the course of consultations in the national country case studies. These challenges will be developed in the following chapter.

3.2 Main challenges

3.2.1 Mobilising resources

The awareness of security stakeholders towards PCP as an innovative procurement procedure of R&D services is very low. PCP is more known in R&D circles than among the actual security prescribers and operators who are the primary targets of such cooperative procurement schemes.

Making security stakeholders aware of the PCP scheme and mechanism is only a first step. The national coordination and international cooperation of stakeholders on security R&D projects also faces acceptability issues in the security field due to several factors:

- Procurer technical expertise and resources vary from one sector to another. In some sectors (urban transport, critical infrastructures) these resources need to be built up
- Participation to such cooperation is seen more as time consuming than as bringing benefits especially for operators who see security as a burden imposed from outside. Mobilising operators' resources to participate in security R&D programmes is therefore a challenge and would require that the project topic should address clear operational issues in addition to security needs.
- There are diverging interests on the commitment to buy between procurers and suppliers of security equipment. Public authorities vigorously refuse that procurement of R&D services should bind them to any form of commercial procurement once the programme is completed, whereas the industry would wish for such a commitment.
- Securing the participation of a large pool of security stakeholders within a PCP project is a necessary but not sufficient condition to maximize the transition of R&D to market. Citizen acceptability in the security field also plays a fundamental role (30% of the R&D budget in Germany's security programme addresses social acceptability issues) and should be taken into account. The challenge lies in the fact that unlike security needs, the social acceptance criteria may be very different from one country to another.

3.2.2 Organizing the cooperation

A PCP programme involves multi-level cooperation between stakeholders, from the common expression of needs (functional and technical) to the review of results and validation procedures. Organizing such multi-level cooperation in the field of security is a challenging task.

The geographical scope of programmes may raise some problems compared to traditional R&D funding schemes under FP7. Since PCP is a procedure for the procurement of R&D services by public authorities, some stakeholders consider that non-EU countries should not participate in such programmes, whether they are partner countries or not.

The common expression of functional and technical needs may also raise some issues. Although sectorial security needs are the same for all Member States, the fine expression of functional and technical needs may differ from one security procurer to another because of varying experiences in managing R&D and differences in threat exposures. The confidentiality of information associated with the definition of security needs might also complicate the formulation of a common expression of needs across national public procurers.

Assessing and validating the results of the different R&D phases in a PCP programme requires a high degree of transparency in the corresponding criteria and procedures applied and must rely on trusted partners/organisations acknowledged by the different national public authorities involved.

This consensus is essential to build trust among participants and guarantee the quality and acceptance of the R&D performed, therefore preserving the potential for the future commercial exploitation of R&D results. This condition is even more critical in the security field, where Member States shall not be bound to any form of commercial procurement because of PCP.

IPR issues might also represent a challenge to the cooperation between public and private stakeholders on security R&D but this issue will be dealt with more specifically in the following chapter.

3.2.3 IPR management

IPR management plays an essential role in a PCP scheme since it can be adjusted to guarantee that risks and benefits are shared between the supplier and the procurer (see chapter Legal analysis for a more complete description).
Provided that the IP is owned by the supplier in a PCP scheme, there are basically 2 ways of managing IPR in a PCP:

- IP owned by the supplier, and the procurer receives a royalty-free license (either exclusive or non-exclusive).
- IP owned by the supplier, and the procurer receives a royalty-bearing license (either exclusive or non-exclusive)

In the security field, IPR management may become a complex issue due to the following factors:

- Integration of existing technologies plays an important part in security R&D. IPR **scope and definition** might therefore be a complex task for large integration projects where the IP generated during the project shall be isolated from the IP held by the supplier (or the procurer) before the start of the project.
- IPR **evaluation** might also be a complex task since it is difficult to estimate the value of a potential market deployment in the field of security that is highly regulated at national level and does not obey to traditional market patterns.
- IPR **sharing principles** could also generate additional complexity when critical or restricted information is being disclosed and associated with the IPR. This is true when information is shared between the procurer and the supplier but also between the procurers themselves in the case of cross-border cooperative programmes.

The purpose of this study is not to solve these sensitive issues. However it results from the consultations conducted in the national country cases that most of the stakeholders felt the question should not be a major obstacle to the development of PCP.

IPR management may be either translated into Member State law or negotiated within specific agreements, as has been done in similar situations, for example in France or the UK:

- In France the CCAGPI[12] regulation offers two options, either a free licence-to-use for procurers and royalties for other users, or exclusive rights to procurers (see below)
- UK ETI IPR management. The Energy Technologies Institute (ETI) operates a pre-commercial procurement scheme in the area of energy. Project funding is variable, and access to Intellectual Property reflects contributions in cash and in kind (see below).

[12] General Contracting Conditions for public procurement of intellectual services (Cahier des Clauses Administratives Générales applicables aux marchés publics de Prestations Intellectuelles)

France:

On the issue of intellectual property rights the CCAG/PI (general administrative rules applicable to intellectual services) established new rules in 2009 for public procurement contracts. For the use of results two options are possible:

- Option A: the beneficiary of the contract grants to the purchaser and to third parties named in the contract the non-exclusive right to use or grant the use of the results. The beneficiary of the contract pays the purchaser a royalty if there is any commercial use of all or part of the results, or if he concedes in whole or in part the rights to use the results. The royalty is calculated on a base of 30% of the revenue (exclusive of tax) received by the beneficiary of the contract, after deduction of the costs of production and marketing.
- Option B: the beneficiary of the contract grants the purchaser the totality of the exclusive rights of any sort pertaining to the results, enabling the purchaser to freely use them, including commercially, for the uses defined in the documents concerning the particular contract concerned.

The UK

The ETI (Energy Technology Institute) runs a pre-commercial procurement scheme for energy technologies, which is, however, not restricted or even focused on security solutions.

According to the scheme projects can be funded by a variable mix of public and private funding and may also be co-funded with project participants.

This gives flexibility in access to Intellectual Property to reflect contributions in cash and in kind.

The Institute's members agreed on a set of rules of how to deal with issues of intellectual property rights arising from their common work. A summary of them is presented in Appendix 2 of the UK case study.

In another field, the National Innovation Centre (NIC) carries out PCP activities on behalf of the Department of Health. The NIC has its own rules and procedures for the allocation of IPR and contract price setting for PCP activities. It follows the advice given in the procurement directives and State Aid Rules.

Netherlands

In the Dutch SBIR program the arrangement related to IPR for both phase 1 and phase 2 SBIR projects is the following[13]:

- The IPR rights remain at the supplier, and are not transferred to the client.
- However, the client has certain rights related to IPR, these are the following:
    - The right to use the results for dissemination purposes.
    - The right to use the knowledge, without paying licence costs.
    - The right to make the knowledge public, if he thinks that is needed for the pulic interest.
    - The possibility to oblige the supplier to provide licences to third parties under reasonable conditions.

[13] Source: "SBIR handleiding voor ondernemers", Agentschap NL, 7 July 2011, version 2011-1.

- The total budget for the SBIR project has to take into account the fact that the IPR rights are not completely transferred to the client, and should therefore be lower than the budget for a project where all IPR rights are transferred to the client. This difference has to be specified by the supplier for the specific SBIR project.

4 Policy options and impact assessment

4.1 Factors influencing the attractiveness of PCP in the field of security

Stakeholders' interviews and literature review point to several generic and specific factors influencing the attractiveness and potential impact of PCP in the field of security.

4.1.1 Generic factors

Generic pros

Primary customers of security R&D services are public bodies and public prescription plays a key role in structuring the security market.

There is a general need in Europe to better align R&D projects with security requirements and end-user needs. This requires that both security prescribers and operators should be associated early on in security R&D projects, and this would in-turn facilitate subsequent commercial product development.

Within a given security application domain, there is a similarity of security needs between public procurers in different countries, which provides a basis for common specifications and bundling of demand. Pre-commercial action at EU level could therefore help in reducing market fragmentation and creating common standards.

SME involvement in security markets and R&D activities is identified as one of the security market failures in Europe. The phasing of R&D programmes could represent an opportunity to develop SME participation in larger R&D programmes.

Generic cons

Public procurers in the security domain have generally only limited capabilities to elaborate technical specification corresponding to operational needs.
Nota: this is not only related to PCP but also to any form of involvement of public procurers in security R&D

Security R&D requires some flexibility and reactivity due to the evolving nature of security threats. Multiple contracts and phasing of R&D are seen as lengthy processes that will create additional delays in bringing innovation to market (programme complexity, alignment of the programme on the slowest participant).

Competitive development would increase the cost of the programme and therefore limit its scope to relatively small programmes to the detriment of large-scale integration projects that are required in the security field. The cooperation between public procurers also has a cost due to cumulative functional specifications and additional overhead.

Opportunities for cooperation between public procurers may be restricted in the security field due to sovereignty and/or IPR management issues and may consequently lead to limit the scope of PCP in the security field.

4.1.2 Specific factors

In addition to the generic factors listed above, interviews and literature review also helped to identify a list of specific factors to be considered when assessing the attractiveness of PCP in the security field. These specific factors are either linked to the security sector or to the country characteristics.

Sectorial factors

The international aspects and requirements of the security domain (inter-operability, regulatory environment, etc.) favour PCP schemes and more broadly the need for cooperation between public authorities since sectorial security needs are fairly similar from one country to another. The availability of existing international cooperation structures (airport, maritime borders, etc.) can also provide a first trusted coordination environment that is necessary for defining common requirements across countries (operational and technical specifications).
Similarly the existence of trans-national industrial champions is also considered as a favourable factor for implementing PCP schemes in the security field.

The security stakeholders' organizations vary considerably from one application sector to another. Application domains where the security prescriber, procurer and operator are the same national entity are favourable ground for PCP schemes since this greatly facilitates the expression of security needs and the governance of such programmes.

Security application domains where the degree of cross-fertilization with other business areas is high (e.g. dual use) are considered also to be favourable for the development of PCP in the field of security since this gives scope for further development of commercial opportunities once the programme is achieved.

Some application domains also require the exploration of multiple solutions to meet security threats (e.g. maritime borders). This characteristic is again favourable to PCP since it provides a technical justification for a competitive development process.

Based on the above criteria the security application domains covered in the study would rank as follows in terms of PCP attractiveness:

- Maritime Border: high
- Aviation Security: high
- Urban Transport: Medium
- Critical Infrastructure: Medium

National factors

Existing R&D organizations and policies, and the attractiveness of PCP may vary considerably from one country to another depending in particular on its size. Larger countries may have their own structures, and are wary of new organisations creating new burdens and constraints,

whereas the smaller countries generally have less structures of their own, and may welcome European initiatives like PCP as a possible way to improve their R&D activities.

Some countries are also engaged in bilateral cooperation programmes in the field of security, and they may wish to privilege them for security R&D. These agreements are often signed with non-European countries (US, Israel, Canada, etc.), and sometimes within the EU (France and Germany have developed a common programme for security R&D).

4.2 Introduction to policy options

4.2.1 Global vs. specific approach to PCP in the security field

The generic factors listed above tend to support the idea that a general approach towards PCP, addressing a wide spectrum of application domains for PCP procedures and practice, may in the end be needed in the security field, across security application sectors and countries. But a number of factors remain specific, and this tends to indicate on the contrary that it may be more productive, at least in the take-up stage, to consider sectorial and also country specificities.

Indeed, ad-hoc sectorial initiatives or structures may facilitate the acceptability of European cooperation in the field of security R&D for the following two major reasons:

- Sectorial specificities, that are often similar across countries, may help recognition of the benefits of European cooperation and harmonisation
- This, in turn, will facilitate the bottom-up approach, between players « speaking the same language » in their sector

However the information available through our interviews with the security stakeholders and the literature review do not enable to elaborate an impact assessment based on a sectorial approach of this nature. The major reasons for such a methodological difficulty are:

- At the sectorial level, the characteristics that may facilitate the implementation of PCP schemes may at the same time reduce its impact and vice-versa
- It is not possible to balance the influence of one factor with respect to another on the basis of available information
- There is no sectorial homogeneity between countries, adding another dimension to the complexity of the impact assessment

4.2.2 Selected policy options

Based on the above and considering the Terms of Reference, 2 policy options have been selected to draw the impact assessment (see next chapter), each option corresponding to a group of security application domains:

- Option 1: Support of the European Commission to centralised PCP schemes engaged by or through existing European coordination/cooperation agencies or structures (provided that the R&D topic and scheme is compatible with EC objectives). This option corresponds to security application domains where such agencies exist, such as Maritime borders or Airport security.
- Option 2: The European Commission funding decentralized PCP / POV jointly with several Member States through FP7-8 projects. This option corresponds to security application domains where there are yet no European agencies or structures, such as Urban transport or Critical infrastructures.

Nota: Option 1 and 2 are not exclusive i.e. option 2 could well be used for Maritime borders or Airport security in case the corresponding agencies do not wish to run, participate in or facilitate a PCP project.

4.3 Impact assessment

4.3.1 Introduction

The problems of existing R&D procurement address the main **market failures** in the security field (maritime borders, airport security, urban transport and critical infrastructures) regarding public procurement. These result in three main issues: the lack of end-user involvement in public R&D schemes, the fragmentation of the public procurement and the limited leverage on innovation in Europe as well as the limited SMEs involvement in innovation. These issues are differentiated and broken down into specifics regarding the various stakeholders during the impact assessment.

Based on these failures, the main policy **objectives** of any policy proposal in this domain would be:

- Reducing market fragmentation
- Bridging the gap from R&D to the market and,
- Increasing competitiveness of the EU Security industry.

4.3.2 Policy options

This section examines different **policy options**, which aim at solving the aforementioned market failures. In the impact assessment, the impacts of the different policy options will be detailed and analysed. Based on the terms of reference, there are a number of policy options that are applicable:

- A **centralised** and a **decentralised** policy option. These policy options will be analysed according to their attractivity, the instruments used, the fields of operation and their impact to the stakeholders;
- Key in any impact assessment is that the policy options are compared with a **baseline option**.

The differences of the defined criteria between a policy option and the baseline option represent the impact. The baseline is defined for this study as option 0.

In summary, within this study the following options are distinguished.

- Option 0: Baseline
  - No EU policy action, continuation of the existing situation.
- Option 1: Centralised EU-PCP
  - Support of the European Commission to centralised PCP schemes engaged by existing European coordination/cooperation agencies or structures (provided that R&D topic and scheme is compatible with EC objectives)
- Option 2: Decentralised EU-PCP - POV
  - The European Commission funding decentralized PCP / POV jointly with several Member States through FP7-8 projects

In this study it is considered that the option 1 and 2 are linked with the security fields' typology. The options and the criteria of analysis can be, in short, found in the following table.

Additional options to the Baseline

Scheme	Option 1 – Centralised PCP		Option 2 – Decentralised PCP-POV	
Field	Maritime borders	Airport security	Urban transport	Critical infrastructure
Attractivity	High	High	Medium	Medium
Instruments	Existing cooperative European agencies or structures		Not yet European agencies or structures – EC funding (FP7/8) jointly with several Member States	
Stakeholders involved	Producers, procurers, RTOs, regulators, society		Producers, procurers, RTOs, regulators, society	

The rationale behind such a link between options and sector organization is the following:

- Option 1 applies primarily to airport security and maritime border security, where there are existing cooperation bodies / agencies such as ECAC and FRONTEX. In this option, the Commission would stimulate these agencies to apply PCP wherever possible to realise the most effective security solutions for identified threats. Some of these bodies / agencies are to some extent active in the area of security R&D, and it would be ineffective to establish a separate line of R&D initiatives with PCP as proposed under option 2.
- Option 2 applies to urban transport and critical infrastructure security. Currently, security R&D is arranged for primarily on national or even regional level, or sometimes not at all (e.g. urban transport in some countries). By establishing a PCP scheme in FP7-8, it would enable and stimulate stakeholders in these sectors to use the new opportunities created and apply PCP for R&D in these two sectors.

4.3.3 Approach for the analysis of impacts

The above implies that for both options, an uptake of PCP schemes is foreseen in the area of security R&D in the four sectors under study. In this impact assessment it is therefore primarily analysed what the impacts of this further uptake of PCP is across these four sectors. In the last section of this impact assessment a brief scoring of the two options on the different impacts has been carried out.

The nature and character of the security sector proved to be a strong limiting factor in any quantification of the impacts, and sometimes even in qualification. The assessment has largely been based on the interviews conducted for the country case studies, position papers of the industry on the topic, and causal chain analysis based on the problem assessment regarding pre-commercial procurement in the area of security products. Unfortunately, the mentioned limitations also hampered any distinction in the assessment of impacts between the security sectors under study in this project (aviation, maritime etc.). The quantitative impacts that have been derived, have largely been based on lessons learnt from the US SBIR programme, a main US innovation research programme with a pre-commercial character (cf. parts 2.3 and 2.4). Annex A to this report provides extensive lessons learnt overview based on literature review.

The approach that has been applied follows the logic and guidance of the Guidelines for Impact Assessment of the Commission. In line with these Guidelines, the economic impacts and social impacts are addressed. The Guidelines also indicate to assess the environmental impacts. However, environmental impacts do not result from the options and are therefore not part of this analysis. In the impact assessment below, economic impacts are marked with an {E} and social impacts with an {S}.

4.3.4 Impacts of Option 0 - Baseline

The Baseline scenario maintains the existing structure concerning the public procurement in all security fields. This scenario does not introduce any new schemes (PCP) but it demonstrates the projects through currently available FP7 instruments.

The existing market failures would persist due to the dysfunctionalities of the existing structure. The gap between real market needs and R&D results would remain as the specifications of the contracts would be delivered by the suppliers (supply-driven procurement), overlooking specific public customer needs (demand-driven procurement). Therefore, the industry will not address these issues nor it will implement solutions. This gap also hampers the exploration of new, potentially promising R&D concepts. The market asymmetry will be maintained in the security sector resulting to inefficiency of R&D activities and incapacity to be aligned to immediate security requirements...

Regarding the fragmentation of the public procurement, the baseline scenario using the existing instruments does not allow sharing the R&D risks for procurers and suppliers. Currently, the procurement is based on exclusive development with IPR left to the public procurer. Hence the investment risks remain under one procurer and the development risks (including IPR costs) are too high. In addition, as the IPR remain to the procurer there is less room for the market potential.

The market fragmentation for security will even create larger discrepancies between Europe and the rest of the world as the public procurement takes place predominantly at local and regional level. At the same time, security sectors such as airport and maritime denote the need for international cooperation. In conclusion the bounded innovation will create difficulties for international compatibility.

Finally, the limited SMEs participation is maintained in the baseline option. Due to the lack of public demand for R&D and R&D procurement strategies, SMEs cannot escape from their traditional subcontractor role. The existing framework involves disproportionate qualifications and financial guarantees on the bidding companies (engaging minimum company turnover), low level of commitment due to narrow assignments, no room for innovation and processing/ exploration of individual ideas and exclusivity of development within EU or locally (local growth). These characteristics will impede the growth of small companies (SMEs), limiting their participation to the projects and their prospective growth.

4.3.5 Impacts of option 1 and 2

The impacts of option 1 and 2 are analysed individually for five stakeholder types:

- Producers
- Procurers / users
- Research and technology organisations
- Regulators
- Society

4.3.5.1 Impacts for producers

The following impacts for producers have been identified.

- Increased market transparency
- Increase of demand volumes for security products resulting in economies of scale

- Decrease of market risk for producers
- Increased R&D efficiency
- Reduction of time-to-market
- Decrease of product unit prices
- Increase of competition in the security R&D 'market'
- Increase of competition on the market for European products
- Competitiveness of producers

These impacts will be detailed below.

Increased market transparency {E}. Previous research[14] indicated that public procurement systems for security equipment and systems are insufficiently transparent and may be used to limit markets access (i.e. preference for 'local' over 'foreign suppliers). PCP should lead to a bundling of demand of multiple (international) procurers and would include a competition element among different development teams. This will increase the market transparency of procurement of security products and solutions.

Increase of demand volumes for security products resulting in economies of scale {E}. PCP should lead to a bundling of demand from multiple public procurers. Rather than developing security solutions solely for the needs and operational requirements of a single procurer, which effectively represents a fragmented market, producers are now able to sell their developed products to multiple procurers. This thus means that the market fragmentation, one of the major current market failures in the security market, is reduced. The effect of PCP to reducing market fragmentation was the most important outcome on the Commission's stakeholder Consultation on an Industrial Policy for the Security Industry (PCP part). The impact of this reduced market fragmentation is that producers are able to produce their security products in larger volumes: rather than producing for a single procurer they will now be able to produce for multiple procurers. Additionally, the similarity of security needs of the multiple procurers will provide ground for common specifications and this to an enhancement of the interoperability of security solutions. Finally, PCP could also lead to increased standardisation of products. After all, both producers and public purchasers benefit from wider commercialisation and take-up of the developed solutions. This provides an incentive to both parties to pursue standardisation and publication of R&D results (depending on IPR arrangements etc.). These developments will lead to an increase of demand for security products resulting in production efficiencies or economies of scale.

Decrease of market risk for producers {E}. One of the key impacts illustrated in previous studies on PCP, is the reduction of market risk for producers[15]. There are a number of underlying factors that contribute to this. First of all, in a PCP scheme there is more certainty that the final product developed is eventually purchased. After all, the development is done in close co-operation and involvement with procurers and users, fully geared to their specifications. The market risk for producers is therefore reduced. After all, in the baseline situation, producers in security R&D generally have to fund part of the R&D investment themselves, and they do not have such certainty that in the end there is a market for the products developed, as users are less involved in the R&D process. Under the policy option, there may be multiple PCP contracts, hence there is no absolute certainty for a *single* producer that he will sell his products. Nevertheless, there will

[14] Ecorys, 2009, Study on the Competitiveness of the EU security industry.

[15] E.g. Bos, L and S. Corvers, 2006, Pre-commercial Public Procurement, A missing link in the European Innovation Cycle, Public Needs as a driver for innovation.

be more certainty that the R&D product of *one* of the producers participating in the PCP process will be eventually procured. Additionally, with PCP risk and benefit is shared between producers and procurers, which is a generic characteristic of PCP[16] that would also apply to PCP in security. When being utilized, public procurement of R&D is in the baseline generally based in Europe on exclusive development and IPR are left to the public procurer. This scheme will normally be reflected in a higher price (IPR value is paid by the procurer), which makes the procurement of R&D a risky non-attractive activity for procurers. Now the IPR is left to the producer, which increases the opportunities for commercial deployment of the developed products. Finally, a PCP scheme with serious involvement of end-users with respect to requirement and specification formulation implies that will be better geared towards the demands of the procurers. This means that producers are better prepared to address the future (wider) market when the PCP scheme is finished.

Increased R&D efficiency {E}. The involvement of multiple procurers in the PCP schemes under the policy options implies that their R&D resources will be pooled. This suggests that duplication of R&D efforts is avoided. Additionally, PCP stimulates close cooperation between producers and users. This will mean that the R&D process is optimally tuned to their needs and requirements, and thus is more efficient compared to FP7 R&D development processes under the baseline.

Reduction of time-to-market {E}. Key feature of the PCP scheme is the closer involvement of the end user in the solution development, for example by early specification drafting or assessing prototype performance in their operational environment. It will thus enable procurers to 'steer' product development to their needs much more than in the baseline. This allows producers in a much better way to respond to user demand and thus prepare for broad European roll-out of their products to the market. As such, the time to market will be reduced for their products. Additionally, PCP is able to bridge the gap between the TRL level reached under FP7 R&D contracts and commercial procurement, as indicated by the manufacturing industry[17]. This has a positive impact on the time to market of products. Finally, the involvement of users also enables producers to 'filter' the most promising R&D concepts in a quicker way, which also speeds-up the time to market of their products. The counter argument though, is that if multiple PCP contracts will run in parallel, there is a risk that this has a negative impact on the time to market, as for deciding to go to each next sub-stage in the R&D process all consortia must be on the same point in the R&D process. Hence development on phases means alignment of the programme to the slowest participant. The expression of a common need between multiple procurers could also be a long process.

Decrease of product unit prices {E}. As assessed above, several factors will have an impact on the prices of security products. First of all, the above-described increase of production efficiencies and economies of scale will have a reducing impact on the overall prices of security products. Secondly, the reduced time to market also results in efficiencies with a downward impact on product prices. Thirdly, under the policy options, products are generally no longer exclusive developed for a single procurer, that in many cases required full transfer of IPR to the procuring authority. This meant the IPR value was paid by the procurer in the baseline. In the PCP schemes this will no longer be the case. The product unit prices are cheaper due to the integration in the producer pricing strategy of the IPR value that is left to the producers (compensation for the procurers)

---

16 Ibid..

17 EOS contribution to the DG ENTR' consultation on an Industrial Security Policy

Improved innovation opportunities for SMEs {E}. The policy options enable the Commission to support the PCP schemes in such a way that they are as open and attractive as possible for SMEs:

- by not using disproportionate qualification or financial guarantee requirements on bidding companies (no conditions on minimum company turnover as is often done in large scale public procurements);
- by increasing the commitments expected from participating companies gradually - phase per phase - along the lines of the natural growth path of a start-up company;
- thereby also giving SMEs the chance to step outside of their traditional subcontractor role and focus on working out their own ideas to successful products; and finally
- by giving companies the chance to grow globally (by assigning IPR ownership and thus the exploitation rights on developed solutions with the companies not the procurers).

Evidence from the US SBIR program (Health part) indicates that 34% of firms that won SBIR awards reported having generated at least 1 patent and just over half respondents published at least one peer-reviewed article[18]. In addition between 30% and 40% of the SBIR awarded projects generate products that reach the marketplace.

Increase of competition in the security R&D 'market' {E}. Multiple PCP contracts for a single solution imply that competition is brought *into* the R&D process. Producers will not be certain that their product is chosen by the procurers in the end of the development phase. This would be an increase of competition in the security R&D market compared to single solution procurements. On the other hand, also in the baseline, FP7, there is some competition to get an R&D contract award. This is competition *before* the R&D process starts. Increased competition during R&D could be a positive factor for industry, increasing the overall performance of companies.

Increased return on R&D {E} A pre-commercial procurement scheme may have a positive impact on the private return on R&D. Evidence from the US SBIR programme indicates that many of the surveyed participating companies mentioned that they would not have undertaken the R&D without public support because the private return that they perceived they would earn would be less than the minimum accepted rate of return required for private financing of projects (private hurdle)[19]. NRC defines the number of no-go projects up to two-thirds of the SBIR projects. The average expected rate of return without SBIR is only 25 % (8 % less than the appropriate amount to surpass the private hurdle rate), while the private hurdle is surpassed by 43-percentage point with the SBIR support, arriving at a private rate of return on the R&D of 76%. In addition, the SBIR support helps in tackling with the funding in order to reach the appropriate social rates on return of R&D.

Increase of competition on the market for European products {E}. In the beginning of this section, it has been described that the options will lead to an increase of market transparency and a reduction of market fragmentation. Both will affect the level of competition on the market for security products. A better market transparency provides manufacturers more insight in the performance requirements of the market. More producers will be able to adapt their products in better way to these requirements, which implies an increased level of competition. Furthermore,

---

[18] NRC (2008). An assessment of the SBIR program.. Board on Science, Technology, and Economic Policy, National Research Council. The National Academies Press. Washington DC.

[19] NRC (2008).

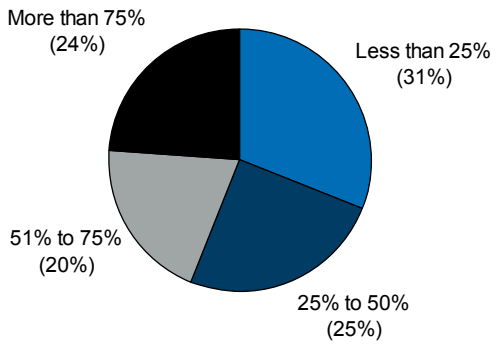
the reduced market fragmentation implies that national markets become more open for producers from another European country. This means rather than sourcing national solutions, international procurement processes are started, hence driving up competition.

Producers' competitiveness {E}. The competitiveness of producers is impacted by a number of developments, which partly have been described above. An important development in this respect is the overall expected decrease of prices of equipment, which improves the competitive position of European producers. Subsequently, one of the key features of PCP is the closer involvement of end users. This drives the innovative character of solutions to be developed, which in the end should be more tuned to the user needs than those products developed under the baseline. In other words, the quality of the products is improved. This has a positive impact on the competitive position of European producers. Finally, the deployment of PCP in the R&D process of security is expected to bridge the gap between the TRL level reached within FP R&D and commercial products. This implies that PCP will lead to a larger number of products brought to the market, which also affects the competitiveness level of producers. As a comparison: the entire US SBIR programme leads to 1800 new products yearly[20]. The 2009 programme value of SBIR amounted to approximately US$ 2 billion (phase I and II).

Company, sales, and employment growth {E}. The above impacts in turn are likely to affect the company and sales growth of producers. Clearly, an improved competitive position drives the sales and company growth of producers. This is difficult to forecast. However, one may make some comparisons with results of the US SBIR programme.

There are different evaluation studies on the US SBIR that indicate that the programme leads to sales growth and company growth of participating companies. An evaluation study performed by the National Research Council[21] indicates that a significant share of companies that participated in SBIR that were surveyed reported more than 50% company growth attributable to SBIR awards. This is depicted in the following figure (see annex 1 for more detail).

SBIR impacts on company growth: Percent of company growth attributable to SBIR awards
Source: NRC Firm Survey

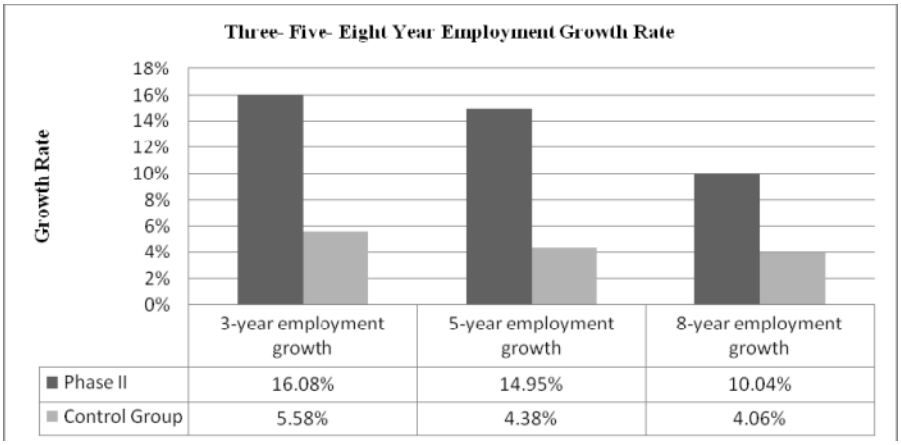


Source: NRC (2008)

[20] Dutch Ministry of Economic affairs (2011): www.comune.torino.it/relint/PPI/pdf/Roos_PPT.pdf.
[21] NRC (2008).

Another study carried out by Ege[22], limited to the Health part of SBIR, indicated a clear relation between SBIR award and company growth rate. The three- five- and eight year sales growth rates of companies that had an SBIR award is found to be 9, 7 and 4 percentage points higher than companies without an SBIR award. See annex 1 for more detail.

In the same study, Ege (2009) also analysed the employment impact of the US SBIR. He compared two samples of data, a test and a control one in order to check the effect of the SBIR programme to the average employment growth for the Health projects for three, five and eight years. It results that the average employment growth was higher in the groups of Phase II awardees than the non-recipients group. The following figure shows that the growth of the SBIR firms reaches 16, 15 and 10 % in three, five and eight years respectively. At the same time, the non-SBIR firms demonstrated a growth of 6, 4.4 and 4 %.



Source: Ege (2009)

4.3.5.2 *Impacts for procurers / users*

The following impacts for producers have been identified.

- Reduction of contract costs
- Increase of contract costs
- More products and solutions tailored to the needs of the procurers / users
- Better value for money from R&D investment in security

These impacts will be detailed below.

Reduction of contract costs {E}. As indicated above, a key characteristic of the PCP schemes in the policy options is the involvement of multiple procurers. This implies that the contract costs are reduced as the PCP schemes divide the investment risk for procurers by the number of procurers that cooperates. Furthermore, also described above, products are generally no longer exclusive developed for a single procurer, that in many cases required full transfer of IPR to the procuring authority. This meant the IPR value was paid by the procurer in the baseline. In the PCP schemes this will no longer be the case[23]. Hence contract costs reduce for procurers.

Increase of contract costs {E}. However, on the other hand there are developments that would increase the contract costs. First of all, issuing multiple R&D contracts would increase the costs of

[22] See annex B for more detail.

[23] This will depend on the final arrangements of the PCP contracts.

a programme, as opposed to a single R&D programme for a certain solution. Additionally, experiences in the aerospace sector indicate that cooperative R&D programmes lead to costs increases up to 25% (for four participants, see the French case study) as a result of:

- technical extra costs due to the superposition of functional specifications of the various participants;
- loss of efficiency in the management of the programme:
- possible duplication of production facilities.

It must be noted that also in the baseline under FP7 the effect of costs increases due to cooperation applies. However, under the policy options, the additional costs of cooperation would apply in each of the multiple procurement contracts.

The counter-side of the stronger involvement of users and procurers in the procurement of R&D is obviously that this would require more staff effort. This could be quite substantial if users are heavily involved in the elaboration of specifications according to operational needs.

More products and solutions tailored to the needs of the procurers / users {E}. A key characteristic of PCP is the strong involvement of users in the formulation of requirements and specifications. Also, there is the opportunity to test the prototypes in the operational user environments at some point. This thus implies that many more security products are tailored to the needs of procurers and users; there is demand-side driven product development. Interviews with experts in the defence sector, that have comparable experience in the user involvement in R&D of complex systems, indicate this as the major advantage of such R&D scheme.

Better value for money from R&D investment in security {E}. Competitive development in a PCP scheme enables procurers to compare value for money of the alternatives. In each stage of the PCP process, procurers can compare the level of achievement with the invested sums so far. In such way, the procurers are strongly involved in the comparison of the different alternatives being developed to respond to their needs.

4.3.5.3 Impacts for Research & Technology Organisations (RTOs)

The following impact for RTOs has been identified.

Decrease of RTOs activities {E}. RTOs have played so far an important role as under FP7 they participate to the elaboration of security needs, the selection of projects and the assessment of R&D results. These roles may be reduced for RTOs if PCP were to develop since procurers and operational users would be more active in all 3 stages (potentially with the support of RTOs however).

One additional argument is that PCP will unavoidably lead to a stronger user involvement. As PCP is market-originating, the user is an active part of the innovation procedure and not just the end-user as it is under current circumstances. This participation of users could limit the scope of the RTOs and, consequently decrease their activities range.

4.3.5.4 Impacts for regulators

The following impact for regulators has been identified.

Increase of products available tailored to the regulatory needs {E}. In general, there is a strong connection between innovation and regulation. Increasing innovation leads to the need of more standards for insuring the technical specifications of the end-products (e.g. in safety, environmental impact etc.). PCP contracts are aiming at increasing innovative activities. At the same time, it is necessary to ensure the quality of these innovations as well as their alignment to the security needs. In addition, regulators are closely related to procurers/ end-users and, as a consequence they can influence the PCP processes according to their own needs and requirements. Hence, regulators are playing a substantial part and are positively affected from PCP.

4.3.5.5 *Impacts for society*

The following impacts for regulators have been identified.

- Increase of security
- Delay in response to threats

Increase of security {S}. The main societal impact of PCP implementation is the increase of security in all sectors regardless the approach to be followed. PCP is expected to potentially improve the development of innovative products, improving also their level of security. The procedure of a PCP contract ensures a high level of competition as well as a high product quality[24] of the innovative product. Hence, it is expected that the society will benefit from such contracts, as they will be delivering strong end-results. As these results are better geared to the security threats are expected to function more efficiently than those developed in the baseline scenario.

Additionally to that, the PCP contacts are expected to deliver end-products in reduced time to the market. This could be justified due to the fact that both risks and costs in the PCP procedure are shared, therefore, these risks and costs reduced per procurer as well as the fact that the product itself is not only technology-driven (technology-push) but also market-driven (demand-pull). The latter also effects positively on the alignment of R&D requirements with actual security requirements and end-user needs.

An important caveat applies though: the overall security system is important, not just the performance of an individual piece of equipment. Security will only be enhanced if the systems (including procedures and processes) are appropriate for the 'subject of protection'. Therefore, PCP for security products does not remove the need to evaluate security systems; including whether the equipment/products employed within the system are appropriate given the threat/risk assessment.

Delay response to threats {S, E}. On the negative side, PCP contracts could lead to delays in threat response concerning security. PCP contracts are multiple competitive contacts, split into different phases (from exploration to original development). Even though such contracts provide better control of the overall project, the main drawback is potential delays of the projects which could omit the up-to-date nature of threats in the security fields. By prolonging the implementation

[24] As mentioned in the Communication (COM (2007) 799 final) from the Commission on December 2007 (Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe {SEC(2007) 1668}) *Organising the risk benefit sharing and the entire procurement process in a way that ensures maximum competition, transparency, openness, fairness and pricing at market conditions enables the public purchaser to identify the* ***best possible solutions the market can offer***.

phase, the probability of new threats occurring increases, having potentially a negative effect on the society.

4.3.6 Scoring and Summary

The impacts as assessed above are summarised in the following table. In the table the magnitude of the impacts have also been assessed for the two policy options compared to the baseline option. Key in the differentiation of the impacts between the options, is the difference in the number of procurers that together set-up a PCP scheme. This number will be larger in option 1 with the agencies running PCP schemes, than in option 2 with PCP applied via an FP scheme. After all, these agencies represent generally procurers / users from the 27 member states (and even more), and via the agencies these procurers / users will thus be involved in the PCP schemes issued by the agencies. Option 2 generally applies to those sectors in which there is no EU coordination body, such as critical infrastructure and urban transport[25]. This means that the cooperation should come from the procurers / users themselves, and given the character of the FP programme, this will be a selected number of procurers / users for a PCP scheme, and not all users from the 27 member states. This has the consequence for the scoring of the option as addressed in the table below, that any impacts that are dependent on the number of procurers / users in a PCP score better in option 1 than in option 2. There are also some impacts that are negatively affected by the number of procurers. For all other impacts the two options score equally good or bad. One should note that both options are not mutually exclusive as already mentioned. This means that if existing agencies in some security sectors are not willing, authorized or capable to run a centralized EU PCP scheme, option2 could well be applicable to these sectors with positive impacts compared to the baseline scenario.

As option 0 is the baseline (do-nothing) against which options 1 and are evaluated, the impacts have been put to '0', to express the change if one of the options would be implemented.

		Option			
Positive/ negative impact	**Impact**	**0**	**1**	**2**	
	PRODUCERS				
+	**Increased market transparency** • Bundling of demand of multiple procurers increases the transparency of the procurement process.	0	++	+	
+	**Increase of demand volumes for security products resulting in economies of scale** • PCP bundles demand from public procurers, hence market fragmentation is reduced. **PCP stimulates product according to common specifications, resulting in interoperable security solutions.** • PCP contributes to further standardisation.	0 0	++ +	+ +	

[25] There is an agency called European Railway Agency but it is not addressing urban transport issues which are local issues by definition.

		Option			
Positive/ negative impact	**Impact**	**0**	**1**	**2**	
+	**Decrease of market risk for producers**				
	• PCP decreases the market risk of product development as producers are more certain that there is a procurement process eventually;	0	+	+	
	• Risk and benefit is shared between producers and procurers;	0	+	+	
	• Better preparation to address the future market through the early collaboration with the public authorities.	0	+	+	
+	**Increase of R&D efficiency**				
	• Pooling of resources for investment by procurers;	0	++	+	
	• PCP stimulates innovation by close cooperation with end users.	0	+	+	
+	**Reduction of time-to-market**				
	• Promising R&D concepts can be developed easier and faster;	0	+	++	
	• PCP enables to supply to a broad home market quicker;	0	++	+	
	• PCP bridges gap between the TRL reached within FP R&D and commercial procurement;	0	+	+	
	• Multiple PCP contracts could slow down time to market though;	0	--	-	
	• Expression of needs by multiple procurers.	0	--	-	
+	**Decrease of product unit prices**				
	• Increased production volume enables economies of scale.	0	++	+	
+	**Improved innovation opportunities for SMEs**				
	• Reduction of disproportionate qualification or financial guarantee requirements;	0	+	+	
	• Gradually increase of commitments from participating companies;	0	+	+	
	• PCP allows a stronger role for SMEs than a subcontracting role and thus allows them to innovate more;	0	+	+	
	• PCP enables companies to grow globally;	0	++	+	
	• PCP may stimulate patent registration.	0	+	+	
-	**Increase of competition in the security R&D 'market'**				
	• Multiple PCP contracts reduce certainty of choice for single solution of producer;	0	+	+	
	• Increased competition during R&D could also be a positive factor for industry, increasing the overall performance of companies.	0	+	+	
	Increased return on R&D				
	• PCP grants positively affect the overall private return on R&D.	0	+	+	
+	**Increase of competition on the market for European products**				
	• Increase of market transparency;	0	++	+	
	• Decrease of market fragmentation.	0	++	+	
+	**Competitiveness of producers**				

Positive/ negative impact	Impact	Option 0	1	2	
	• PCP stimulates innovation by close cooperation with end users; • PCP decreases product unit prices; • PCP bridges gap between the TRL reached within FP R&D and commercial procurement; • PCP may increase the number of new products on the market.	0 0 0 0	+ ++ + +	+ + + +	
	Company, sales growth and employment growth • Increased competitiveness affects company, sales and employment growth.	0	+	+	
+	**Larger investment base** • Pooling of resources for investment by procurers.	0	++	+	
	PROCURERS / USERS				
+	**Reduction of contract costs** • Division of investment risk with multiple procurers; • No remuneration for IPR paid.	0 0	++ +	+ +	
-	**Increase of contract costs** • Competitive development increases the cost of a programme; • Increased cost of cooperation (additional overhead, cumulative specifications); • Procurers and users need to be strongly involved in the elaboration of specifications according to operational needs.	0 0 0	- -- -	- - -	
+	**More products and solutions tailored to the needs of the procurers / users** • Stronger involvement of procurers / users in the products and solutions developed (demand-side driven product development).	0	+	+	
+	**Reduction of investment risk** • Bundling of demand in PCP divides the investment risk by the number of procurers that cooperate.	0	++	+	
+	**Better value for money from R&D investment in security** • Competitive development in PCP scheme enables procurers to compare value for money of the alternatives.	0	+	+	
	RESEARCH & TECHNOLOGY ORGANISATIONS				
-	**Decrease of activities by RTOs** • Shift from pure R&D to capability development; • Stronger involvement from procurers / users.	**0** **0**	- -	- -	
	REGULATORS				
+	**Increase of products available tailored to the regulatory needs** • More innovative products developed; • Increased alignment of R&D with security needs.	0 0	+ +	+ +	
	SOCIETY				
-	**Delay in response to threats** • Multiple competitive contracts could imply long programmes not adapted to evolving nature of threats.	0	-	-	
+	**Increase of security**				

		Option			
Positive/ negative impact	**Impact**	**0**	**1**	**2**	
	• More innovative products developed; • Reduced time to market of security products; • Increased alignment of R&D with security needs.	0 0 0	+ + +	+ ++ +	

Maintaining the baseline situation would lead to a continuation of existing market failures. These would notably be a continuation of market fragmentation, lack of end-user involvement in the R&D process and a relative deterioration of the competitiveness of security manufacturing industry. Both options 1 and 2 bring about a broad set of impacts, which are to a large extent positive. The options 1 and 2 bring about impacts for each of the five different stakeholder groups. Option 1, PCP via existing Agencies, is scoring better for a selected number of impacts that are dependent on the level of coordination required or on the number of involved procurers / users. Option 1 applies to airport security and maritime border security with existing agencies such as ECAC and FRONTEX, while option 2 is suited for sectors in which there are no coordinating bodies, such as the critical infrastructure and urban transports sectors in our study. There are some impacts, especially related to the time to market for which option 2 scores better.

The overall conclusion would be that positive impacts with option 1 are relatively higher than option 2 so option 1 should be prioritized whenever possible/feasible. The benefits of pulling a large number of public procurers and reducing market fragmentation are larger than the reduced time to market for a limited set of public procurers. This can be argued by the security sector specificities were the expression of common needs, the validation/approval/certification of R&D results is strongly connected to national interests and sovereignty. Thus having from the beginning a broad consensus on these issues is key for further exploitation of the R&D results and subsequent innovative products. If agencies in option 1 are not willing to develop PCP, then option 2 might be an alternative for the airport and maritime border security sectors.

4.4 Legal analysis

This chapter provides a legal analysis of the research and development (hereafter: R&D) services exception under Directive 2009/81 (also known as the Defence Procurement Directive) in comparison with the pre-commercial procurement (hereafter: PCP) procedure developed by the European Commission on the basis of the exceptions for R&D services of Directives 2004/18 and 2004/17. The first part describes the increasing political interest at European level in stimulating the use of procurement of R&D services by contracting authorities/entities and details the content of the PCP procedure developed by the European Commission, based on this exception. The second part details the provisions on R&D services included in Directive 2009/81 (the Defence Procurement Directive) and provides an analysis of the differences with the PCP approach. The final part provides a legal analysis of the ex ante mechanisms the contracting authority can apply in order to exclude the presence of state aid according to article 107(1) TFEU.

4.4.1 Introduction on Pre-commercial Procurement mechanism and R&D procurement (e.g. 2007 Communication) within the framework of Directives 2004/18 and 2004/17

The procurement of R&D services is excluded from the scope of application of Directives 2004/18 and 2004/17, when the R&D services are co-financed by the contracting authority/entity and the R&D service provider and when the benefits do not accrue exclusively to the procuring authority/entity, but are shared with the R&D service provider[26]. This exception is based on the exclusion of R&D service contracts and prototypes from the application of the open tendering procedures under the WTO's Agreement on Government Procurement (GPA)[27].

The exemption grants the public authorities/entities more flexibility in conducting the procurements of R&D services contracts. These public authorities/entities are in this way encouraged to introduce innovations, which would increase the efficiency and effectiveness of the public service. Moreover, they are encouraged to act as first customers for innovative solutions and stimulate European (based) industry to exploit them on global markets[28].

The European Commission decided in 2006 to enhance the awareness and knowledge among public procurers regarding this possibility to promote innovation outside the strict procedures of Directives 2004/17 and 2004/18. The decision was determined by the assertion that Europe invests substantially less in R&D than its competitors - the US and Japan- and as a consequence is growing at a slower pace. A considerable difference between the US and Europe in investment in R&D was noticed in the field of public procurement. The request by public authorities of innovative solutions for the improvement of the public service is 20 times lower in Europe than in the US (2,5bn euro per year in Europe, compared to 50bn euro per year in the US)[29].

---

[26] Articles 16(f) of Directive 2004/18 and 24(e) of Directive 2004/17.

[27] Article XV(1)(e): 'The provisions of Articles VII through XIV governing open and selective tendering procedures need not apply in the following conditions, provided that limited tendering is not used with a view to avoiding maximum possible competition or in a manner which would constitute a means of discrimination among suppliers of other Parties or protection to domestic producers or suppliers: (e) when an entity procures prototypes or a first product or service which are developed at its request in the course of, and for, a particular contract for research, experiment, study or original development. When such contracts have been fulfilled, subsequent procurements of products or services shall be subject to Articles VII through XIV'.

[28] See recital (37) Directive 2004/17 ; recital (23) Directive 2004/18; Rambøll Management A/S, Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008

[29] COM (2007) 799 Final, Communication from the Commission, Pre-commercial Procurement: Driving Innovation to ensure sustainable high quality public services in Europe, dated 14 December 2007, p.11

As a consequence, the Commission detailed in a Communication of 2007 one possible approach to the procurement of R&D services, namely the PCP procedure. Because the Treaty on the Functioning of the European Union remains applicable to procurements falling partially or totally outside the public procurement directives, the PCP mechanism was developed to comply with the applicable fundamental Treaty principles and with the state aid rules.

By 2009 the procedure of pre-commercial procurement remained largely under-utilised across Europe[30]. The European Parliament released in February 2009 a Resolution in which the important role of PCP as an instrument to stimulate innovation is stressed. The Resolution requests the European Commission to take further steps to encourage public authorities to make use of this instrument, in balance with other compatible instruments of public procurement[31].

In the security sector, studies commissioned at EU level identified PCP as an alternative means to bridge the gap from technology development to commercial production. PCP would particularly benefit the small and medium sized suppliers of security equipment and systems, who encounter difficulties in transitioning from technology development (research) to full commercial development of products. Despite this favourable assessment of PCP, the public procurement procedures for security equipment and systems have been criticized as insufficiently transparent and liable for misuse, in the form of creating barriers to market entry (i.e. preference for 'local' over 'foreign suppliers)[32].

The Commission announced its intention to speed up the application of PCP in the security domain, following the conclusions of the ESRIF final report and in particular its dedicated working group on innovation[33], in order to bring research results obtained in other research programmes closer to the market[34].

4.4.2 Content of the PCP procedure within the framework of Directive 2004/18 and Directive 2004/17

The PCP procedure developed in the 2007 Communication by the European Commission represents the purchasing of R&D services with shared risks and benefits between the contracting authority/entity and the R&D service provider. The purchasing of R&D is intended to lead to the development of a new technology or a new service. The innovative solution may be desired to fulfil a need of the government (direct procurement), or it can be intended to develop a solution to a societal problem (catalytic procurement). In the first case, the public authority/entity will be interested in buying the developed product (through a subsequent competitive procurement). In the second case, the objective of the public authority/entity will be to 'pull' onto the market a technology/service that finds itself in one of the innovation phases (feasibility study, prototype, a first batch of products). In between these two cases, there is the case of cooperative

[30] Rambøll Management A/S, Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008; The Commission Communication setting a Strategy for ICT R&D and Innovation COM (2009) 119

[31] European Parliament resolution of 3 February 2009 on pre-commercial procurement: driving innovation to ensure sustainable high-quality public services in Europe (2008/2139(INI))

[32] Ecorys, Decision and TNO, Study on the Competitiveness of the EU security industry within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054, Final Report, 15 November 2009, p.32, 110, 118

[33] European Security, Research and Innovation Forum (ESRIF) Final Report, December 2009, p.200-201

[34] COM(2009)691 final Communication from the Commission, "A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations", dated 21 December 2009, p.7, 14.

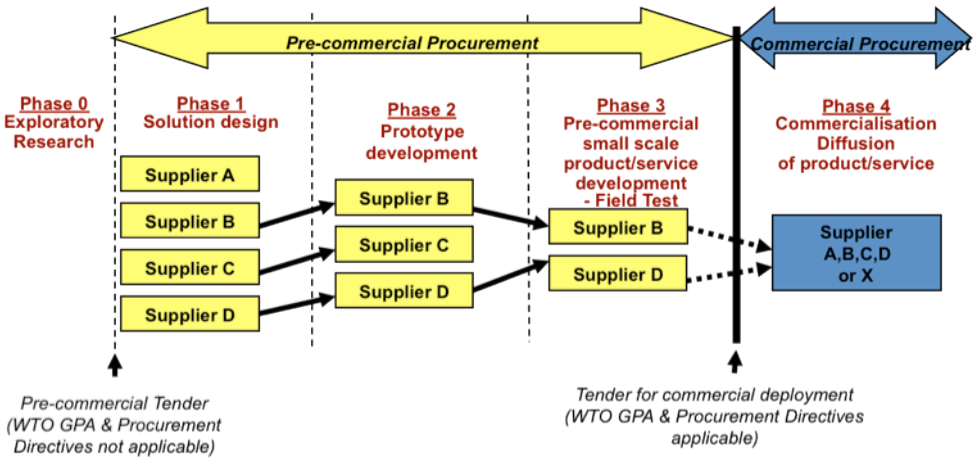
procurement, which is intended to stimulate an innovative solution of interest to the procuring authority/entity and to the private market.

PCP covers only the applied R&D part of the typical product innovation life cycle[35]. This implies that PCP does not cover fundamental research. At the other end, R&D does not include commercial development activities such as quantity production, or supply to establish commercial viability or to recover R&D costs, integration, customisation, incremental adaptations and improvements to existing products or processes[36].

The approach developed in the PCP Communication of 2007 sets out all the phases of the PCP procedure in one tender. As a starting point, it assumes that the total value of the services over all the phases in question exceeds the value of products covered by the contract. Where the value of the products covered by the contract is higher than that of the R&D services, the respective contract would constitute an R&D supply contract. Such contracts are not exempted from the application of the public procurement directives (see article 31(2)(a) Directive 2004/18[37]).

PCP thus takes the form of a single public procurement contract for R&D services managed in three stages. The first stage involves a solution exploration phase (stage1), followed by a prototyping phase (stage2), and finally a test series where the R&D service covers the development of a first batch of pre-commercial volume pre-products, validated via field tests (stage3). The first phase of this process commences with multiple different technological solutions, which are successively eliminated to yield at least 2 suppliers remaining at the final stage of development. During the PCP process the developed technologies and proposals can be evaluated and the common specifications may be adjusted.

PCP approach based on COM/2007/799 & SEC/2007/1668



Although the GPA allows discrimination against other members of the agreement (because R&D services do not fall under the scope of application of the GPA[38]), the European Commission does not recommend the exclusion of non-EU providers from participation in a PCP. The Communication recognises that each case may be different and case-by-case analysis is

[35] See FAQ 10, Frequently Asked Questions on Pre-Commercial Procurement (PCP); Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008, p.17

[36] Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008, p.15,

[37] Under the Directive 2004/17, the contracting entities have the freedom to choose for a negotiated procedure in all situations.

[38] See Annex IV Appendix I of the Government Procurement Agreement

advisable. The Communication proposes that companies bidding for a pre-commercial procurement contract can be encouraged to locate a relevant "centre of gravity" of the R&D and operational activities related to the PCP contract in Europe, without mandating companies to be European or European-owned (such as to have their head offices located in Europe or to have European shareholders[39]).

However, when procurers are concerned with issues relating to national security, participation in the pre-commercial procurement can be limited to EU service providers.

4.4.3 Correlation/relation between R&D procurement and PCP in Directive 2009/81/EC in comparison with Directives 2004/18 and 2004/17

Directive 2009/81 was adopted in order to offer more appropriate procedures for the purchase of military and sensitive equipment (and related services and works), in order to limit the need of Member States to rely on the exemptions provided by articles 36, 51, 52, 62 and 346 TFEU (ex articles 30, 45, 46, 55 and 296 EC Treaty). Member States thus have suitable means to open up the defence and security procurement to competition, in order to achieve a common European defence and security market. Directive 2009/81 is applicable both to contracting authorities in the sense of Directive 2004/18 as well as to contracting entities in the sense of Directive 2004/17[40].

For the award of contracts for R&D supplies and services, which are the key to strengthening the European Defence Technological and Industrial Base, Directive 2009/81 recognized that maximum flexibility is justified[41]. It reiterates in article 13(j) the exemption of Directives 2004/18 and 2004/17 for R&D services procured with a shared risk-benefit approach.

But unlike the other two procurement directives, Directive 2009/81 defines in detail what R&D intends. The concept of R&D services includes fundamental research, applied research and experimental development[42]. The Directive also clarifies that research and development does not include the making and qualification of pre-production prototypes, tools and industrial engineering, industrial design or manufacture[43]. These definitions of R&D activities are in line with the Frascatti Manual[44].

Directive 2009/81 deviates in this regard from the approach adopted by the Commission in the PCP Communication. There, fundamental research is excluded and original development is

[39] SEC(2007) 1668, Commission Staff Working Document, Example of a possible approach for procuring R&D services applying risk-benefit sharing at market conditions, i.e. pre-commercial procurement, 14 December 2007, p.10

[40] Note that, due to continuous privatization in the water, energy, postal, transport sectors, the number of contracting entities is reducing. Based on article 30 of Directive 2004/17, the European Commission is able to decide that a certain activity in a Member State is exposed to competition on a free market and that the directive is no longer applicable.

[41] Recital 55, Directive 2009/81

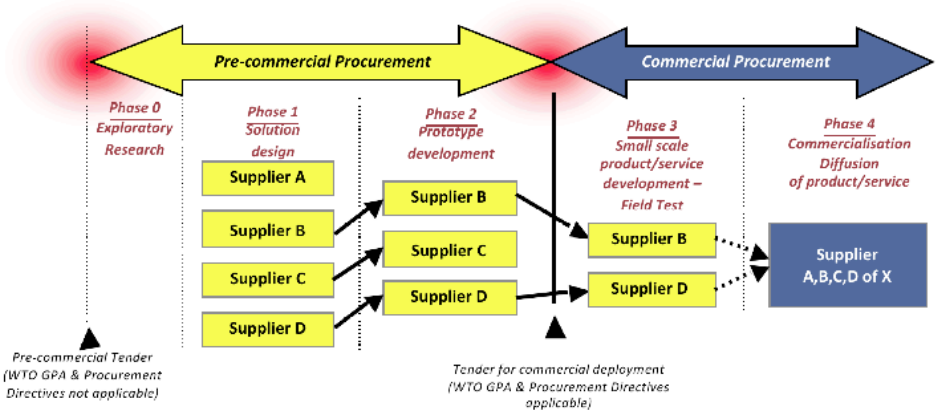
[42] See recital (13) For the purposes of this Directive, research and development should cover fundamental research, applied research and experimental development. **Fundamental research** consists in experimental or theoretical work undertaken mainly with a view to acquiring new knowledge regarding the underlying foundation of phenomena and observable facts, without any particular application or use in view. **Applied research** also consists of original work undertaken with a view to acquiring new knowledge. However, it is directed primarily towards a particular practical end or objective. **Experimental development** consists in work based on existing knowledge obtained from research and/or practical experience with a view to initiating the manufacture of new materials, products or devices, establishing new processes, systems and services or considerably improving those that already exist. Experimental development may include the realisation of technological demonstrators, i.e. devices demonstrating the performance of a new concept or a new technology in a relevant or representative environment; See also article 1(27).

[43] Recital 13

[44] Frascatti Manual, p.41.

included[45]. The justification for this deviation lies in the sensitive character of the defence and security sectors. Because it is expected that Member States will be reluctant to collaborate in R&D contracts, Directive 2009/81 imposes the opening to competition at an earlier stage during the innovation cycle, namely at the prototype stage. Hereunder we visualize how a PCP procedure under Directive 2009/81 would look like:

PCP approach based on COM/2009/81



When the contracting authority/entity organizes a procurement of R&D services outside the scope of the Directive, it may be interested to buy the product developed during this procedure. Directive 2009/81 provides the possibility to purchase directly the developed product without following a separate procurement procedure, if the contract which covers the research activities already includes an option for the direct purchase and was awarded through a restricted procedure or a negotiated procedure with the publication of a contract notice, or, where applicable, a competitive dialogue[46].

In the case of R&D contracts falling outside the scope of the directive (R&D services with shared risk-benefits), the provision entails that the contracting authority/entity will be able to buy the products developed during the R&D contract(s), when the award of the R&D contract(s) was designed as a restricted procedure or as a negotiated procedure with prior publication of a contract notice (the directive allows the free choice between these two procedures also for contracts falling under its scope of application). The contracting authority/entity would have the same possibility also when it would chose to design the award procedure of an R&D contract with shared risk-benefit approach as a competitive dialogue.

When the contracting authority/entity decides to follow one of the above-mentioned procedures and to include an option to buy the developed products at the end of the research and development trajectory, the provisions of Directive 2009/81/EC become applicable. This includes the provisions regarding the review procedures. A rejected tenderer will thus be able to contest in court the decisions taken within the award procedure of the R&D contract(s).
The Defence Procurement Directive contains an additional exception compared to the procurement Directives 2004/18 and 2004/17. All contracts procured within the framework of a cooperative programme based on research and development, conducted jointly by at least two

[45] SEC(2007) 1668, Commission Staff Working Document, Example of a possible approach for procuring R&D services applying risk-benefit sharing at market conditions, i.e. pre-commercial procurement, 14 December 2007, p.3: "Original development of a first product or service may include limited production or supply in order to incorporate the results of field testing and to demonstrate that the product or service is suitable for production or supply in quantity to acceptable quality standards".

[46] See recital 55

Member States for the development of a new product are excluded from its scope. This exception covers R&D contracts awarded within these programmes, but extends also to contracts which do not strictly regard the performance of R&D, as well as to contracts in the later phases of all or part of the life-cycle of this new developed product[47]. This provision is intended to support the activity of the European Defence Agency (hereafter: EDA), which since its establishment in 2004 has been active in the area of collaborative projects in armaments and military Research and Technology, as well as to direct collaboration between Member States, when the contracting authority/entity of one Member State awards such contracts on behalf of one or more other Member States[48].

Directive 2009/81 is also more flexible towards the award of R&D services other than those excepted from its scope of application by article 13(j) (thus not procured by following a shared risk-benefit approach, but where the contracting authority/entity keeps all the benefits and pays the total costs for the development of the innovative solution). Unlike Directive 2004/18 which allows the use of the negotiated procedure without publication of a contract notice only for R&D supplies, Directive 2009/81 allows the use of this procedure also for R&D services which are not exempted on basis of article 13(j)[49]. Directive 2004/17, on the other side, goes even further. It allows the use of the negotiated procedure without publication of a contract notice for all R&D contracts (thus also R&D works)[50].

It is also important to note that the Member States can still rely on article 346 TFEU in order to exempt the procurement of R&D services with a shared risk-benefit approach from the application of the TFEU fundamental principles and State aid rules, provided that the conditions of article 346 TFEU are met. This exception to EC law must be interpreted strictly. It is limited for example to contracts which are so sensitive that their very existence must be kept secret or to certain strategic and highly sensitive military equipment where the manufacture, purchase or sale of such equipment could in fact undermine the security of a Member State.

Summary of differences

The provisions of Directive 2009/81 for R&D services awarded through a shared risk-benefit approach contain a few differences in comparison to the equivalent provisions in Directives 2004/18 and 2004/17 and in comparison to the PCP concept as developed by the European Commission.

Firstly, the concept of R&D services under Directive 2009/81 covers fundamental research and excludes the making and qualification of pre-production prototypes, tools and industrial engineering, industrial design or manufacture. Fundamental research is though excluded from the concept of PCP as developed by the European Commission within the context of Directives 2004/17/EC and 2004/18/EC, while the pre-production prototyping phase is included.

This difference entails that contracting authorities/entities may in principle follow the procedural steps described in the PCP procedure - as outlined by the European Commission within the

[47] Directive 2009/81/EC on the award of contracts in the fields of defence and security, Guidance Note Research and development, Directorate General Internal Market and Services, p.1-2
[48] Recital 28, article.13(c)
[49] See article 28(2) (a) and (b) Directive 2009/81
[50] See article 40(3)(b) of Directive 2004/17/EC

context of Directives 2004/17/EC and 2004/18/EC - when they procure R&D services with a shared risk-benefit approach, if they limit its application to Phase 0, Phase 1 and Phase 2 of the PCP (see figure in §4.4.2). Phase 3 Field Test could not be procured outside the scope of application of Directive 2009/81/EC.
Secondly, Directive 2009/81 expressly provides that the contracting authority/entity may buy the product developed within an R&D contract (with shared risk-benefit approach) without having to organise a separate procurement procedure if the contract which covers the research activities already includes an option for those phases and was awarded through a restricted procedure or a negotiated procedure with the publication of a contract notice, or, where applicable, a competitive dialogue.

Thirdly, all contracts awarded within the framework of a cooperative programme based on research and development, conducted jointly by at least two Member States for the development of a new product are excluded from the scope of application of Directive 2009/81.

4.4.4 Legal analysis and practical implementation/scenario's of ex ante mechanisms in order to avoid illegal state aid;

Article 107(1) TFEU lays down the principle that State aid is prohibited. In certain cases, however, such aid may be compatible with the common market on the basis of Article 107
(2) and (3). Aid for research and development and innovation (hereafter: R&D&I) will primarily be justified on the basis of Article 107(3)(b) and 107(3)(c) TFEU.

When public authorities do not commission R&D from companies or do not buy the results of R&D at market price, this will normally involve State aid within the meaning of Article 107(1) TFEU.
In order to ensure that the R&D services are bought at the market price and that State aid elements are avoided, the contracting authority/entity should determine ex ante (before the start of a PCP procedure) its strategy on the sharing of risks and benefits. Subsequently, it should publish in the tender documents the distribution of risks and benefits and should carry out the tender in a competitive and transparent way in line with the Treaty principles and without any indication of manipulation[51]. This approach should normally enable the state to establish the correct (best value for money) price for the R&D service according to market conditions[52].

The procuring authority/entity will thus decide upfront which risks it will assume (related to technological development, to subsequent commercialization, to organization of the project etc.)[53] and how it will share the benefits (such as the IPRs). The risk-benefit sharing should try to balance two aspects: on the one hand, the procurement must be interesting enough for relevant

[51] The provisions on rights and obligations, including the allocation of IPRs, should for example not be the subject of negotiation after the choice of participating companies. Otherwise, the fundamental Treaty principles would be breached (the freedom of movement and non-discrimination, equal treatment and transparency principles) and State aid might be present.

[52] COM (2007) 799 Final, Communication from the Commission, Pre-commercial Procurement: Driving Innovation to ensure sustainable high quality public services in Europe, dated 14 December 2007, p.8;
SEC(2007) 1668, Commission Staff Working Document, Example of a possible approach for procuring R&D services applying risk-benefit sharing at market conditions, i.e. pre-commercial procurement, 14 December 2007

[53] Assuming risks in the commercialization phase could, for example, involve the formulation of a business case for post-project commercialization or the involvement of a buyers' group with some degree of commitment to buy the winning product(s).

suppliers from a financial point of view; on the other hand, the procurer should not carry all financial, technical or operational risks[54].

The procuring authority should calculate in advance the maximum price it will pay for the R&D services, based on a calculation of the price paid for exclusive development[55] (this is made of all the costs incurred by the company - for example the market value of the salaries of researchers/developers in a certain sector and the costs of R&D material required to perform the work - plus a reasonable margin[56]) minus the market 'present' value of the commercialisation opportunities (this value will need to reflect also the risks assumed by the participating company, such as the cost carried by the company for maintaining the IPRs and commercialising the products)[57].

Another good practice is to ask bidding companies to supply the calculation of the price reduction they can offer in return for the IPR benefits (this calculation should be relate to their business cases analysis in their PCP offer) and (2) to include a financial expert in the PCP tender evaluation committee who is charged with assessing whether the business cases and associated price reductions for the IPRs offered by different companies are indeed in line with normal market conditions in that sector[58].

In case the contracting authority/entity does not follow the above described approach and the financing of the R&D services contract could be qualified as State aid, the contracting authority/entity should analyse whether the measure is compatible with the Common market on the basis of one of the provisions of Article 107(2) or (3) of the TFEU, or with the specific rules laid down by the Commission in application of these provisions (such as the State aid framework for R&D&I). If the measure constitutes State aid, the procuring authority/entity should notify it to the European Commission, unless exempted from notification under a block exemption[59].

One of the reasons for applying the analysis of the State aid aspects ex ante is that one essential requirement of a valid exemption from the need for prior notification is that the aid is clearly identified as State aid[60]. In case of doubts on State aid issues, it is also recommendable to notify

---

[54] Rambøll Management A/S, Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008

[55] When the State keeps all the benefits

[56] FAQ Cordis, question nr.8

[57] SEC(2007) 1668, Commission Staff Working Document, Example of a possible approach for procuring R&D services applying risk-benefit sharing at market conditions, i.e. pre-commercial procurement, 14 December 2007, p.9.

[58] FAQ Cordis, question nr.8: 'one way used by patent traders to calculate the price reduction for IPR ownership rights uses the so-called present value method. It is normal practice that companies make a business case, and thus estimate the potential market over the years to come, when deciding to start investing in a new development or not. The price reduction on the PCP bid towards the procurer can be calculated as a portion of the 'present' value of projected profits for the company (the 'present' value is the value discounted back in time to the day of the bid), that is proportional to the investment/risks taken by the government (PCP price paid to the company) compared to the total investments required to turn the R&D efforts into a commercially viable product (this includes the projected investment/risks that will be carried by the company e.g. costs of maintaining IPR projection, further production, marketing and commercialisation investments). Companies can extract these values from the business case they prepare at the moment they make their PCP offer'.

[59] The Community Framework for State Aid for Research and Development and Innovation extends the scope of the block-exemption for R&D (it regards here an exemption from notification), which is currently limited to aid to small and medium-sized enterprises (hereafter: SMEs). The Framework applies also to the assessment of all non-notified aid. The Framework applies a strengthened economic approach to the State aid analysis. The aim of this Framework less and better targeted aid. In the case of fundamental research, the Framework admits that the market may be completely absent and not just inefficient. As general knowledge could benefit the whole society through spill-overs, the government is justified in these cases to pay the full cost of conducting fundamental research to companies(para.1.3.2).

[60] Framework for R&D&I

the measure to the Commission in order to exclude that the contract contains an element of State aid or to establish that the measure constitutes a compatible State aid[61].

4.4.5 IPR strategies

The issue of intellectual property rights is a crucial element of R&D procurement.
Distribution of intellectual property (IP) ownership and usage rights help to apportion incentives, risks and liabilities, as well as setting the framework for follow-on innovation in the market. The general consensus is that IP ownership should as a default go to the supplier, with due protection of the procurer's rights as an end-user in the form of either royalty-bearing or royalty-free licenses, depending on the structure of the cooperative financing. By allocating the IP to the supplier, the procurer avoids the costs of exclusive development and the supplier can consider it to be an investment in intellectual property, which could be re-applied later as a building block for other projects[62].

First, let us describe the possible IPR strategies in general, when R&D is procured. These include:

- IP owned by the supplier, and the procurer receives a royalty-free license (either exclusive or exclusive[63]);
- IP owned by the supplier, and the procurer receives a royalty-bearing license (either exclusive or non-exclusive), equal to, less than or greater than a market rate, depending on the structure of the cooperative financing (for example, 30% of the value of the contract) if the content being commercialized is developed by the private party; and, for example, 15% if the content being commercialized is being developed partially by the procurer;
- IP owned by the procurer with the non-exclusive right for the supplier to exploit commercially the IPR in exchange for a royalty-free or royalty-bearing license, depending on the structure of the cooperative financing. This model may raise concerns with the supplier that the IPRs are also made available to its competitors;
- IP owned by the procurer and the supplier receives an exclusive royalty-free or royalty-bearing license to commercialise the product;
- Shared IP ownership between supplier and the procurer.

The IP may therefore be owned by the procurer or the supplier. Licenses may be free, for a symbolic, modest or a larger fee, depending on the market value of the IPRs and the strategy of the procurer. What should be chosen must depend on the project in question (e.g. on the potential of the innovation for civil applications), and on the capabilities and ambitions of the procurer and the supplier. Many factors point to the advantages of IPRs being owned by the supplier. At a minimum the procurer should have the right to use the IP (on exclusive or non-exclusive terms) in order to ensure continuity of its internal operations and a competitive supply chain[64].

---

[61] P.9.

[62] Expert Group Report, Public Procurement for Research and Innovation: Developing practices favourable to R&D and Innovation,(Directorate General for Research, 2005), p 39.

[63] An exclusive license to use the IP means that the licensee is the sole beneficiary of the licensed rights to exploit and commercialize the IP.

[64] Rambøll Management A/S, Opportunities for Public Technology Procurement in the ICT-related sectors in Europe, Final Report, June 2008

Nevertheless, exclusive development (when IP is owned by the procurer without the possibility to award licenses) can be justified: e.g. when the public purchaser "needs" exclusive rights over projects' results (e.g. in defence or security related fields which require secrecy of results) or when the public purchaser "is" the only interested customer (e.g. development of very special customer specific equipment)[65].

At the other extreme, leaving all the IPRs to the service provider is justified when the procurer does not have the capability to develop IPR management strategies. Sharing the IPRs in the field of defence on the other side is justified when the developed innovation may have civil applications, which entail substantial societal benefits.

Let us now describe the approach of the Commission within the PCP procedure:
The approach to the procurement of R&D services, as developed by the European Commission, recommends to leave the IP ownership with the undertaking involved in the PCP procedure. The procurer will obtain a free licence to use the R&D results for internal use and will be able to require participating companies to license IPRs to third parties under fair and reasonable (FRAND)[66] conditions. Moreover, participating companies would typically not be allowed to assign the IP ownership without the consent of the public purchaser. A call-back provision could ensure that companies which fail to exploit the IP after a given period of time must re-assign the IP back to the public purchaser[67]. Such a provision would act as a safety valve in case of underutilization of potentially valuable IP due to specific failures of the company in question. The IP could then either be commercialized by the public purchaser or auctioned off to the open market.

4.4.6 Conclusions

The provisions of Directive 2009/81 on R&D services awarded through a shared risk-benefit approach differ in certain essential aspects from the PCP procedure developed by the European Commission in within the context of Directives 2004/17/EC and 2004/18/EC. This means that the PCP procedure developed by the European Commission could be applicable to R&D services in the defence and security sector from Phase 0 (Exploratory Research) up to Phase 2 (Prototype Development). Phase 3 (Field Test) could not be procured outside the scope of application of Directive 2009/81/EC.

The reasoning regarding the state aid rules and the IPRs on the other side remains valid.

[65] PCP Communication 2007, p.6; Wilkinson (2005): Public Procurement for Research and Innovation, European Commission, DG Research.

[66] FRAND means 'Fair, Reasonable and Non Discriminatory' licensing terms. The concept has been developed in the context of IPR in the standard-setting context. See OJ 2011/C11/01, Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, recital 289, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:011:0001:0072:EN:PDF

[67] SEC(2007) 1668, Commission Staff Working Document, Example of a possible approach for procuring R&D services applying risk-benefit sharing at market conditions, i.e. pre-commercial procurement, 14 December 2007, p.8.

The above mentioned differences in the scope of the R&D concept do not affect the possibilities for contracting authorities/entities from different Member States to initiate a bottom-up procurement of R&D services with a shared risk-benefit approach, unless there is national legislation which constitute a barrier to collaboration. The provisions of Directive 2009/81/EC do not limit the potential of the EU to finance cross-border procurements of R&D services with a shared risk-benefit approach. The Framework Programme 7 (FP7) is currently used to finance the costs of PCP procedures as well as the networking, related to this topic. The costs for the organization of PCP procedures cannot be financed under the Competitiveness and Innovation Framework Programme (CIP). Under CIP support can be provided to projects concerned with the first applications or market replication of innovative or eco-innovative techniques, processes, products or practices of European relevance, which have already been technically demonstrated with success but which, owing to residual risk, have not yet significantly penetrated the market[68]. Contracting authorities can also receive funding for networking and innovation policy development under CIP[69].

The Commission is currently reviewing its rules on research and innovation funding. The envisaged amendments aim to ensure coherency between the funding instruments along the whole "innovation chain" and easier access to EU funds. Amongst the measures to achieve these aims, the Commission proposes to set a "Common Strategic Framework" which would cover the current Framework Programme for Research (FP7), the Competitiveness and Innovation Framework Programme (CIP) and the European Institute of Innovation and Technology (EIT).

[68] See the PRACTICAL GUIDE TO EU FUNDING OPPORTUNITIES FOR RESEARCH AND INNOVATION, available at ftp://ftp.cordis.europa.eu/pub/fp7/docs/practical-guide-rev2_en.pdf, p.49

[69] Idem, p.21

5 Recommendations

On the basis of the country case studies and the interviews with both national public authorities and industry, we can put forward some possible policy recommendations for the European Commission to facilitate the development of PCP in the field of Security.

These recommendations are structured in order to take into consideration all the different stages of a PCP programme, from its start until the potential exploitation of R&D results:

- Preparatory actions
- Programme implementation
- Market take-up actions

Nota: recommendations voiced during our interviews with public authority officials or industrialists are summarised in the appendixes section.

5.1 Preparatory actions

Active measures are required to **'educate the market'**. Even in countries with running PCP schemes like the UK awareness of and knowledge about PCP is still confined to certain public sector organisations. Public authorities as well as private actors need to be made aware of, for example:

- The need for pre-commercial procurement (PCP);
- The difference between PCP and R&D grants or other 'conventional' procurement;
- The reasons for adding new instruments to those in the existing procurement legislation;
- The challenges, pitfalls, and solutions that are related to operating PCP schemes;
- The possibilities for EU support (both from other member states and from EU institutions).

Priorities should be given to promising sectors or technologies:

- An EU sectorial approach to PCP should focus on those cases in which European or EU institutions or agencies exist and could address security issues. Examples are ICAO, FRONTEX or EUROPOL whose role can go from organising the cooperation to recommending or even procuring technologies;
- An EU technological approach to PCP should focus on those technical fields offering the most cross-fertilization potential across security domains and beyond (possible articulation with security coordination bodies within Member States).

Above all, the Commission should consider PCP as part of an **integrated approach to security innovation policy:**

- PCP projects are positioned at the early stage of the innovation cycle and facilitate the expression of common operational security needs.
- The EC should therefore link potential PCP policies with other activities related to innovation in the field of security like standardisation and conformity assessment of security products, systems and services.

5.2 Programme implementation

One of the acknowledged EU security market failures is the misalignment between R&D activities and end-market requirements. PCP is a demand based innovation programme that could contribute to address this issue and the EC should therefore stress **end-user involvement** in programmes, including both public and private operators if applicable:

- End-users should be involved throughout the course of the project, from the expression of operational needs down to the validation stages.

The EC should ask for clear **project phasing and deliverables**

- To reduce the risk of a declining involvement due to the programme length
- To encourage SMEs and Medium Sized Enterprises participation

The EC should encourage the **financial involvement of all interested parties** in a PCP project including national public authorities but also private operators if applicable:

- Such a financial involvement shall help stakeholders appropriate the project as their own.
- It could be justified by and translated in IPR agreements. The Commission should inform interested parties of the best practices and available range of mechanisms to manage IPR in a PCP scheme.

The EC should encourage the emergence and involvement of **authoritative third parties** to translate operational needs into technical specifications and evaluate/validate R&D results

- This is a key factor of success where such capability to drive R&D is not available within public procurers
- It is also a necessary condition to build trust and confidence in the programme, both internally and externally

5.3 Market take-up actions

PCP projects only concern pre-commercial products and do not commit participants to any form of commercial procurement engagement. However, one should keep in mind that one of the key objectives of PCP is to reduce the security market fragmentation within Europe, and to mobilise public prescribers and procurers as coordinators and buyers of technology, in other words to create a bridge between R&D and the end market.

Recommendations to support the development of PCP in Europe shall therefore also consider accompanying actions to promote market adoption once the project is completed.

To this aim, the European Commission could facilitate the transition of PCP to commercial procurement by the **dissemination and promotion** of PCP results:

- towards public procurers, focusing on security benefits and increased protection level;
- towards private operators, focusing on associated return on investment;
- towards potential investors (in particular if SMEs are involved in the programme), focusing on business plan and market opportunities.

Social acceptance is identified as a major factor to consider in Europe for the security market development. Citizens may have different attitudes towards security in different Member States. The Commission could therefore leverage the cooperation on security research undertaken in PCP to **raise the social acceptance level** of commercial products and solutions, provided that the citizen's concerns have been integrated into the programme including the expression of needs and the validation of results.

6 Appendix

6.1 Annex A: Relevant legal provisions

Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts

Article 16 (f)

'This Directive shall not apply to public service contracts for:

(f) research and development services other than those where the benefits accrue exclusively to the contracting authority for its use in the conduct of its own affairs, on condition that the service provided is wholly remunerated by the contracting authority'.

Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors

Article 24 (e)

'*This Directive shall not apply to service contracts for:*

(e) research and development services other than those where the benefits accrue exclusively to the contracting entity for its use in the conduct of its own affairs, on condition that the service provided is wholly remunerated by the contracting entity'.

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

Recital 55

'Stimulating research and development is a key way of strengthening the European Defence Technological and Industrial Base, and the opening-up of procurement helps to achieve this objective. The importance of research and development in this specific field justifies maximum flexibility in the award of contracts for research supplies and services. At the same time, however, this flexibility should not preclude fair competition in the later phases of the life cycle of a product. Research and development contracts should therefore cover activities only up to the stage where the maturity of new technologies can be reasonably assessed and de-risked. Research and development contracts should not be used beyond that stage as means of avoiding the provisions of this Directive, including by predetermining the choice of tenderer for the later phases.

On the other hand, the contracting authority/entity should not have to organise a separate tender for the later phases if the contract which covers the research activities already includes an option for those phases and was awarded through a restricted procedure or a negotiated procedure with the publication of a contract notice, or, where applicable, a competitive dialogue'.

Article 13

'*This Directive shall not apply to the following:*

(c) contracts awarded in the framework of a cooperative programme based on research and development, conducted jointly by at least two Member States for the development of a new product and, where applicable, the later phases of all or part of the life-cycle of this product. Upon the conclusion of such a cooperative programme between Member States only, Member

States shall indicate to the Commission the share of research and development expenditure relative to the overall cost of the programme, the cost-sharing agreement as well as the intended share of purchases per Member State, if any;

(j) research and development services other than those where the benefits accrue exclusively to the contracting authority/entity for its use in the conduct of its own affairs, on condition that the service provided is wholly remunerated by the contracting authority/entity'.

Article 55

'1. The review procedures provided for in this Title apply to the contracts referred to in Article 2, subject to the exceptions provided for in Articles 12 and 13'.

TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION

Article 107

'1. Save as otherwise provided in the Treaties, any aid granted by a Member State or through State resources in any form whatsoever which distorts or threatens to distort competition by favouring certain undertakings or the production of certain goods shall, in so far as it affects trade between Member States, be incompatible with the internal market.

2. The following shall be compatible with the internal market:

(a) aid having a social character, granted to individual consumers, provided that such aid is granted without discrimination related to the origin of the products concerned;

(b) aid to make good the damage caused by natural disasters or exceptional occurrences;

(c) aid granted to the economy of certain areas of the Federal Republic of Germany affected by the division of Germany, in so far as such aid is required in order to compensate for the economic disadvantages caused by that division. Five years after the entry into force of the Treaty of Lisbon, the Council, acting on a proposal from the Commission, may adopt a decision repealing this point.

3. The following may be considered to be compatible with the internal market:

(a) aid to promote the economic development of areas where the standard of living is abnormally low or where there is serious underemployment, and of the regions referred to in Article 349, in view of their structural, economic and social situation;

(b) aid to promote the execution of an important project of common European interest or to remedy a serious disturbance in the economy of a Member State;

(c) aid to facilitate the development of certain economic activities or of certain economic areas, where such aid does not adversely affect trading conditions to an extent contrary to the common interest;

(d) aid to promote culture and heritage conservation where such aid does not affect trading conditions and competition in the Union to an extent that is contrary to the common interest;

(e) such other categories of aid as may be specified by decision of the Council on a proposal from the Commission'.

Article 346

'1. The provisions of the Treaties shall not preclude the application of the following rules:

(a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security;

(b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of

competition in the internal market regarding products which are not intended for specifically military purposes.

2. *The Council may, acting unanimously on a proposal from the Commission, make changes to the list, which it drew up on 15 April 1958, of the products to which the provisions of paragraph 1(b) apply.'*

WTO Government Procurement Agreement

Article XV(1)(e)

'The provisions of Articles VII through XIV governing open and selective tendering procedures need not apply in the following conditions, provided that limited tendering is not used with a view to avoiding maximum possible competition or in a manner which would constitute a means of discrimination among suppliers of other Parties or protection to domestic producers or suppliers: (e) when an entity procures prototypes or a first product or service which are developed at its request in the course of, and for, a particular contract for research, experiment, study or original development. When such contracts have been fulfilled, subsequent procurements of products or services shall be subject to Articles VII through XIV'.

Article XXIII (1)

'Nothing in this Agreement shall be construed to prevent any Party from taking any action or not disclosing any information which it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes'.

6.2 Annex B: Impact assessment – lessons from the US SBIR programme

6.2.1 Lessons learnt from the US SBIR programme

Evidence from the US SBIR programme

This section provides statistical results and lessons learnt from the US SBIR project as it has been the only programme which has been implemented for more that twenty years. SBIR has been assessed by the National Research Council in order to clarify whether the set goals and objectives of the programme were met. The NRC assessment (NRC, 2008) mentions that the programme has not been easy to evaluate so far mainly because of the limited data collection (many results are extrapolations of interviews from not more that 50 firms).

Overview of the SBIR programme

The SBIR (Small Business Innovation Research) programme was created in 1982 (1982 Act) in order to support innovation in the small businesses. Moreover, SBIR stated the following objectives, as indicated in the 1982 Act:

I. to stimulate technological innovation;
II. to use small businesses to meet Federal Research and development needs;
III. to foster and encourage participation by minority and disadvantaged persons in technological innovations and;
IV. to increase private sector commercialisation of innovation derived from federal research and development.

The Act required that all agencies with external research programmes greater than 100 billion $ (extramural budget)[70] to establish their own SBIR programme and to set aside funds redirecting a percentage of these funds to private businesses (Figure 5). There are 11 agencies participating in the programme including NASA, the NIH (National Institutes of Health), the DoD (Department of Defence) etc. From these the largest amount of amounts are distributed from the DoD (36 % annually for the Phase I awards and almost 50 % for Phase II awards). The SBIR programme functions mainly in two phases, I and II. The third phase of the programme is not financed from public sources (commercialised project) with the exception of some cases like the DoD partial financing[71]. Phase I (research feasibility) is standardised at 100.000$. Phase II (research towards prototype) involves extensive R7D and its funding amount ranges from 500.000$ to 850.000$. The scheme below depicts the structure of the SBIR programme.

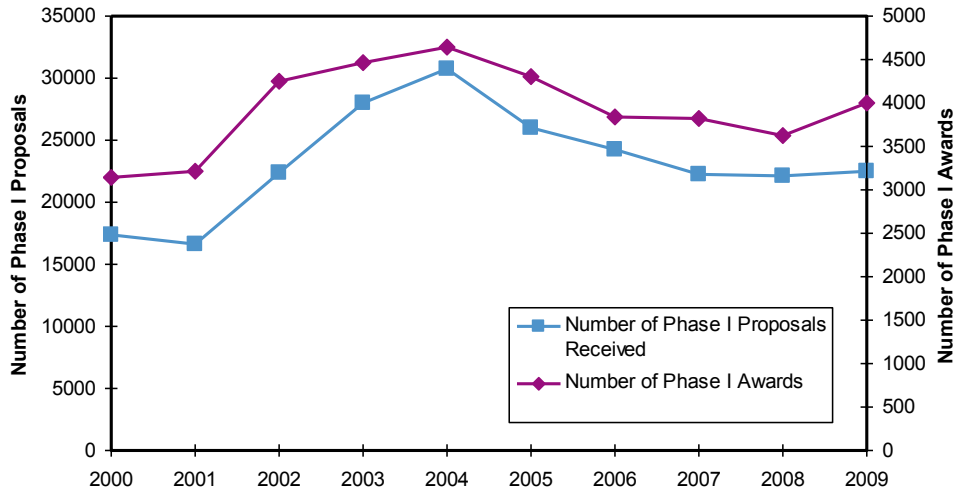
General statistics

The statistical data are retrieved from the SBIR annual reports[72] for the years 2001 to 2009 for all the agencies participating in SBIR. It should be mentioned that for a clearer picture, it is preferable to study these agencies individually. In short, the DoD is the one attributing the highest budget to SBIR, and the one receiving the largest amount of applications. As it is expected, the number of applications is relevant to the funding resources of each department and, as depicted in figure 3, to the Phase of the award.

---

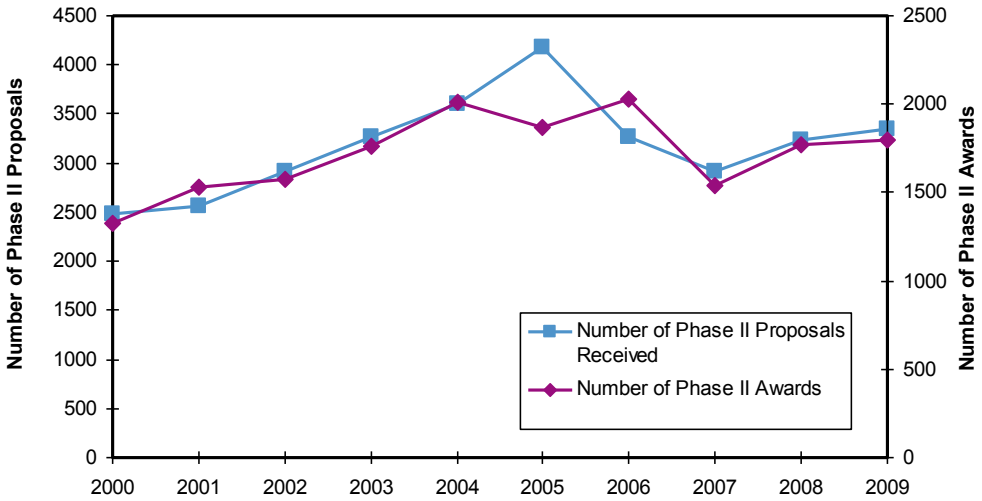
[70] The budget attributed to external research programmes
[71] At this point (Phase III), the small businesses are expected to gain additional funds from private investors etc.
[72] http://www.sbir.gov/awards/annual-reports?program=SBIR&year=2009

Figure 1 Number of proposals and awards for Phase I of SBIR



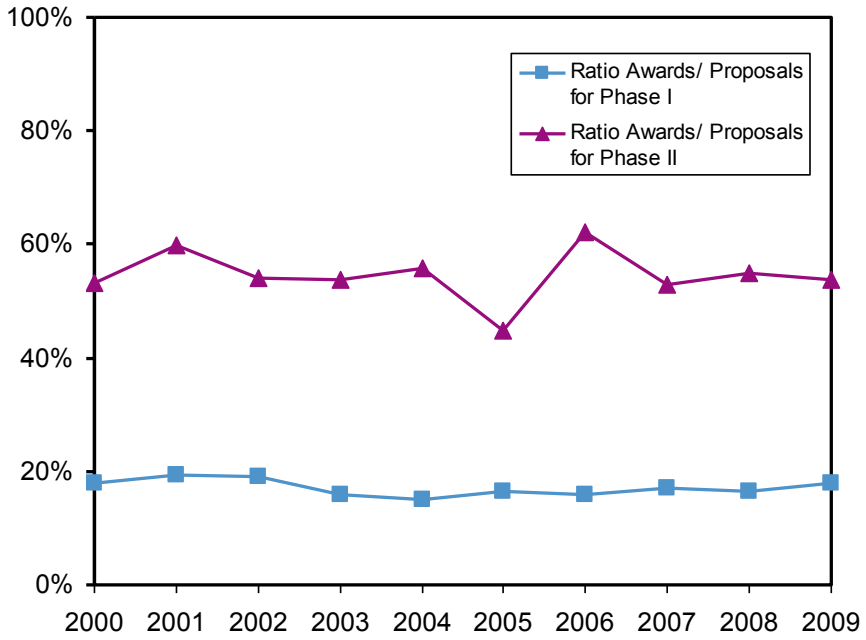
In total the SBIR applications for Phase I was on average more than 23 thousands annually, for the time-period of 2000 to 2009. For the same time period more than 232 thousands were in total submitted. From these, almost 32 thousands were awarded in total (more than 3 thousands on annual average). The ratio of awards to applications from Phase I is less than 20 % annually (figure 3). As figure 1 depicts, this ratio is representative, as the plots of proposals and awards are quite similar, almost having a linear relation. Figure 1 also shows that the highest number of applications and awards occurred in 2004. After that, the trend for both parameters declined and almost stabilised since 2007.

Figure 2 Number of proposals and awards for Phase II of SBIR



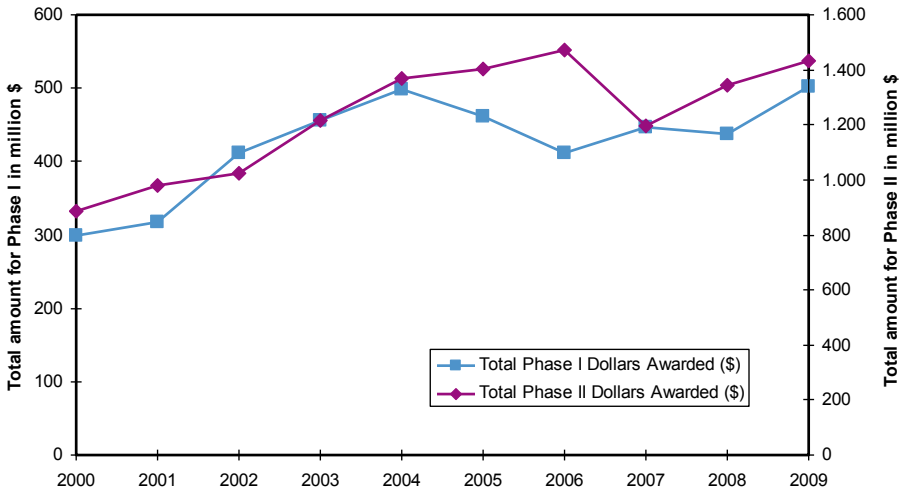
As expected, facts are considerably different for Phase II of the awards. It is safe to assume that in most second phases, there are two companies competing for the award (and sometimes only one company), as the awarding rate is in most cases more than 50 % (except from 2005, where the ratio falls to 45 %). On average, each year more than 3 thousands applications for SBIR Phase II are received; the accumulated number for the time-period 2001-2009 was more than 32 thousands. From these, more than half (17,216 proposals) were awarded. Here it is worth mentioning that the average annual growth rate of the number of applications and awards, for Phases I and II, is 3 %.

Figure 3 Ratio of awards to proposals for Phases I & II



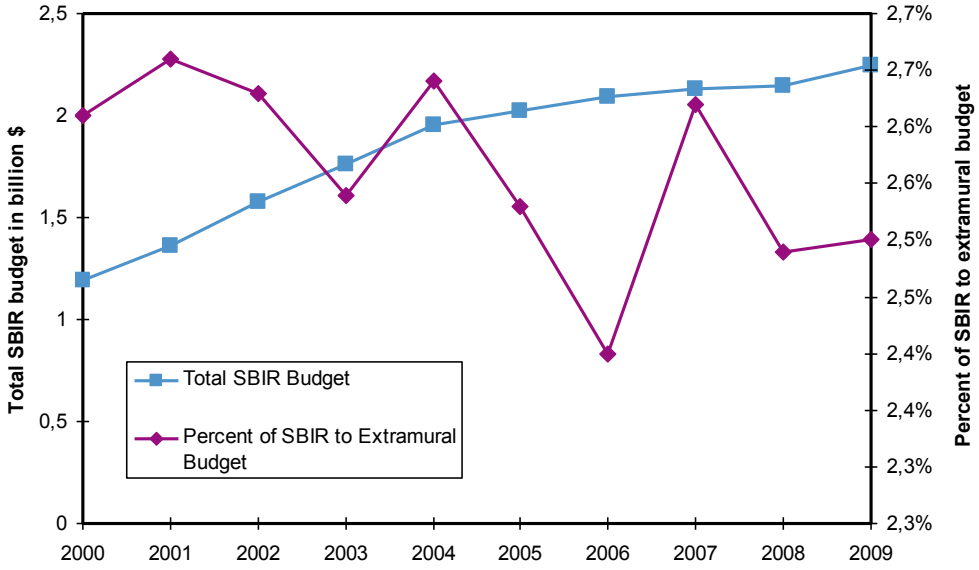
The next figure depicts the average and total values of the contracts for both phases per year. Year 2003 presents a large discrepancy compared to the other average values due to a raised average from NASA[73]. Overall, one can see that the annual average value of the Phase I contracts is increased with an annual average rate of 4 % each year (also following the inflation). Phase II awards average values also grows but on average by 2 % annually. Phase II growth is not so smooth as the Phase I growth. This could be due to the fact that Phase II is the implementation phase and incorporates more risks.

Figure 4 Total amount of awards for Phases I and II



[73] In year 2003 NASA had an average of almost 13 million dollars, while this value normally fluctuates around 600 thousands.

Figure 5 Total SBIR budget and percentage attributed regarding the Total budget



6.2.2 Evaluation Studies

Innovation and commercialisation

Audretsch et al. (2001) estimated the expected sales[74] for each project based on actual sales realised until 1999 from the DoD funded Phase II projects. The actual sales had a mean per project of $175.021, which reflected the limited number of firms with actual sales (specifically according to this result 78 out of 112 made no sales of their product). However, when the sample was limited to the 34 projects reporting sales, the mean increased to $575.539.

Audretsch et al. (2001) calculated the expected sales for all observations to be greater than zero. The positive result of the calculated expected and the actual sales coming from the SBIR projects was the first linkage of the SBIR to commercialisation. Along with that, study case-based information that if the SBIR programme did not exist, the probability of these projects reaching the Second Phase would be very limited, supported in further the positive connection of the SBIR programme and commercialisation.

NRC (2008) also mentions that:

- 34% of firms that won SBIR awards from NIH reported having generated at least 1 patent and just over half of NIH respondents published at least one peer-reviewed article;
- 80% of respondents that at least one founder was previously an academic;
- 54% of Phase I projects that did not get a follow-on Phase II, 32% did not apply for a Phase II (half of them for technical reasons).

Entrepreneurial Behaviour

The case studies as well as the survey covered in Audretsch et al. (2000) provide the following outcomes relating to the SBIR programme and the entrepreneurial behaviour:

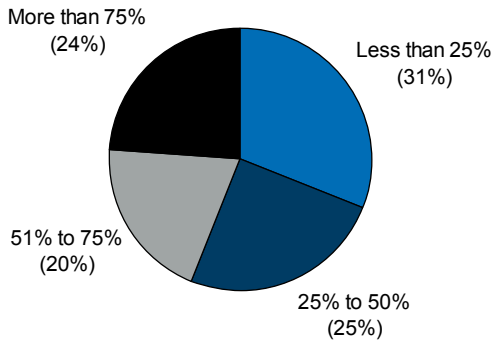
[74] The expected sales represent the sales after the completion of Phase II. Expected sales are defined in many cases due to the fact that commercialisation of a product does not occur instantly after its implementation.

Without the SBIR programme,

- a significant number of firms would not have been started. 20% of companies indicated that they were founded entirely or partly because of an SBIR award (NRC, 2008);
- a significant number of scientists and engineers would not have been involved in the commercialisation process of knowledge;
- the follow-up of the efforts from scientists from other firms;
- SBIR projects attract significant additional funding (NRC, 2008);
- After Phase II about 10% of projects were eventually supported by other federal research funding (NRC, 2008);
- Even though the findings are dependent on a limited survey (for all SBIR awards), NRC (2008) indicated that only 31 % of the respondents noted growth less than 25 % in their company. On the contrary, 44 % of the respondents mentioned that the company growth rate was more than 50 % (as shown in the figure below).

Figure 6 SBIR Impact on growth (NRC, 2008)

SBIR impacts on company growth: Percent of company growth attributable to SBIR awards
Source: NRC Firm Survey



More specifically for **university researchers**

- There is evidence that SBIR induces scientists and engineers to change their career path and apply their technological knowledge to the development of a new firm
- The SBIR awards provide a source of funding for researchers to launch start-up firms that otherwise would not have access to alternative sources of funding
- SBIR awards can have a powerful demonstration effect. Scientists commercialising research results by starting companies induce colleagues to consider applications and the commercial potential of their research. The awards also encourage other scientists to submit their research to the award process for review

Toole & Czarnitzki (2005) in their paper study the SBIR programme as a policy to adopt **academic** entrepreneurship via the NIH programmes. They build three hypotheses[75] which attempt to defined the relation of the policy measure (SBIR) to the academia.

Hypothesis 1: University researchers choose to commercialize through the SBIR program since SBIR funds are available earlier and cost less in terms of risk and return

[75] There are two more hypothese which refer to the personal development of the researchers.

Hypothesis 2: The probability of follow-on venture capital funding is greater for SBIR firms that complete the funded portion of the SBIR program indicated by winning a Phase 2 award

Hypothesis 3: Scientist-linked SBIR firms perform better than non-linked SBIR firms in terms of follow-on venture capital investment, program completion, and patenting.

Toole & Czarnitzki conclude that even though the NIH program is small in value, the number of researchers using SBIR as a "commercialisation channel" has increased. They also find evidence regarding the patenting (hypothesis 3 also known as Lerner's certification hypothesis; 1999), and specifically, they show that firms that complete the SBIR program are more likely to receive follow-on venture capital funding. Here, it is important to note that their study results are based on limited data and limited set of control variables.

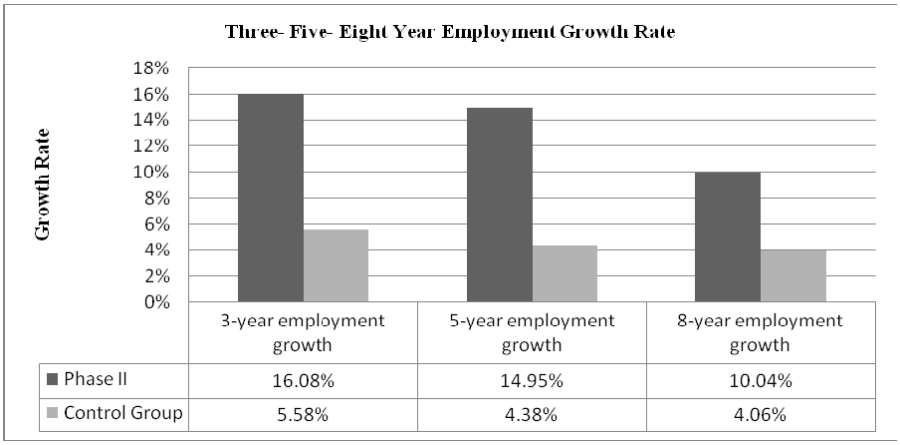
Employment growth and SBIR

Overall, two-fifths of all projects retained zero employees after completion and over one-third retained only one to two employees. Thus, on average, the direct impact of SBIR funded projects on employment is small, especially when compared to the mean number of employees in the firms. However, there are substantial cross-project differences in the number of retained employees that are explained by differences in the firms and their SBIR projects:

- funding agencies that projects with intellectual property— patents, copyrights, trademarks, or publications—retained more employees after completion of the project.
- the public funding of research by the SBIR program is more likely to stimulate employment when the government created a market for the products, processes, or services developed by the research projects.

Besides the assessment results, Ege (2009) in his research compared two samples of data, a test and a control one in order to check the effect of the SBIR programme to the average employment growth for the NIH projects for three, five and eight years. The results demonstrated at 1 % significance level that the average employment growth was higher in the groups of Phase II awardees than the non-recipients group. The following figure shows that the growth of the SBIR firms reaches 16, 15 and 10 % in three, five and eight years respectively. At the same time, the non-SBIR firms demonstrated a growth of 6, 4.4 and 4 %.

Figure 7 Comparison of employment growth rates (Ege, 2009)



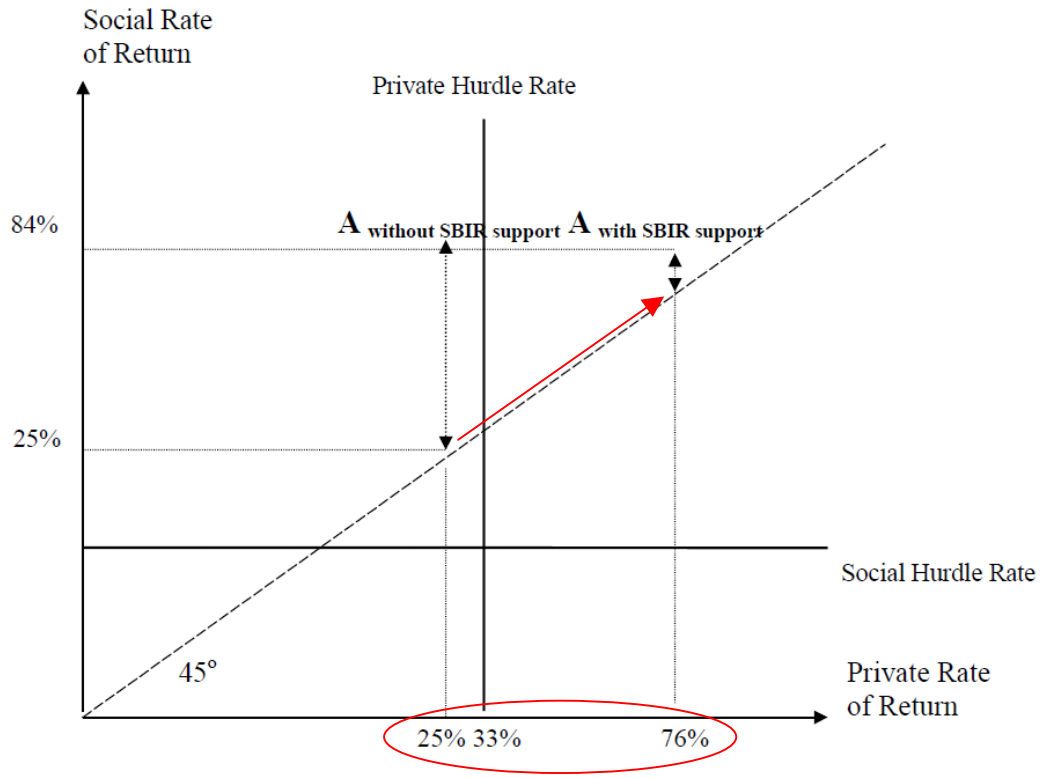
Estimates of the social returns to SBIR projects

NRC examines if the government support of private-sector R&D through the SBIR programme is justified because the social benefits associated with the funded research are greater than the social

costs, with precondition that without public support, the private costs would be greater than the private benefits. The gap between the social benefits and private investment was investigated[76] in regard to the estimated values (as mentioned in commercialisation). Based on 44 interviewees the paper concludes to:

- The funded companies (interviewees) mentioned that they *would not have undertaken the R&D without public support* because the private return that they perceived they would earn would be less than the minimum accepted rate of return required for private financing of projects (private hurdle). NRC (2008) defines the number of no-go projects up to two-thirds of the SBIR projects.
- The *estimated lower bound on the social benefits associated with the funded research is greater that the estimated private returns if there were no public support* (in the figure below 84 % for society compared to 25 % for the private investors). The average gap between the lower bound and the estimated private rate of return without SBIR support was 59 %. Public support aims at diminishing this discrepancy (red arrow in the figure below).
- The average expected rate of return without SBIR is only 25 % (8 % less than the appropriate amount to surpass the private hurdle rate). That decreases the probabilities that the private firms will undertake the research (also mentioned in bullet 1).
- The private hurdle is surpassed by 43 % with the SBIR support.
- The SBIR support helps in tackling with the funding in order to reach the appropriate social rates on return.

Figure 8 Social and Private returns relation from Audretsch et al. (2001)



In short, this study shows that, for the specific sample, the private return on investment is increased by 50 % if the implementing company is an SBIR Phase II awardee, an amount which is 34 % higher than the private hurdle rate.

[76] The authors conducted a study within 44 companies which were awarded with the SBIR Phase II funding.

Other findings from NRC (DoD)

The NRC Phase II Survey, which was sent to all firms with Phase II awards for the Department of Defence, from 1992-2002, provides evidence of substantial, if highly skewed, commercialisation. More specifically,

- Nearly half (46.7 %) of respondents indicated that the surveyed SBIR project had reached the marketplace. (i.e. They reported more than $0 in sales and licensing revenues from the project by May 2005, which is the closing date of the survey);
- Of the 420 projects reporting some sales, just four reported sales greater than $50M, another 9.4 % of projects reporting some commercialization, indicated sales between $5M and $50M.4;
- In addition, 17.6 % of respondents reported sales by licensees of their technology, with three reporting licensee sales of greater than $50M.

Sales results

NRC (2008) assesses the results of the SBIR programme also in terms of sales. The sales figures are reported for Phase II projects, based on the Phase II survey. From the overall 790 projects participating, more than 50 % of the sales was produced by 26 projects (1.4 % of the total projects). Almost three quarters projects had up to one million $ sales. One should take into account here that in order one project to reach the commercialisation phase, it could take few years. Hence, it is possible that existing projects demonstrate sales in the coming years. The NRC survey indicated that 36 % of the respondents, with no sales so far, expected sales in the future.

Figure 9 Distribution of projects based on sales (NRC, 2008)

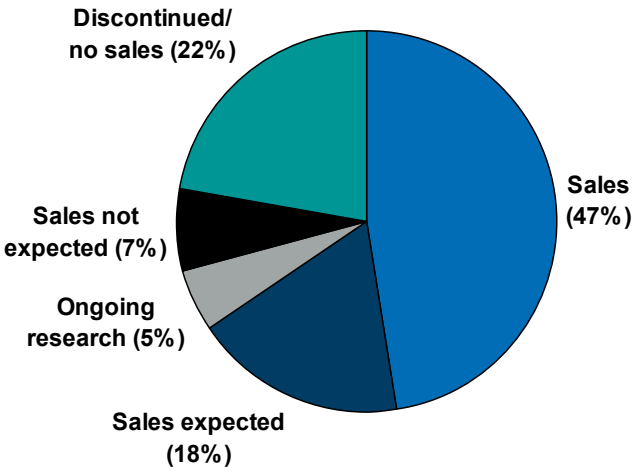
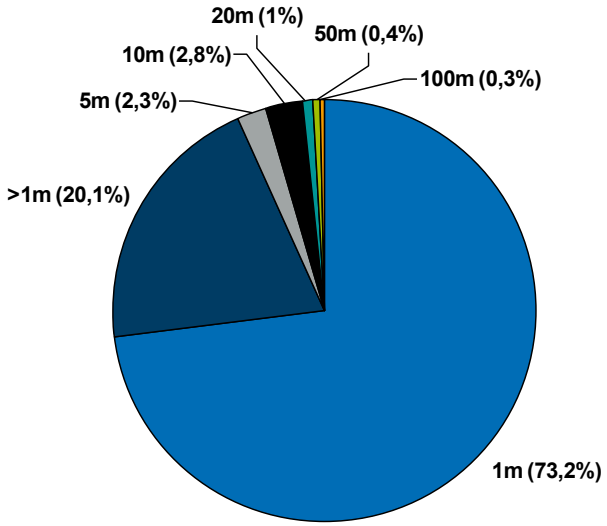


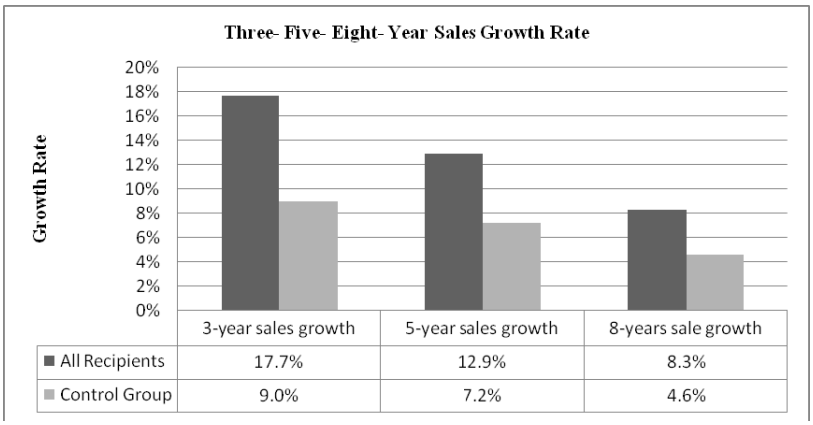
Figure 10 Distribution of sales by total sales, % of total sales $ (NRC, 2008)



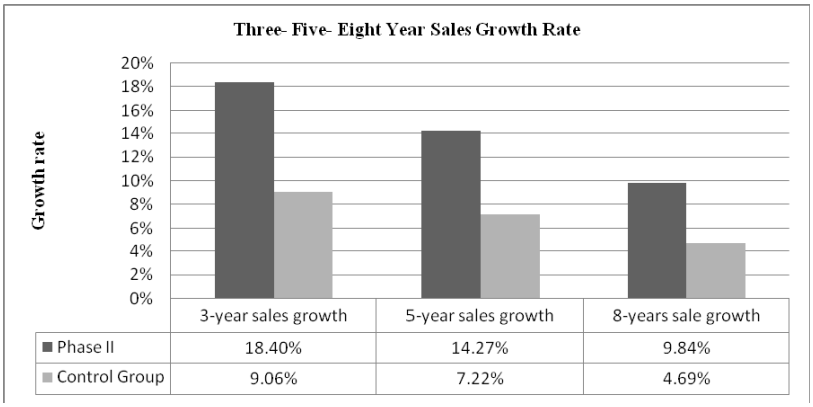
Even though the sales results are not robust, they still demonstrate that the SBIR programme can have a positive effect on the commercialisation of the project. Figure 9 shows that less than one third of the projects had or expected no sales in the future. On the other hand, almost two thirds of the projects had or expected for sales in the future. In addition, figure 10 depicts the distribution of sales in $. Almost three quarters of the projects demonstrated sales of up to 1 million $, while less than 7 % of the projects had sales more than 5 million $.

By comparing two samples of sales, Ege[77] (2009) showed that the Phase II recipients had higher sales than the non-recipients. For that he used two separate groups, one control group and the test group. Ege examined two cases: the first was comparing all recipients to the non-recipients and the second, comparing the Phase II awardees to the non-recipients. In terms of sales, in both cases, the control groups (non-recipients) showed lower average results within, in most cases, a 5 % significance level.

Figure 11 Average sales growth rate comparison (Ege, 2009)



[77] Ege's (2009) research is based on data from the NIH.



The average sales figures depict a growth rate for the first three, five and eight years. For both outcomes, the sales growth is around 18 % for three years. The Phase II growth rates are quite relevant to the overall results showing that the mean growth rate for only Phase II is similar to the one of all recipients. However, Ege's research is limited to NIH data. Hence, it is unclear whether the sales are effected equally for other agencies (e.g. the DoD which also is the main contributor to the SBIR programme). Overall, the existing information cannot show a clear-cut relation of SBIR and the sales.

6.2.3 US SBIR evaluation

The US SBIR programme (A Summary Prepared by the Small Business Technology Council)
The Small Business Innovation Research (SBIR) program was created by the US Congress in 1982. In 2002, Congress directed the National Research Council (NRC) to "conduct a comprehensive study of how the SBIR program has stimulated technological innovation and used small businesses to meet Federal research and development needs" and to make recommendations with respect to the SBIR program. The resulting study, the most scientific and comprehensive of SBIR ever undertaken, was performed by the National Academy of Sciences and was released in 2007. SBIR Programs at the following agencies were studied: the Department of Defence, the National Institutes of Health, the National Aeronautics and Space Administration, the Department of Energy, and the National Science Foundation. These five agency programs account for over 90% of the SBIR Program by dollars.

The NAS focused its study on two sets of concerns. First, how well do the agency SBIR programs meet four societal objectives set by Congress? Second, can the management of agency SBIR programs be made more effective? Are there best practices in agency SBIR programs that could be extended to other agencies' SBIR programs? The four Congressional objectives of SBIR are to:

1. stimulate technological innovation;
2. use small business to meet federal research and development needs;
3. foster and encourage participation by minority and disadvantaged persons in technological innovation;
4. increase private sector commercialization of innovations

Summary of Key Findings:

A - "The SBIR program is sound in concept and effective in practice."

- The SBIR is an effective program that is successfully meeting most of the Congressional objectives;
- The program is fair and open and regularly attracts new participants. Between 1992 and 2005, inclusive, more than 14,800 firms received at least one Phase II award;
- SBIR successfully fills a gap in early stage financing that is not addressed by other funding sources;
- Multiple SBIR awards to individual companies are not a problem. Agencies tracking new awardees indicate that at least one third of awards go to companies that have not previously won an award at that agency. Most multiple award winners are providing the government with valuable innovations and producing the significant commercial products and sales that SBIR was designed to stimulate;
- Individual departments, agencies and military services have adapted the SBIR program effectively to their particular needs. This flexibility is a key factor in the program's achievements: "The program has been successful partly because a 'one size fits all approach' has not been imposed.".

B - "Currently, the program is delivering results that meet most of the Congressional objectives"

1. Stimulating technical innovation.

Using a variety of metrics, the NAS study found that the SBIR program is contributing to the nation's stock of new scientific and technical knowledge. Knowledge output metrics included patents, publications, licenses to use patents, presentations, analytical models, algorithms, new research equipment, reference samples, prototypes, new products and processes, spin-off

companies, and "new" human capital. SBIR has also fostered a variety of relationships between universities and small business, aiding the transfer of university research to the marketplace.

2. Using small business to meet federal research and development needs.
   The NAS study found that the SBIR program objectives are aligned with, and contribute significantly to, fulfilling the mission of each of the agencies studied.
   a. • Small businesses in SBIR are providing the agencies with rapid responses to changing needs.
   b. • SBIR solicitations at DOD and NASA are directed at high-priority needs, including acquisitions.
   c. • SBIR solicitations at NSF and DoE are strongly focused on the agencies' research agendas, including those of units within the agencies, and SBIR proposals are responsive to these agendas.
   d. • SBIR topics are guidelines are utilized at NIH. Applications falling within these topics and guidelines are accepted. Committees, called "Study Sections", made up of experts from the research community, evaluate and score the applications based on their merit.
   e. • The DOD "prerelease" process helps the services receive better, more focused proposals and helps companies avoid the cost of a non-responsive application and better understand the problems the government seeks to solve.

3. Fostering and encouraging technological innovation by minority and disadvantaged persons.
   The NAS study found a mixed record in regard to this objective. The program does support the growth of a diverse array of small businesses, including minority- and women- owned business by providing market access, funding and recognition. Numerous individual instances of meeting this objective were noted. But agencies do not have a uniformly positive record in funding research by minority- and women- owned businesses, and current trends are "troubling". The study noted that documentation of minority- and women- owned business has been inadequate at certain agencies and that better monitoring and more analysis is needed.

4. Increasing private sector commercialization of innovations
   SBIR commercial success includes sales, license revenues, R&D investment and research contracts and ultimate sale of equity. The ability to track commercialization results, however, is limited and it is highly likely that efforts at quantification understate the true commercial impact of SBIR.

SBIR addresses a funding gap for early stage, high risk technology development that is not handled by venture capital investment. Venture capitalists are often focused on a given geographic area and are prone to herding tendencies, as illustrated by the dotcom boom and bust. "Many good ideas die on the way to market. This reality belies a widespread myth that U.S. venture capital markets are invariably able to identify promising entrepreneurial ideas and finance their transition to market." Most venture capital in the United States is directed at later stage innovation development.

An NAS survey of 790 Phase II projects with commercial sales showed average sales per project of about $2.4 million. The results were bifurcated. There were a handful of outsized successes, but more than half of the projects examined had sales of less than $1M. Of the sales studied, 35% were to the private sector, 32% to DOD, 10% to DOD prime contractors, and the rest to other public sector purchasers. About 14% of sales were exports.

In addition to sales revenue, SBIR companies have financed themselves through the following means (in decreasing rank of dollar value): funding and investment from non-SBIR federal funds,

private (angel) investment, US venture capital, foreign investment, company self-investment, personal funds, and state and local government funds. The average additional investment reported by 839 Phase II projects was about $1.5 million.

C - Conclusions and recommendations

The SBIR program is proving effective in meeting Congressional objectives. It is increasing innovation, encouraging participation by small companies in federal R&D, providing support for small firms owned by minorities and women, and resolving research questions for mission agencies in a cost-effective manner. The SBIR programs at each of the agencies are, by and large, operated in a fair and open manner. Although there is no single simple metric for determining commercial success, multiple metrics strongly support the conclusion that the program has a solid commercial focus, effectively commercializing innovative technologies in a variety of ways.

Perhaps the most crucial NAS conclusion was the following:
“Should the Congress wish to provide additional funds to the program is support of these objectives, those funds could be employed effectively by the nation’s SBIR program”

The NAS study makes the following recommendations:

- No fundamental changes should be made to the program;
- The program’s inherent flexibility should be maintained;
- The basic Phase I, Phase II, Phase III structure should be kept in place. Allowing firms to apply directly for Phase II awards would be detrimental to the program;
- Experimentation by the agencies, such as the Fast Track program, should be encouraged. Agencies should be encouraged to develop pilot programs and experiment with further potential improvements to the SBIR program;
- Evaluation methodologies and practices should be strengthened. Congress should consider a provision for additional program funds for SBIR management and evaluation;
- Outreach to women and minority technology entrepreneurs should be strengthened;
- Funding mechanisms beyond Phase II, such as the NSF Phase IIB program and NIH continuation awards, could be adopted at other agencies. Any such program should be carefully monitored and evaluated to ensure the result is positive;
- The standard limits on award size have not changed since 1995. If only to keep pace with inflation, Phase I awards should be increased to $150,000, and Phase II awards should be increased to $1,000,000;
- The processing periods for awards vary substantially by agency. Agencies should also specifically report on initiatives to shorten decision cycles;
- No intervention is needed regarding multiple awards to individual firms. Indeed, such intervention is likely to be counterproductive. Awards should be based on merit. Imposing quotas on multiple award winners would limit the government’s access to the highest quality solutions to science and technology needs.

6.2.4 Literature

- **Act (2000).** Federal agency expenditures for the SBIR program. Public Law APPENDIX I—H.R. 5667. TITLE I—SMALL BUSINESS INNOVATION RESEARCH PROGRAM
- **Audresch et al. (2001).** Public/Private Technology Partnerships: Evaluating SBIR-Supported Research. Published in *Research Policy 31*, , January 2002, p. 145-158
- **Ege (2009).** HOW DO GRANTS INFLUENCE FIRM PERFORMANCE? AN ECONOMETRIC EVALUATION OF THE SBIR PROGRAM AT NIH. A thesis submitted to the Graduate School-New Brunswick Rutgers, The State University of New Jersey In partial fulfilment of the requirements For the degree of Master of Science Graduate Program in Food and Business Economics
- **Gans, J. and Stern, S. (2003).** When Does Funding Research by Smaller Firms Bear Fruit?: Evidence from the SBIR Program.
- **Lerner, J. (1999).** The Government as Venture Capitalist: The Long-run Impact of the SBIR Program. Journal of Business, 72.
- **Link & Scott (2010)**. Albert N. Link, John T. Scott. Employment growth from the Small Business Innovation Research program. *Small Business Economics*. Springer Science and Business Media, LLC. 2010
- **NRC (2008)**. An assessment of the SBIR program. Board on Science, Technology, and Economic Policy, National Research Council. The National Academies Press. Washington DC
- **NRC (2007).** SBIR and the Phase III Challenge of Commercialization: Report of a Symposium www.nap.edu/openbook.php?record_id=11851&page=37
- **Toole & Czarnitzki (2005**). Biomedical Academic Entrepreneurship through the SBIR program.
- **Wallsten, S. (2000).** The Effects of Government-Industry R&D Programmes on Private R&D: The Case of the Small Business Innovation Research Program. Rand Journal of Economics, Vol. 31, N°1 (Spring 2000).
- [**copyrighted**] NRC The Small Business Innovation Research Program: An Assessment of the Department of Defence Fast Track Initiative. Board on Science, Technology, and Economic Policy, National Research Council
- [**copyrighted**] NRC The Small Business Innovation Research Program: An Assessment of the Small Business Innovation Research Program at the Department of Defence. Board on Science, Technology, and Economic Policy, National Research Council

6.3 Annex C: Table of abbreviations

Abbreviation	*Definition*
ADS (UK)	Trade organisation for the UK Aerospace, Defence, Security and Space industries
ANR (FR)	Agence Nationale de la Recherche (National Research Agency)
BBK (Ger)	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (the Federal Office for Civil Protection and Disaster Assistance).
BMBF (Ger)	Bundesministerium für Bildung und Forschung (Ministry for Education & Research)
BMI (Ger)	Bundesministerium des Innern (Ministry for Interior)
BMVg (Ger)	Bundesministerium der Verteidigung (Ministry for Defence)
BMWi (Ger)	Bundesministerium für Wirtschaft und Technologie (Ministry for Economy)
CAST (UK)	Centre for Applied Science and Technology
CCAGPI (FR)	Cahier des Clauses Administratives Générales applicables aux marchés publics de Prestations Intellectuelles (General Contracting Conditions for public procurement of intellectual services)
CIP	Competitiveness and Innovation Framework Programme
CNIL (FR)	Commission Nationale Informatique et Liberté (French data protection agency)
CONTEST (UK)	Counter Terrorist Strategy
COSG	Concepts and Tools for Global Security (Cooperative security research programmes between France and Germany)
CPNI (UK)	Centre for the Protection of National Infrastructure
CROSS (FR)	Centres Régionaux Opérationnels de Surveillance et de Sauvetage (Regional Operational Centres for Monitoring and Rescue)
DAM(FR)	Direction des Affaires Maritimes (Maritime Affairs Directorate)
DECC (UK)	Department of Energy and Climate Change
DfT (UK)	Department for Transport
DGA (FR)	Direction Générale de l'Armement (Defence Procurement Agency)
DGAC (FR)	Direction Générale de l'Aviation Civile (Civil Aviation Directorate)
DLR (UK)	Docklands Light Railway
DoD (US)	Department of Defence
DoE (US)	Department of Energy
ECAC	European Civil Aviation Conference
EDA	European Defence Agency
EIT	European Institute of Innovation and Technology
ENISA	European Network and Information Security Agency
EOS	the European Organisation for Security
ERA	European Railway Agency
ESRIF	European Security Research and Innovation Forum
ETI (UK)	Energy Technology Institute
EUROSUR	European External Border Surveillance System
FAQ	Frequently Asked Question
FIPD (FR)	Fonds Interministériel de Prévention de la Délinquance (Interministerial Fund for Crime Prevention)
FP	EU Framework Programme for Research
FRONTEX	EU agency in the field of border security
GPA	Government Procurement Agreement (under WTO rule)

ICAO	International Civil Aviation Organization
IPR	Intellectual Property Right
KIWA (NL)	Branch organisation of engineering companies
LNG	Liquefied National Gas
MEAST	Middle Eastern Countries
MEDDTL (FR)	Ministère de l'écologie, du développement durable, des transports et du logement (ministry of ecology, sustainable development, transport and housing)
NASA (US)	National Aeronautics and Space Administration
NCTB (NL)	National Coordinator for Counterterrorism
NIC (UK)	National Innovation Centre
NIH (US)	National Institute of Health
NRC (US)	National Research Council
NSF (US)	National Science Foundation
OCCAR	Organisation Conjointe de Coopération en matière d'ARmement
OFGEM (UK)	Office for Gas and Electricity Markets
OSCT (UK)	Office for Security and Counter-Terrorism
PCP	Pre-Commercial Procurement
POV	Pre-Operational Validation
PPP	Public Private Partnership
PPSL (FR)	Pôle Pilote de Sécurité Locale (Field Lab for Local Security)
R&D&I	Research & Development & Innovation
RTO	Research and Technology Organisation
RWS (NL)	Rijkswaterstaat (responsible for the main waterways and water system in the Netherlands)
SAIV (FR)	Secteur d'Activité d'Importance Vitale (Critical infrastructure of vital importance)
SBIR	Small Business and Innovation Research
SBRI	Small Business Research Initiative
SDIS (FR)	Services d'Incendie et de Secours (Departmental service for fire and rescue forces)
SGDSN (FR)	Secrétariat Général de la Défense et de la Securité Nationale (General Secretariat for Defence and National Security)
STAC (FR)	Service Technique de l'Aviation Civile (Civil Aviation Technical Department)
STIF (FR)	Société des Transports d'Ile de France (Public body in charge of regulating public transport in the Paris region)
TFEU	Treaty on the Functioning of the European Union
TOC	Train Operating Company
TRANSEC (UK)	Transport Security and Contingencies Directorate
TRL	Technology Readiness Level
TSB (UK)	Technology Strategy Board (Trade Ministry)
UITP	The International Association of Public Transport
VDI (Ger)	Verein Deutscher Ingenieure (The Association of German Engineers)
VEWIN (NL)	Branch organisation of water companies
WETSUS (NL)	Centre of excellence for sustainable water technology
W-SMART	Water Security Management Assessment, Research and Technology
WTO	World Trade Organisation

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

Watermanweg 44
3067 GG Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com

W www.ecorys.nl

Sound analysis, inspiring ideas