flemish peaceInstitute

A European Agenda for Security Technology: From Innovation Policy to Export Controls

Jocelyn Mawdsley

Report
January 2013

Table of Contents

Executive Summary

This report examines the EU agenda on security technology. It questions whether security and defence or internal and external security have largely merged since the end of the Cold War so that there is no longer any significant difference between user needs, technologies and suppliers. This belief has underpinned a variety of policy actions on security and defence technologies and industry spearheaded by the European Commission over the last decade. The report considers whether the conceptual blurring of the concepts of defence and security in academic and policy literature is in fact matched in the policy reality. It concludes that there are still significant differences particularly in terms of end user requirements, although there is overlap in terms of both technologies and suppliers.

The Commission's policy activism in developing EU policy on security industry and technology has gone largely unnoticed. The report aims to define the scope of this market and the types of technologies used. It also evaluates the policy actions taken by the EU to improve the competitiveness of EU security and defence industry. This means the report offers a clear overview of a complex developing sector. It argues that the emergence of homeland security raises difficult ethical questions inside the EU about the correct balance between civil rights and security, which are highlighted by the types of technologies emerging from the EU security research priority in the 7th Framework Programme. However, another pressing issue, highlighted by the Arab Spring, is whether the EU has sufficient control over the export of these technologies to repressive regimes, as numerous media reports showed how surveillance technologies and other policing equipment were used to repress political dissidents. The report outlines existing control mechanisms and their weaknesses and evaluates the possibilities for improving control measures in the future.

About the author

Dr Jocelyn Mawdsley is a lecturer in European and EU Politics at the University of Newcastle upon Tyne in the UK. She has published widely on European armaments issues, most recently on Franco-British defence relations and on the growth of the homeland security industrial sector. Her current research concentrates on security technologies and export controls, large states and the CSDP and interpretivism in security studies. She is also coordinating a collaborative research network on CSDP Strategy.

List of abbreviations

ASD: Aerospace and Defence Industries of Europe
CBRNE: Chemical, Biological, Radiological, Nuclear and high- yield Explosives
CCTV: Closed Circuit Television
CEA: Commissariat à l'Énergie Atomique
COARM: EU Council Working Party on Conventional Arms Exports
CSDP: Common Security and Defence Policy
DITB: Defence industrial and technological base
ECJ: European Court of Justice
EDA: European Defence Agency
EDEM: European Defence Equipment Market
EDITB: European defence industrial and technological base
ESDP: European Security and Defence Policy
ESRAB: European Security Research Advisory Board
GNI: Global Network Initiative
GoP: Group of Personalities for Security Research
ICISS: International Commission on Intervention and State Sovereignty
ICT: Information and communications technologie
MENA: Middle East and North Africa
MEP: Member of the European Parliament
MoD: Ministry of Defence
OCCAR: Organisation Conjointe de Coopération en Matière d'Armement
OECD: Organisation for Economic Co-operation and Development
SME: Small and Medium Enterprises
UAV: Unmanned aerial vehicle
UGV: Unmanned ground vehicle
UNDP: United Nations Development Programme
WEAG: Western European Armaments Group
WEU: Western European Union

1 Introduction[I]

1.1 Research Questions

Since the emergence of the modern state system in Europe, security threats have been predominantly defined as external military threats, and the armed forces have been configured accordingly. This external focus, combined with the Weberian principle that the state should have the monopoly on the legitimate use of violence, meant that the military domain was largely immune from the hollowing out of the state seen in other areas of governance. Since the end of the Cold War however, the role of the European military has changed considerably in response to changing definitions of security threats (the broadening and deepening of the security agenda), and there is much greater private sector involvement in security tasks meaning the line dividing civilian and military tasks has been blurred.

The 9/11 terrorist attacks opened up the field of internal security, particularly in the US, but also elsewhere. The desire on the part of governments to make citizens and critical infrastructure safe from any terrorist threat has led to the emergence of a global homeland security market as new technology requirements emerged. Within the EU, the complex treaty basis for action in the security domain has meant that the policy dynamics surrounding this development are not entirely straightforward. According to Edler and James (2012) the European Commission has acted as a policy entrepreneur to drive an agenda on homeland security technology development, which did not have full buy-in from either the member states or industry. The conceptual blurring in the security domain described above has allowed the ambiguous terms security industry and security technology to be elided with defence industry and defence technology, where the Commission's legal mandate is far from clear. The question is whether this blurring is now an accurate reflection of reality. Or can the civilian and military technologies and their industrial suppliers and customers still be differentiated?

The EU agenda on security technology begs an initial question of whether it remains possible to differentiate between internal and external security, military and civilian, and security and defence in the 21st century but also sparks a number of sub-questions. It is these sub-questions that drive the structure of the report:

- How has the concept of security changed in the post Cold War era? And how has this been interpreted in the EU?
- What is the security market? What are the parameters that determine its technologies and supply and demand side? Can these be differentiated from the more established defence technologies, firms and customers / users?
- What are the European policy initiatives in this area and what is driving them? What impact are they having on the market? Who are the policy entrepreneurs – the EU institutions or the member states? Are the different policy aims coherent? Is it beneficial or problematic to conflate defence and security? What impact do the security industrial and technological issues have on other EU policies?

[I] The author would like to thank Ulpia Botezatu, a PhD candidate at Newcastle University, for her enthusiasm for and highly capable research assistance with this project.

– Finally, the place of security technologies in the strategic export control system needs analysis. Do existing regimes cover security technologies? Should security technologies be controlled? What are the ethical issues?

1.2 Methodology

In order to investigate the research questions a variety of qualitative research methods were used. The rationale for selecting qualitative methods rather than quantitative ones was purely pragmatic. As the introduction to section 3 of the report will show, there are major problems with reliable data availability. Comparable national data, for example, exists for defence research spending but not for security research. This in turn substantially limits the type of quantitative analysis that can be carried out.

As Edler and James (2012) argue there has also been comparatively little academic research carried out on this topic and so much of the analysis refers to primary documents rather than secondary studies. The report also draws heavily on semi-official publications and studies carried out by members of the policy and advocacy communities. In addition to the use of official documents and grey literature, sections 3, 4 and 5 drew on a series of semi-structured interviews carried out in April 2008 (funded by the British Academy) and January 2012. Interviews were carried out in both cases with European Commission, European Parliament and European Defence Agency officials as well as with industry representatives. The initial round of interviews were carried out in 2008, shortly after the first tranches of funding had been allocated in the Security Research priority of the Seventh Framework Programme, the first major EU action connected to security industry, and aimed to discover what the industrial policy aims were, how they fitted with wider EU policies, and how they were initially received by other institutions, user groups and industry. The second round of interviews tried to elicit perspectives from all groups involved on whether they felt EU initiatives supporting the security industry had been successful, the extent to which they had contributed or would contribute to wider policy aims and to industrial competitiveness, and how interviewees viewed proposed future actions. In some cases, it was possible to re-interview the original interviewee, but in most cases individuals had moved to new posts, responsibilities had been reallocated or the agenda had moved in a different direction, making a different person more important to meet. In this report, the interviewees are not identified by name or job title, but rather by institution or sector, in order to preserve the confidentiality that many interviewed requested. Section 5 also draws on a series of telephone interviews carried out with experts on export controls carried out between May and July 2012. These aimed to scope out the current debate on the control of security technologies and the preferred methods for doing so rather than to provide specific information. Finally, section four includes an evaluation of the security research programme. To evaluate whether critical reports were accurate in their claims, a database of projects funded before July 2012 was created and used for analysis.

1.3 Structure of Report

The report starts with a literature review to consider how and why the concepts of security and defence, internal and external security and civilian and military seem increasingly intertwined. It begins with an overview of key academic and practitioner attempts to reconceptualise the notion of security in response to the challenges of the post Cold War era. It moves on to consider the emergence of the concept of homeland security and questions whether it is possible to differentiate between European and US understandings and practices in this field. Finally, it offers a brief overview of the particular usage of these concepts within the EU and the reasons why practice may be different in this arena than elsewhere. This section is conceptual in nature.

The second substantive section aims to elucidate whether or not there has been a blurring of the boundaries between security and defence, internal and external security and civilian and military as far as industry, technology and user groups are concerned. The research attempts in particular to clarify what the European Commission understands to be security industry, technologies and customers and whether this is identical to their understanding of defence counterparts. It also looks at the way in which the supply and demand side have responded to the security field as understood by the Commission.

The third substantive section offers an evaluation of the different policy initiatives within Europe which aim to improve the competitiveness of security and defence industries and foster technological development in the field and questions whether there is a coherent approach. After outlining the legal basis for EU action in this sphere and its limits, the section critically assesses EU security research funding, security and defence industrial policy, homeland or internal security policies and the intergovernmental work of the European Defence Agency. It then looks at bilateral, multilateral and NATO cooperation in this area and evaluates their ability to contribute to or disrupt EU policy. It ends by questioning the tendency within the EU to overstate the convergence between security and defence and asking whether both the supply and demand side would benefit from a more differentiated approach.

The final substantive section looks at the impact of security technologies on the arms export control agenda. It outlines why the export of certain technologies has become problematic. It then questions whether framing the debate in the same terms as the arms export control debate is productive. It offers an overview of existing controls within various regimes and discusses potential amendments to these regimes to improve the situation. Finally, it discusses the disjuncture between the desire to control some of these technologies on human rights grounds and the external requirements of the EU's internal security priorities.

2 Security and Defence: Concepts and Usage

2.1 Introduction

When discussing matters of security and defence, it is widely agreed that both academics and policy practitioners find it increasingly difficult to pinpoint what it means to be secure in the contemporary environment. This brief conceptual overview attempts to map the relevant debates to show how and why it can be argued that there has been a blurring of the concepts of internal and external security, civilian and military and security and defence. The clear national military threat definitions of the Cold War era have been replaced by a myriad of transnational security challenges (many of which require international cooperation because of their nature), changing understandings of the appropriate roles for the armed forces and other security providers, and the hollowing out of the nation state in security provision, through both privatisation and changing modes of governance. The issue is complicated further within the European Union because of overlapping institutional competences and rivalries.

This review section will first review the key academic and practitioner responses to the post Cold War challenges to the definition of security purely in terms of external military threat to a nation state. It will go on to outline the emergence of the concept of homeland security and look at whether the EU and US have converging or diverging agendas and approaches. The third section will look at the EU member states and pinpoint different practices in the area of internal security. The final substantive section will look at the EU itself and the ways in which the concepts of security and defence are used in policymaking.

2.2 Changing Academic and Practitioner Understandings of Security: Broadening and Deepening

2.2.1 The Concept of National Security / Defence in the Cold War

It is perhaps a myth that there was a clear understanding of what national security was during the Cold War. The predominance of realism as an explanatory framework for state behaviour in the world within both practitioner and academic Cold War circles, allowed policymakers to make the assumption that states act rationally to maximise their interests while prioritising state survival. But even during the Cold War security decisions were made that were not based entirely on rational calculations of national interests. If, as Katzenstein (1996: 2) points out, the Cold War is understood solely as a “bipolar, ideological struggle”, then the question of a more complicated understanding of national security can be avoided, but if the Cold War’s complexities are considered more thoroughly, similar issues regarding norms, identities and interests emerge to those identified in

the post-Cold War era. That said, it is of course true that there was a clear military threat evident during the Cold War and this took priority over any other security concerns for most European states. After the conflicts leading to decolonisation had ended, only where domestic terrorism was prolonged and serious, were substantial resources diverted from the main security concern of the East-West confrontation.

It is necessary for this study to discuss the genesis and concept of national security. The concept of national security was developed most overtly in the United States. First emerging in documents surrounding the US entry into World War I, the concept came to the fore in US government in the aftermath of World War II as a means of distinguishing between national defence (viewed as the activities of the armed forces) and security, which was seen to encompass the nation's entire capacity for war including matters such as industry, research and resources (Relyea, 2002). As far as academia was concerned, Wolfers (1952) is generally credited with developing a definition of what national security was understood to mean, by suggesting it marked a prioritisation of the security of the nation over that of the wider international community. More broadly it was defined as the ability of a nation to protect its internal values from external threats. Although it is often assumed that national security was an universally understood academic concept during the Cold War in fact, as Baldwin (1997) points out academic publications tended to avoid definitions, enabling Buzan (1991) to bemoan the lack of conceptual work on security prior to the 1980s, and the continuing neglect of this issue.

The centrality of the East-West confrontation to global security policy, and the crucial role of both nuclear weapons and the large standing armies stationed in East and West Germany in the conflict, meant that security was also defined through the prism of armed forces and their weaponry. The central concepts of Cold War analysis were the balance of power, bipolarity, containment and deterrence. This concentration on hard security for the nation state, and the resources needed to supply it, also constricted academics and practitioners from thinking more broadly or idealistically about global security. The end of the Cold War and the lack of a clear successor in terms of military threat however opened up space to reconceptualise security. Within this debate two main strands were discernible; the broadening of the national security agenda to include non-military threats, and the deepening of the security agenda to consider the security of individuals not just states.

2.2.2 New Security Concerns – the Broadening Agenda

The broadening of the security agenda has been predominantly associated in academia with neo-realists[I], who accepted the need to move beyond purely military threats to state integrity. Ullman (1983) was one of the first to critique the concentration on external military threats, pointing out that this risked both ignoring non-military threats with the power to destabilise states and underestimating threats from within. Ullman argued that:
"a threat to national security is an action or sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state or to private, nongovernmental entities (persons, groups, corporations) within the state" (1983: 133).

[I] The deepening agenda is associated more with social constructivist and critical theorist scholars, while the Copenhagen School advocated a parallel broadening and deepening agenda.

Following on from this, scholars have suggested different types of threat that should be categorised as security threats. The Copenhagen School, for example, identifies five general categories or sectors of security; military, environmental, economic, societal and political security (Buzan et al, 1998). Migration, international terrorism and environmental degradation have become standard chapters in security studies textbooks.

However, the broadening of the security agenda is not without its critics. Some, like Ayoob (1997), argue that broadened definitions of security just obfuscate issues and confuse the discussion of security, and that it is therefore unhelpful to conflate problems of global management with international security. A more serious critique is outlined by proponents of securitisation theory; here it is suggested that by defining an issue as a security issue through speech acts, politicians can claim the need for extraordinary measures to block the threat (Buzan et al, 1998). Bigo (2002) suggests, further to the Copenhagen School, that securitisation is not just about speech acts, but also about the particular practices of security professionals that securitisation allows to be applied to the threat, which may endanger human rights. As this review will show later, this critique is particularly applicable to the field of homeland security.

2.2.3 Human Security and the Responsibility to Protect – the Deepening Agenda

The deepening agenda in academic security studies has focussed on challenging the state as the referent object of security; that is the thing to be secured. The question is whether entities other than the state should be able to claim security threats that need to be dealt with. While authors have proposed moving upwards to the level of the international, and downwards to regional and societal levels, the argument that has gained most attention in the academic and practitioner worlds is that of human security; the security threats to the individual. This is not to replace the broadening agenda: if one considers referent objects other than the state, it rapidly becomes clear that existential threats extend far beyond military threats. As the 1993 Human Development Report pointed out:
"The concept of security must change from an exclusive stress on national security to a much greater stress on people's security, from security through armaments to security through human development, from territorial security to food, employment and environmental security" (UNDP Human Development Report 1993: 2).

The UNDP's 1994 Human Development Report developed this theme further arguing that freedom from fear and want for all individuals was the best way to tackle global insecurity outlining seven sources of insecurity (economic, food, health, environmental, personal, community and political security). These arguments attracted a lot of attention from academics and policy practitioners and were considered key to two policy developments: the Ottawa Treaty banning landmines and the development of the responsibility to protect guidelines for humanitarian intervention.

It is this latter development that is most important for this report, as it had a profound impact on how the EU began to think about a military role. Briefly, in 2001 the Canadian government sponsored the International Commission on Intervention and State Sovereignty (ICISS) to look at the question posed by Kofi Annan about how the UN should respond to atrocities like Rwanda and Srebrenica if humanitarian intervention was an unacceptable assault on state sovereignty. The ICISS (2001) concluded that the right to humanitarian intervention could be exercised, because the right to security of the individual can override that of the state, if the individuals are being

threatened internally by their own state or externally by other states. They also argued that it was vital to understand and address the root causes of instability and that prevention was better than intervention. ICISS (2001) agreed though on six criteria for military intervention to be permissible, namely; right authority, just cause, right intention, last resort, proportional means and reasonable prospects. The concept of intervention was later adopted by the UN with respect to genocide, ethnic cleansing, war crimes and crimes against humanity. Military intervention remains controversial and UN inconsistency in its use has been criticised. Moreover, some critics like Chandler (2008) claim that the human security agenda has led to an exaggeration of post-Cold War security threats, located them in the developing world with negative consequences for development policy, and in the developed world encouraged short term interventionism rather than long term strategic thinking.[I]

2.2.4 Consequences for Policy

There have been a variety of consequences of these debates for policy. Firstly, the shift away from viewing security through the prism of external military threats to the integrity of the nation state has changed the way in which European states, and the EU, define threats and how to deal with them. The EU Security Strategy, for example, identifies five key threats to EU security: terrorism, proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime (European Council, 2003). These require very different security policies than were prevalent during the Cold War, and where military force is to be used, it demands differently trained, armed and configured armed forces. Secondly, the human security agenda's more holistic approach to conflict intervention at all stages has meant different types of actors, both public and private, becoming involved in interventions. This has led to a blurring of the previously fairly distinct lines between civilian and military categories.

Moreover, those academics with concerns about the securitisation of a large array of challenges as security threats have their counterparts in policy-making. If academics were quick to identify new security threats, policymakers have been equally as quick to follow suit. Increasingly the EU talks in terms of security across a bewildering array of policy fields. We have policies, committees and legislation on aviation security, border security, energy security, environmental security, food security, health security and social security to list just some. Perhaps the concerns about the legitimisation of extraordinary measures through the definition of a challenge as a security threat are most obvious in the area of homeland security.

[I] The EU's CSDP missions have been criticised, for example, for the lack of strategic rationale (Flechtner, 2006).

2.3 The Concept of Homeland Security

2.3.1 Genesis

The term homeland security is often credited to President George W Bush for a speech he made shortly after the 9/11 attacks. However, homeland security was a concept used in the late 1990s by military analysts working on post-Cold War US security policy, who had labelled it a primary security concern – the 2000 report from the United States National Commission of Security in the 21st Century recommended for example that the USA needed to develop improved homeland security capabilities given the threat of terrorism (2000: 14). Cohen et al (2006) argued that at that stage there were three main problems with the US homeland or internal security status quo; firstly, the massive fragmentation of internal security responsibilities was tolerated to avoid centralisation, secondly, that the agencies charged with homeland security functions almost invariably had other primary responsibilities, and thirdly, that coordination between agencies was not always sufficient. Following the 9/11 attacks there were rapid attempts to solve these problems with the creation of first an Office and then a Department for Homeland Security and the appointment of a Homeland Security Advisor to coordinate activity. The PATRIOT Act of October 2001, which removed many restrictions on law enforcement, intelligence and immigration officials' activities to monitor the activities of citizens and non-citizens, became very much associated with the homeland security concept.

Morag (2011) suggests that homeland security is a uniquely American concept and *"is a product of American geographic isolation and the strong tendency throughout American history to believe that there was a clear divide between events, issues, and problems outside US borders and those inside US borders"* (Morag, 2011: 1). Morag (2011) argues that unlike its allies, the USA had traditionally made a clear distinction between the tools it was able to deploy abroad and those it could at home, meaning that national security techniques could not legally or institutionally be applied on US territory. Homeland Security was an attempt to bridge this divide. It was intended to be an integrative concept that brought together preparedness, response and recovery to any event that could cause massive social and economic disruption. Critics view it as an authoritarian security state. Nevertheless, the need to respond to the US homeland security agenda has led to the adoption of the terminology elsewhere without, according to Morag (2011), a clear understanding of the concept.

Morag's (2011) suggestion that the US's allies have adopted homeland security terminology without understanding the concept needs though to be set against the lack of conceptual clarity in the USA itself. Bellavita (2008: 1-2), for example, suggests that there are at least seven defensible definitions:

- a concerted national (federal, state and local) counterterrorism effort;
- a concerted national effort on counterterrorism and protection, response and recovery from manmade and natural hazards;
- what the Department of Homeland Security does to prevent, respond to and recover from terrorism and catastrophes;
- a locally directed effort to prevent and prepare for incidents likely to threaten citizens' safety and security;
- a national effort to prevent or mitigate any social trend or threat that might endanger the stability of the American way of life;

– an element of national security or
– a symbol used by government to justify the curtailment of civil liberties.

This strongly suggests that homeland security in the US is far from being accepted as an integrative concept. The Department for Homeland Security has also been controversial and has been accused of civil liberties infractions, waste and pork barrel-based distributions of grants (Mueller and Stewart, 2012; Coats, Karahan and Tollison, 2006).

2.3.2 EU-US Usage: Convergence or Divergence?

The EU and its member states, as close allies and trading partners of the US, have had to respond to the demands of its homeland security agenda not just in the counterterrorism field but also in efforts to secure US borders. This has not been a straightforward cooperation. As Rees and Aldrich (2005) point out the strategic cultures related to terrorism are very different on both sides of the Atlantic. Firstly, they claim that, in contrast to the US which declared a global war on terror, European states have regarded counterterrorism as a law enforcement and internal security issue. The more legalistic rights-based European approach meant that US policies like extraordinary rendition and Guantanamo Bay were problematic for many European politicians (Archick, 2011). Secondly, Rees and Aldrich (2005) suggest that some EU states had a long domestic history of dealing with terrorism and that this led them to think that Al Qaeda was not as radically different as the US claimed. Thirdly, attitudes to citizens' rights on electronic surveillance and private data protection differ. The European Parliament in particular raised concerns about and demanded revisions to agreements on the transfer of banking data (Swift Accord) and air passenger data (Passenger Name Record) to the US (Archick, 2011). Finally, although the EU has a counterterrorism coordinator, it has nothing corresponding in size or powers to the Department of Homeland Security.

However, many commentators claim there has been a convergence in EU-US stances on homeland security. In part, this is due to the more multilateral approach of the second Bush administration and particularly the Obama administration, which has started to act on EU civil rights concerns particularly about the treatment of detainees (Archick, 2011). Others however stress the use that the Commission made in the immediate shock of 9/11 to push for a rapid transfer of internal security powers to the EU level; something that member states had traditionally been cautious about; meant that the EU's emerging internal security policies were partially constructed in response to the US and the need for transatlantic cooperation (Lodge, 2004; Pawlak, 2009). Archick (2011) points particularly to the EU's agreement in 2010 on a first internal security strategy, which in scope at least resembles the tasks covered by the US homeland security concept. One could also point to the way in which the need for the EU to be seen to be doing something on counterterrorism, also meant the passage of measures, which had been proposed earlier but not agreed. Bossong (2008), for example, points out that 14 out of the 18 measures proposed by the Commission to the special European Council meeting of 21 September 2001 went beyond or had only tenuous connections to counterterrorism. In particular, the growing interest in surveillance technologies applies as much to other fields of the Area of Freedom, Security and Justice like migration and organised crime. For critics like Hayes (2006; 2009) and Lodge (2004) this has allowed the EU to push ahead with measures that do not correspond to the values that the EU is founded upon. For Lodge (2004: 253) the *"EU homeland security agenda and the associated biometric instruments signal the increasing securitisation of the EU but challenge the EU's commitment to the principles of freedom, democracy and justice and potentially compromise citizens' right to privacy."*

Lodge (2004) sees the EU's adoption of homeland security measures as driven by a supine subservience to the US rather than by internal imperatives.

Other commentators like Archick (2011) and Bossong (2008) are rather more sceptical about the levels of actual implementation of the agreed measures. Both cite the very different national attitudes to internal security amongst the EU states as a hindrance to successful implementation. There are many problems facing any EU attempt to implement common internal security regulations. Policing, intelligence and border control customs vary considerably within the EU as does the role of the military in internal security. There are moreover 29 distinct legal systems[I] within the EU's member states, all of which have different procedures, case law and traditions. Finally, national Constitutional Courts can declare EU measures to be unconstitutional as the German court did with the European Arrest Warrant.

However, just as within the US, critics see evidence of European states being reconfigured as security states. Hallsworth and Lea (2011: 142) suggest that there are *"three areas in which the security state is emerging—the transition from welfare to workfare and risk management; new measures to combat terrorism and organized crime; and the blurring of warfare and crime control"*. At the EU level criticism has focused particularly on attempts to secure the external border and in particular the EUROSUR integrated border management proposal, which would rely heavily on surveillance technologies sited on the EU's borders and in third countries to control the border territory. This is seen by critics as evidence of the militarisation of border control (Hayes and Vermeulen, 2012). These developments raise important ethical questions that will be returned to in section five.

2.4 Security and Defence: Usage within the EU Context

2.4.1 The EU and Defence

Although the EU now possesses a Common Security and Defence Policy, it should be stressed that it has little to do with defence as it is traditionally understood. Rather in its current state, it is primarily a mechanism to allow the EU to launch humanitarian interventions (Mérand, 2008). Member states remain keen that the policy remains intergovernmental in character. The policy area is complicated further by the fact that increasingly member states seem to prefer to keep NATO as the provider of classic defence, and by intergovernmental defence cooperation outside the EU like the Franco-British Agreements of 2010. Despite these factors, for many years the Commission has been keen to play a role in defence issues, but until recently with the security research initiative has not been successful.[II] National protectionism of uncompetitive defence firms is one reason, sensitivities about a policy that is at the core of national sovereignty another, but one important reason is that the Commission itself did not display a united front.

Mörth (2000 and with Britz, 2004) has concentrated on explaining the Commission's comparative failure by considering the governance characteristics of 'framing' (2000) and 'organising' (2004). It

[I] Within the UK, Scotland and Northern Ireland have separate legal systems to those of England and Wales.

[II] The Commission's efforts and their limitations are described at length in section 4 of the report.

can be argued that the Commission *could* have gained a defence role earlier, had it not been for its internal battles, and the relative success of member states in creating intergovernmental organisational fields such as OCCAR for multinational defence procurement management and the Framework Agreement on defence industrial restructuring. Mörth (2000) argued that rivalry between the Industry and External Relations Commissioners (Bangemann and van den Broek) in the 1990s about whose portfolio the issue belonged to, prevented two communiqués on defence industrial issues being presented as successfully as they could have been and thus leading to their rejection by the Council. This confusion about whether armaments policy belongs in the Single Market, enterprise or external relations portfolio has prevented the Commission always acting in a united or coherent fashion on this process.

2.4.2 Blurring the Concepts of Security and Defence

Within the EU itself, there is some evidence that the blurring of security and defence has been deliberately carried out by the Commission to permit it to expand its role in the defence sector (Mawdsley, 2011; Edler and James, 2012). Two key 2002 reports (STAR21 and ACARE) by lobby groups for aerospace and aeronautics made the case that technological innovation in the defence and aerospace fields was key to wider economic success for the EU. The Commission response in a March 2003 Commission Communiqué 'Towards an EU Defence Equipment Policy' was positive. Under the heading *towards a more coherent European advanced security research effort*, the Commission called for increased coordination of security research. It said it would ask national administrations, the business community and research institutions their opinions on what European agenda for research in this field should look like and *"to launch a preparatory action to coordinate such research at the EU level, focusing on a limited number of concrete technologies linked to the Petersberg tasks"* (European Commission, 2003a). The Commission seemed to be planning to fund defence research but the 2003 establishment of the European Defence Agency with a remit in that area made it politically impossible (Mawdsley, 2011). The Commission set up a Group of Personalities to look at the issue, which duly reported in 2004 making the case that there was no real difference between military and civilian research and pointing out the US investment in homeland security as a further example of how the EU was falling behind. Their report helped to shape the civilian security research priority in the 7th Framework Programme. More recently, in May 2009 a decision was taken by the European Defence Ministers to task the European Defence Agency to establish a European Framework Cooperation for Security and Defence together with the European Commission with the aim of *"maximising complementarity and synergy between defence and civil security-related research activities"*.[I] This suggests that as far as research is concerned the EU no longer really recognises a difference between the two types of research.

Does this matter? For some, it is merely a question of semantics. Tim Robinson, senior vice-president of Thales' security division, is quoted as commenting on the changing homeland security market: *"I see a shift in emphasis and an increasing balance between what we see as defence and homeland security. 'Security' is a more politically acceptable way of describing what was traditionally defence."* (Euractiv, 2006) For others like Hayes (2006; 2009), the blurring of the boundaries of military and civilian is a worrying development with concerning implications for civil liberties in Europe. Moreover, the manner in which these developments have taken place has meant that the Commission's engagement with defence issues has been concentrated in the industrial and technological sphere, which potentially leaves it with a limited outlook.

[I] Council of the European Union, 2943rd External Relations Council meeting, Conclusion on European Security and Defence Policy (ESDP), Brussels, 18 May 2009

2.5 Summary

This brief review of some of the policy and academic debates, which impact on the question of whether we can still adequately distinguish between a civilian-based homeland security and a military-based defence, has shown that the question is complex. It has shown that academic debates about the post-Cold War meaning of security have been picked up by EU policymakers. Firstly, the deepening of the security concept to look at threats to individual rather than just states and the development of the human security 'Responsibility to Protect' doctrine has deeply influenced the development of the Common Security and Defence Policy, which is not really about military defence but rather humanitarian intervention. This means that a variety of non-military public and private actors are involved in the field alongside the military. Secondly, the broadening of the security concept to encompass non-military threats forms the basis of the European Security Strategy and associated policies. There are though fears that the securitisation of a growing number of fields legitimises actions that may not be wholly compatible with EU values.

The second part of the review looked at the emergence of the homeland security concept in the United States and the influence it has had on the European Union. It argued that while there were clear differences between the European states and the US on responses to terrorism, a decade of transatlantic cooperation post 9/11 has increased convergence. It was suggested that in part this was due to the adoption by the US of some EU ideas, but more importantly that homeland security had impacted on the EU considerably because of a previous absence of policies at the EU level in this field and the need to respond to the US demands for cooperation, allowed this to frame the field within the EU. For some this was an unwelcome development particularly where civil liberties were concerned. For others, the fact that the EU was still so split by big national differences on internal security meant that the EU was a far from effective actor.

The final part of the review looked at the emergence of defence in the EU. The determination of most member states to keep the field intergovernmental had led to Commission to try to frame defence in different ways to allow it an entry point. After intra-Commission disagreements the industry and research portfolios were seen as their best opportunity to gain a role. However the setting up of the European Defence Agency with a remit in those areas meant that the Commission had to label its funding plans as security and draw on the Homeland security model. This has had the effect of blurring the lines between civilian and military still further and anchoring Commission activism in the industrial and technological spheres. In conclusion, this review suggests that there is a firm basis for questioning whether one can still draw a distinction between security and defence, civilian and military or internal and external security in the EU. However, the lack of conceptual clarity in the ways that these terms are being used mean that empirical investigations of the material factors (market and technologies) and policy aspects need to be undertaken.

3 The Characteristics of the Security and Defence Market in the EU

3.1 Introduction

This section of the report aims to outline the characteristics of both the security and defence markets in the EU. This entails looking at both the supply (firms) and demand (users) sides of the market(s) as well as the products being researched, developed and procured. The aim of the section is to see whether the security and defence markets are separate entities, have some overlap or can be largely seen as interchangeable. The section begins by outlining some of the methodological problems in defining the security and defence sectors. It then offers a definition of the security sector and what it entails. The next sub-section looks at research and technologies; it briefly discusses research funding, the uses and limitations of the taxonomy approach, and asks whether it is possible to differentiate between security and defence technologies, and finally tries to address the contemporary role of the defence and security sectors in systems of innovation. It then considers industry, offering a discussion of how security industry might be defined and how it will be treated in this report, followed by analysis of how both defence and non-defence firms have approached the sector as it expanded, and what trends are emerging. The final substantive sub-section looks at user groups; after identifying the key groups, it questions whether in the contemporary security environment, civilian and military roles and technology requirements have become blurred. Finally, it assesses whether very different civilian and military procurement and requirement definition processes mean that the demand side of the market remains fragmented, and if so whether this can be overcome.

3.2 Defining the Security and Defence Sectors: Problems and Limitations

It is important to start by recognising that any analysis of either the EU defence or even more so the security sector will struggle to find adequate quantitative data. Defence economists have long pointed to such problems as the inadequacy of OECD categories to measure defence research, given the growing importance of dual-use and civilian technologies in the sector (Molas-Gallart, 1999), or issues about defining the defence industrial base, which lead to problems of satisfactory measurement (Dunne, 1995; Hartley, 2011). Even companies widely considered to be defence firms are rarely engaged entirely on defence projects, but also have substantial civilian portfolios. Moreover, while figures for EU member states' defence expenditure, and the proportion thereof dedicated to equipment, are collected in a standardised fashion by both NATO and the European Defence Agency[I] and so can be compared, it remains the case that outside fairly well-documented major procurement projects, data on what the equipment budget is spent on, can be difficult to obtain. Similarly, detailed company accounts are not available for commercial reasons. Moreover,

[I] Additionally, the yearly analysis of global military expenditure by the Stockholm International Peace Research Institute and the International Institute for Strategic Studies are reliable sources of data.

it has thus far been impossible to get comparable data across the EU member states for the proportion of additional government expenditure used to support defence industry, through support for arms exports, offset deals, research subsidies for research carried out by state-funded universities and research institutes, regional funding, and preferential procurement processes to name just a few. These lacunae all hinder comprehensive cross-national quantitative research.

These problems are considerably greater when the security sector is considered. Firstly, the boundaries of the security sector are not the subject of a widely agreed definition (the definition of security industry used throughout this study and the rationale will be explained in 3.2.1). Even the European Commission (2012a) accepts there is no generally accepted definition. Secondly, even in comparison to the defence sector reliable statistical information is hard to obtain. As Martí Sempere (2011) points out, although Eurostat does offer some information that could help to identify expenditure, imports and exports, the NACE[I] codes that cover some security products and services e.g. code 80 for security and investigation activities and 84.24 for public order and safety activities are problematic as they do not cover everything. Moreover, codes that would cover other types of security equipment aggregate security with non-security equipment. In other words, in terms of industrial activity classifications, the security industry cannot be adequately identified and so defined. Similarly, attempting to reconcile national government data is problematic. Many states do not have a single budget line for security, rather security responsibilities are divided across ministries and agencies, and often in federal states between federal and regional levels of government (Masson and Marta, 2011). This means that comparison between states is problematic. Company level data is also sparse again for commercial reasons. While this report will draw on accumulated data from EU-level industry associations and the data in two major reports for the European Commission (ECORYS et al (2009) on the industrial competitiveness of the security industry and IRIS et al (2010) on the blurring of dividing lines between defence and security), it should be recognised that in all cases the figures given are recognised to be estimates or to represent partial or contradictory data (Hartley, 2011). IRIS et al (2010: 26) for example claim that they found it impossible to quantify the security sector as the available data were not verifiable.

3.2.1 What is the European Security Sector?

What is the European security industrial sector? A simple question perhaps, but it is one that is surprisingly difficult to answer. Viewed as a catch-all term, it covers a large number of firms supplying products and services to a range of customers from individuals to nation states in response to a wide spectrum of security issues. Drawing on definitions proposed by ESRAB (2006) among others, Martí Sempere proposes that in this sense, security industry could be defined as follows:

"The security industry addresses all products and services used specifically by the human being to prepare, prevent, protect, respond, reduce, palliate and deal with the threats and consequences that undesired events have on our society. These consequences may be summarised in terms of damage to people's life, health, property or other assets, including information." (Martí Sempere, 2011: 246)

However, as Martí Sempere (2011) accepts, for analytical purposes, it is necessary to narrow the focus. He proposes a focus on the industry that has developed to tackle insecurity caused by the

[I] Nomenclature générale des activités économiques dans les Communautés Européennes

new threats of international terrorism and organised crime, which he identifies as the most important contemporary threats. However, this suggestion leads him to exclude firms that supply traditional military equipment (Martí Sempere, 2011: 248); an exclusion which is problematic for this report, which concentrates on the EU position, given the prominence given to representatives of this sector of industry in the consultations and advisory groups set up by the European Commission to consider the security industrial section (see Section 4). Moreover, similar to the US catch-all understanding of homeland security, what EU legislation there is in this area, such as Directive 2008/114/EC on critical infrastructure protection, makes it clear that while terrorism is viewed as the primary threat, the legislation is also intended to cover all threats, including those from natural disasters (Council of the EU, 2008b).

Like Martí Sempere, ECORYS et al (2009) also emphasised the need to narrow the definition of the security sector in their report for DG-Enterprise and Industry on the competitiveness of security industry in Europe. Their model for scoping the sector differentiated between the traditional security market, based around the largely private and corporate provision of protection for persons and property, the defence market, and the 'new security market' responding to 'new' security threats such as terrorism, organised crime, cyber-crime and protection from and response to major catastrophes. The latter they argue is immature, arguably only having been called into existence since 9/11 and the subsequent US launch of a major Homeland Security programme. They do however, also point out that there is noticeable blurring between their three categories. While they may disagree on which 'new threats' to concentrate on Martí Sempere (2011) and ECORYS et al (2009) agree that there is a new type of security industry sector emerging to tackle these issues.[I]

IRIS et al (2010) took a rather different approach, as their work concentrated on analysing the extent of blurring between security and defence rather than defining the security industrial sector. Their analysis starts from an identification of mission areas identified as relevant thus defining security missions as the four types identified by ESRAB (2006) (protection against terrorism and organised crime; border security; critical infrastructure protection and restoration of security in case of crisis) and armed forces missions as limited to three areas outlined by French, Italian and German defence policy guidelines[II] (traditional defence of territory and deterrence; crisis management operations and support to civil protection) and established where blurring occurred. They then identify the technologies and equipment needed by the missions in this blurred area. Their argument that there has been a blurring between internal and external security missions is convincing and will be returned to in section 3.5.2. However, this approach left them with the conclusion that the relevant market segment is characterised by *"extreme complexity and fragmentation, with numerous industrial players coming from various industrial areas and providing different types of solutions"* (IRIS et al, 2010: 139), whereas both Martí Sempere (2011) and ECORYS et al (2009) were able to offer more focussed discussions of the nature of the security sector.

What all three analyses share (implicitly if not explicitly) is a concentration on technological products[III], rather than the full spectrum of security products and services, and an expectation that the customer will be a governmental organisation. This fits well with the EU policy agenda in this sector. Indeed the Commission (2012a) explicitly says that its security industrial policy does not

[I] This was an opinion shared by European Commission officials from DG-Research and DG-Enterprise and Industry interviewed in April 2008.

[II] This does suggest a degree of commonality between these documents that is perhaps over-stated in this report.

[III] There is a very interesting gap here between the academic literature on the security industry sector, which has largely ignored security technologies and instead concentrated on those firms supplying personnel and services to conflict zones and these policy studies funded by the European Commission with a strong technology focus.

cover service provision. For the purposes of this report therefore the security industrial sector will be defined as firms from a variety of industrial backgrounds offering technological products to governmental customers in response to security concerns. It does not therefore seek to exclude defence firms from the analysis, or to limit security concerns to specific issues, but does limit the products considered to technology-orientated ones and omits the corporate and private security customer in favour of governmental actors as this latter group has been the focus of EU policy actions.

The European Organisation for Security (EOS), which represents private security sector providers of technology solutions and services, commissioned an evaluation of the security market (thus defined) in 2011. While again they stress the limitations of the quantitative data collected, they have attempted to reconcile internal marketing figures from their members with data from commercial studies. They suggest four main sectors exist within their industry:

- Border Control
- Civil & Citizens' Protection
- Cyber Security
- Critical Infrastructure Protection.

They estimate that overall turnover in the EU for 2009 was €10.5 bn. including exports outside the EU (internal turnover estimates - border control €1.54 bn., civil and citizens' protection €2.69 bn., cyber security €1.85 bn., critical infrastructure protection 1.57 bn.€ totalling €7.65 bn.) and employed an estimated 50,000 people within the EU (EOS, 2011). ECORYS et al (2009) estimated the total value of the security sector to be approximately €36 bn. in 2008, with 80% of the demand side coming from the public sector. What technologies does this require? The ESRAB report (2006: 50) argued that the following technologies are needed:

Table 1: Security Technologies

Technology Domain	Priority Technology Areas
Signal & information technologies	Data fusion techniques, data collection/data classification, image/pattern processing technology, information fusion technology, data and information management technology (DB, etc.)
Artificial intelligence and decision support	Text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modelling and simulation, optimisation and decision support technology
Sensor equipment	Cameras, radar sensor equipment, NRBC sensors (in particular biological and chemical threat detection technologies), passive IR sensors equipments
Sensor technologies	Hyperspectral/multispectral sensors, hyperspectral/multispectral processing, autonomous small sensors/smart dust technololologies, IR sensor technologies, Terahertz sensors, optical sensors technologies, acoustic sensors — passive
Communication equipment	Reconfigurable communications, mobile secured communications, communications network management and control equipment, network supervisor, network and protocol independent secured communications, information security, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment
Human sciences	Human behaviour analysis and modelling, population behaviour, human factors in the decision process, teams, organisations and cultures
Information security technologies	Encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)
Computing technologies	Protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering
Information warfare/intelligence systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Scenario and decision simulation	Impact analysis concepts and impact reduction, advanced human behaviour modelling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation
Information systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Navigation, guidance, control and tracking	RFID tags, tracking, GPS, radio-navigation, direction finding and map guidance, bar code based tracing
Forensic technologies — biometry	Fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance
Integrated platforms	UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites
Survivability and hardening technology	EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, etc., critical buildings specific architectures, blast and shock effects

Electronic authentication	Electronic tagging systems, smart cards
Biotechnology	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques
Simulators, trainers and synthetic environments	Virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments
Chemical, biological and medical materials	Chemical and biological detection techniques
Signal protection (warfare)	Non-cooperative target recognition, geographic information systems
Space systems	Earth observation (image and communications)
Light and strong materials, coatings, …	Light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surfaces treatments for improvement of life duration, corrosion reduction
Energy generation storage and distribution	Electrical generators, electrical batteries, energy distribution

As the table shows there is some clear crossover between the technologies required in the key areas of this new market segment and those used in the defence sector. Examples include unmanned aerial vehicles, sensor technologies and mobile secure communications. Does this mean the technologies are interchangeable?

3.3 Security and Defence Technologies

This section will discuss the links between security and defence technologies. It begins with a short discussion of how defence research and development funding has worked in the EU given that there are clear implications for the way in which security R&D might work in the future. It then discusses whether or not the technologies are interchangeable and the consequences of them both being highly reliant on generic technologies.

3.3.1 Defence R&D Expenditure and Trends: Implications for Security Technology?

This brief section seeks to outline various issues that have an impact on European defence research and development funding, which are likely to be relevant to security research and development. Firstly, as the table below shows, EU spending on defence research and development is heavily focussed on two states, France and the UK, with Germany in third place. Many EU member states spend little or no money on defence research and development. Moreover, the effects of the financial crisis can be observed, noticeably in Italy and Spain post 2008.

Table 2: EU Defence R&D Spending 2006-10 (in € million)

	2006	2007	2008	2009	2010
Austria	0.81	1	0.87	7.5	1
Belgium			9.66	9.3	9.2
Bulgaria	0.42	0.42	0.244	0	0
Cyprus				0	0
Czech Rep.	18.5	18.4	21.8	20.8	20.2
Estonia	1	1	1.8	0.3	0.7
Finland	30.7	44	27.6	44.1	38.3
France	3777	3231	3281	3704	3580
Germany	1035	1213	1183.1	1088	1455
Greece	0.06	7.3	10.89	4.7	10
Hungary	0.82	0.974	2.79	3.5	0.3
Ireland	0			0	0
Italy	252	341	251.7	139	64
Latvia	0.423	0.27	0.171	0.2	0.03
Lithuania				0	0
Luxembourg				1.6	2.1
Malta				0	0
Netherlands	112	107	105	105	75
Poland	37.6	53.9	50.89	88.9	121
Portugal	5.624	4.699	4	9	7
Romania	3.4	15.3	7.3	2.3	2.1
Slovakia	3.7	2.49	3.5	5.3	0.1
Slovenia	19.5	12.8	17.5	11.2	7.8
Spain	201	276.6	314	229	162
Sweden	266	299	235	151	107
UK	4012	4011	3214	2770	2895

Source: European Defence Agency

As Masson and Marta (2011) point out these trends appear to be being followed in the government funding of security research and development. The only major programmes that they note are in Britain, France and Germany:

"In Germany, the Federal Ministry of Education and Research allocated around 123M€ for the period 2007–2011 for civil security research. In France, the Délégation Générale pour l'Armement (within the MoD), alongside the Agence National pour la Recherche conducts a "concepts, systems and tools for global security" program with 12.7M€ in funding for 2009. In the UK, the Home Office Scientific Development Branch supports the Home Office's mission, which is an investment of approximately 65M€ per year." (Masson and Marta, 2011: 113)

While this is clearly not a comprehensive overview of all security research spending in the member states, if as section 3.4 suggests, the financing of research is a concern for both defence and non-defence firms i.e. that firm-funded research will need to be complemented to a large degree by state funding, then it strongly suggests that research and development may be concentrated in comparatively few states. It is noticeable for example that prior to the EU initiative on security

research, only Sweden and Austria considered security research and development worth special funding, despite the high entry costs for firms looking to enter the market.

The European Defence Agency has, since its establishment, been trying to foster collaborative research and development. However, as the table below shows, such efforts are declining again, and do not show a great advance over the Western European Armaments Group's (WEAG) collaborative efforts.

Table 3: EU Collaborative Research and Technology Spending (in € million)

Year	Amount
2005	206
2006	254
2007	332.75
2008	412
2009	290
2010	246

Source: European Defence Agency

This suggests that the European Commission may struggle to increase member state participation in collaborative security research outside of the EU research framework programmes and other EU funding.

3.3.2 Can Security and Defence Technologies be Differentiated?

There are a variety of different systems of technology labelling, or taxonomies, in use in Europe and worldwide including those from the European Defence Agency (EDA), the Western European Armaments Group (WEAG), the European Security Research Advisory Board (ESRAB), the Militarily Critical Technologies List (MCTL), and the Developing Science and Technologies List (DSTL). A project called the stakeholder's platform for supply chain mapping, market condition analysis and technologies opportunities (STACCATO) tried to bring in particular the work done by WEAG and ESRAB together to provide a taxonomy that would be of use to both the supply and demand side.[I] The taxonomy attempted not just to map technologies used and how these feed into equipment, but also how to classify the needs of missions as defined by EU policy. The seven sections are:

- (I) Technologies and Components
- (II) Equipments and sub systems
- (IIIA) Systems-Services Functions
- (IIIB) Design-Manufacturing
- (IV) Integrated platforms and systems and Human Factors
- (VA) Missions Capabilities
- (VB) Policy and Support

A later attempt was made by the Joint Research Centre to map the technologies that firms possessed onto mission capabilities and support needs but this required voluntary participation by firms and proved not very successful. The STACCATO taxonomy has also been criticised for not paying sufficient attention to the security technologies supplied by non-defence suppliers. The

[I] The full taxonomy can be found at: http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf

problem of the multiplicity of taxonomies or classifications that are in use is that it can prove difficult (potentially in arms control / export negotiations) to agree on how a particular technology should be classified.[I]

It is true to say that there has been some blurring of the line between military and non-military products supplied to defence and security end-users; this is partly due to some convergence in their missions e.g. counter-insurgency has commonalities with counter-terrorism, but also because of the dynamics of technological innovation. However, it is important not to overstate this case. While there are some products that are of interest to both military and non-military users such as secure communications and surveillance technologies like unmanned aerial vehicles and sensors, there still is a large amount of difference between military and non-military products.[II] Aircraft-carriers, fighter jets and advanced missile technology, for example, remain clearly military products. A missile manufacturer like MBDA is unlikely to enter the security market precisely because there is little crossover in useful technologies. Stankiewicz et al (2009) insist that this division will be maintained as ministries of defence will be careful to retain control over and investment in some defence technologies for reasons of national security and security of supply. Where there is less difference in the technologies underpinning the products. If we reconsider the STACCATO taxonomy of technologies of interest to security and defence users, then James (2009a: 7) argues that there are still several technology classes that "are essentially defence-specific and have limited (or no) application outside in other fields (namely, 102 – Materials for deterrence; 103 – Stealth materials and technologies; and, 105 – Energetic materials)."[III] Most defence and civilian security products however are heavily reliant on a wide range of generic technologies.

3.3.3 Innovative Technologies and the Security and Defence Sectors

While during the Cold War, it was assumed that defence technologies were the most advanced, spinning out into commercial applications but with the technologies themselves essentially secure, today as Stankiewicz et al (2009: 21) argue:

"The end of self-sufficiency is indeed a pervasive phenomenon. It affects firms, industries, sectors and countries. The vertically-integrated techno-military complexes are no longer secure sources of most relevant technologies. Defence and civil security products rely heavily on generic, globally available technologies not least information and communications technologies (ICTs). Advances in microsystems, nanotechnology, unmanned systems, communications and sensors, digital technology, bio- and material sciences, energy and power technologies and neuro-technologies have all been identified as important for the defence sector and most if not all can be characterised as generic technologies."

In other words, the Cold War defence innovation model is breaking down. Industry representatives interviewed in January 2012 were ready to admit that defence firms were no longer at the forefront of innovation and had not been for some time. Because both military and non-military security products draw on generic technologies, this does blur the boundaries around both

---

[I] There has been some work using data mining techniques to overcome this. See for example Thorleuchter and van den Poel (2011).

[II] In addition obvious areas of overlap are in non-technological areas such as uniforms, protective clothing, logistics etc.

[III] One industry representative interviewed in January 2012 suggested that the overlap between security and defence technologies shown in the Staccato taxonomy had possibly been overstated as the participants in the research had come from the defence sector. It was suggested that if telecommunications or ICT firms had carried out a similar exercise the results might be different.

knowledge production and the application of the technologies, not just between military and non-military security products, but with wider civilian and commercial technology innovation (James, 2009b). Moreover, the fact that many defence and security products draw on commercially available technologies, particularly ICT technologies, mean that these technologies are also potentially available to hostile users if they have or acquire the systems integration capacities to utilise them. European systems integration capacities, and the protection of these capacities, may therefore turn out to be more important than the technologies per se. Industry interviewees in January 2012 pointed out that this also means new dilemmas around security of supply are emerging. Microchips, for example, are crucial for many contemporary defence products, but the quantity and frequency of supply that defence firms need in Europe is not sufficient to be highly attractive to suppliers in Asia and North America. This also means that there are new challenges for those concerned about defence and security technology proliferation. In conclusion, the question is perhaps less whether defence and security products are blurring but more the fact that they are both dependent on generic technologies and so much less able to be protected than in the past.

3.4 Supply Side

3.4.1 Defence Firms and their Approaches to the Security Sector

It is not possible to generalise about the approach of all defence firms to the security sector, but if we breakdown the structure of the defence industrial sector into tiers of producers, some generalisations become possible. The defence industrial sector can be described as a pyramid with systems integrators like BAE, EADS, Thales and Finmeccanica at the top in the first tier, specialised sub-system producers in the second tier, and below this a large range component and service suppliers, which act as sub-contractors to the higher levels and are often SMEs.[I] Contrary to what is often assumed, after a period of contraction following the end of the Cold War, many of Europe's defence firms are performing well. Employment across the aerospace and defence industry has risen steadily since 2003 and has been strong in the defence sector (notably in the land industry), while profit margins have remained good: this is partially explained by changes in statistical calculations on employment in the sector by some states like Germany and the Netherlands, but is largely explained by steady export growth particularly to Asia and the Middle East (ASD-Europe, 2010).[II] While future prospects within Europe will be negatively affected by the financial crisis and austerity measures, the point that is important to make here, is that the defence sector has not been forced to enter into the security market, rather firms have been able to do this on their own terms. This has meant that the strategic calculations have varied from firm to firm. Interviews in 2012 with industry representatives from the defence sector suggested that initial belief amongst defence firms, in the period around 2003 after US announcements of Homeland Security funding, that this would be a thriving new market segment with substantial business opportunities, have since been tempered as European government demand has failed to meet these early predictions.

Defence firms have three options to enter into the security market; firstly, they can develop a presence in the security market through exploitation of their existing defence technologies;

[I] It is worth emphasising that while identifying as defence firms, many have a substantial civilian business especially in aeronautics. Interviewees from the sector in 2012 suggested that the civilian-military divide was more meaningful to categorise their business activities than a defence-security one.

[II] These statistics do not include suppliers which do not consider defence to be their main interest: this includes many firms within supply chains.

secondly, they can diversify through the acquisition of security firms; and thirdly, they can enter the market through partnerships. IRIS et al (2010: 143-44) suggest however that for defence firms to move successfully into the security market three business conditions need to be in place:

- Valuable and distinctive technologies that are viewed as such by security customers and which have a commercial advantage over those offered by non-defence firms. (It is worth noting that for some defence firms their technologies may be more readily diversified into different sectors entirely.)
- Access to the necessary complementary capabilities – here they suggest that marketing to new types of customer is a weakness that defence firms have to compensate for (potentially by acquiring firms that are already active in the sector).
- Viable business model that accepts that the security sector works in a different way to the defence sector and that is realistic about different overheads, investment needs and regulatory environments.

The different types of customer, business and regulatory environments will be returned to in more depth in section 3.5.

Let us consider how the systems integrators have responded to the security market. Firstly, they have all made a number of acquisitions of smaller firms[I] as the table below shows:

Table 4: Major Acquisitions by European Defence Firms 2005-10

Companies	Date	Firms acquired	Domains
EADS	2005	Nokia's Professional Mobile Radio (PMR) activities	Secure telecommunication
	2006	French company Sofrelog	Vessel Traffic Service (VTS) systems and Coastal Surveillance Systems (CSS)
	2008	US PlantCML	Emergency response solutions and services
	2010	EADS DS and Atlas Elektronik (AE) have decided to consolidate their position in maritime safety and security market by merging their subsidiaries Sofrelog and Atlas Maritime Security, a spin-off of AE, to form "Sofrelog Atlas Maritime Security" (SA Maritime Security)	
Thales	2007	Rail signalling and security systems business acquired from Alcatel-Lucent	
	2008	British company n-Cipher	Encryption firm (Internet and communications system security market)
Safran	2008	Dutch company Sdu-Identification	Secure identification documents, including electronic and biometric passports, ID cards and driver licenses
	2009	US Motorola's biometrics business	Printrak trademark. Automated fingerprint identification systems (AFIS)
	2009	81% of US GE Homeland Protection	Systems to detect dangerous or illicit materials (X-ray tomography detection systems). Much of the technology is designed for use in airport screening.

[I] Several interviewees suggested in January 2012 that the acquisition of SMEs in particular by defence firms on occasion was in order to meet requirements for participation in the security research programme, which looked for geographical balance and SME participation.

Finmeccanica	2007	British VEGA Consulting Services Ltd (VEGA)	Project management as well as advanced solutions for simulation and training
	2008	US DRS Technologies	VTMS, port security, law enforcement, border control; subcontractor to Boeing on SBInet
BAE Systems	2008	British DETICA	Technologies for analytical decision support, real-time situational awareness and control, secure computing and communications (anti-terrorism and anti-fraud applications)
	2000-2009	More than ten US acquisitions in IT, defence electronics and land armament sectors	

Source: Masson and Marta (2011: 122)

In addition to this table, recent noticeable acquisitions in 2010 include French defence and aerospace group Safran's purchase of L-1 Identity Solutions biometric, identity and recruitment operations for around €1 billion, which will make Safran the world's biggest biometric identification company. BAE also strengthened its profile in the security sector in 2010 with the acquisition of L-1 Intelligence Services group and OASYS Technology which makes components for surveillance and reconnaissance. More recently, acquisition activity seems to have slowed.

However, despite seeming similarities there are major differences between the firms. Thales already had a security division which it has since consolidated with additional acquisitions. It concentrates on surveillance, identity, intelligence and critical infrastructure protection technologies, and therefore was in a strong position to challenge for contracts. It is pursuing a dual-use technology strategy. IRIS et al (2010) suggest that unlike its competitors, security is a key part of its business, with the division accounting for 25% of revenue in 2008. Thales therefore is perhaps an outlier among the European defence systems integrators. The French firm Safran is also of interest although a sub-system supplier. It has a strong presence in both the security and defence markets, but has tried to separate its security activities from its defence work to pursue a targeted growth strategy, therefore differing from its competitors. It owns Morpho, formerly known as Sagem Sécurité, which is a world leader in biometric technologies. As IRIS et al (2010) reported press speculation in 2009-10 was that an asset swap between Thales and Safran was being negotiated to exchange security and defence assets, so that Thales would concentrate on defence, Safran on security, thus reducing duplication of research. These talks collapsed in 2010 and despite French government pressure a further round of talks over swaps on avionics and optronics failed in November 2011 due to union pressure over jobs.[I]

EADS has an integrated defence and security division (Cassidian) but as yet very little revenue comes from non-defence contracts, and its core business remains its traditional civilian and military portfolios. It is however, attempting to develop its integrated communications technologies into the security market, particularly outside the EU, but for the moment militaries remain the key customers. Cassidian has identified law enforcement, cyber security and surveillance drones as potential growth areas (IISS, 2012). It has been involved in the security research programme so that it remains well-positioned if EU demand became stronger for security products (IRIS et al, 2010). EADS' most prominent acquisitions in 2011 though were Vector Airspace and Satair, both of which will strengthen EADS' support and services division – an area that the firm regards as both profitable and countercyclical. Finmeccanica has also tried to leverage its defence technologies into the security sector. It has been challenged by slow demand in both defence and security in its Italian home base, and was over-optimistic about the development of consolidated demand in the

[I] http://www.reuters.com/article/2011/12/13/thales-safran-idUSWEA540420111213

EU, and thus its security work has been predominantly non-EU export driven. Although on paper it has an impressive security portfolio, IRIS et al (2010) suggested that outside its export contracts, the security part of the overall business is small. Finmeccanica has been keenly involved in EU activities in the security industrial sector, particularly the security research programme. BAE, in comparison, has not been active at the EU level, but has concentrated its efforts in securing security work in its home UK and US markets, where it has concentrated on an area of strength, information-based intelligence systems. Its activities however remain predominantly defence-based. For EADS and BAE continuing strength in their classic markets means that the security market is currently of interest but not of overriding significance.

In the second and third tiers of defence producers the picture is also often blurred. For some sectors particularly IT and defence electronics, it has been comparatively straightforward for firms to offer substantially the same product to both security and defence customers, assisted by some acquisitions of smaller firms. A notable success in this category for example, is Smiths Detection, part of Smiths Group, which specialises in threat detection and screening technologies. For others, for example missile manufacturers, there is little attraction in the new security market, or like the German firm Diehl (which recently chose to acquire capacities in civil aerospace services) alternative diversification strategies look more interesting. For the third tier of suppliers, the blurring is again highly dependent on product but few would ever have been entirely defence-dependent anyway.

As an interviewee from the European Defence Agency pointed out in January 2012, if consolidated customers emerged in the security sector in a framework that was similar to the defence customer then established defence firms would be in a strong position. They are strong in terms of managing governmental relations, are good at succeeding with tendering processes and have relevant technologies in many cases. However, success is not guaranteed. An early success for the defence sector was the selection of Raytheon as prime contractor in 2007 for the British E-Borders programme, an advanced border control and security programme. The contract was terminated in 2010 over claims by the UK government of missed deadlines and substandard work. Raytheon is now suing the UK government (Curtis, 2011). Defence firms are also particularly concerned about embarking on major contracts without agreements in place on liability if their systems fail.

3.4.2 Non-Defence Firms and their Approaches to the Security Sector

Ecorys et al (2009) identified three main types of non-defence supplier in the security market: the traditional security industry supplying general security applications e.g. protective clothing, access control, fire detection, CCTV and, new entrants either from other civilian industrial sectors spinning in their technologies for security use (particularly ICT and telecommunications) or high-tech innovative start-up companies. However, within the high-end of the 'new security' market, as fostered in the EU Security Research programme, Ecorys et al (2009) found a fairly limited involvement of the traditional security firms, except in some surveillance technological areas. The relative absence of traditional security providers is perhaps not surprising. Their market has been characterised by short or mid-range product life cycles, privately funded R&D, a highly fragmented demand side and low, mainly production costs to participate. The new segment looks likely to be very different. ECORYS et al (2009) pointed to the nature of the demand side in this high-end market as being characterised by a limited number of customers (predominantly national governments, as they are the only legitimate users of the products), with highly specific demands, which combine to produce a corresponding concentration in the supply of security equipment.

They also argued that at the high-end of the new security market there are significant barriers to entry relating to

- High investment costs relating to technological development and then the transition to the market (this is similar to the worries of defence firms albeit that they are accustomed to a very different model of R&D funding than either type of non-defence firm).
- High costs in securing markets (lobbying, marketing and government relations) – ECORYS et al (2009: iv) suggest that this is related to 'the need to 'educate' clients on technological possibilities and choices as opposed to selling 'off-the-shelf' technology predominantly to non-government clients that such businesses are more accustomed to doing.

This means that SMEs struggle for market share within the sector despite being present within the sector in quite high numbers,[I] and so when SMEs do develop technologies, they tend to either be acquired by the large equipment integrators or licence them to develop the technology. In other words the non-defence firms have very similar problems to the defence firms but coming from the opposite end of the business spectrum. This is not to say that non-defence firms will always be at a disadvantage in the new market segment. IRIS et al (2010) cite the case of a British contract, for a national radio for first responders, which was won by the O2 Airwave consortium led by telecommunications firm BT over a bid by a consortium led by defence firm EADS. However, ECORYS et al (2009) noted that firms originating in the civilian market were only major players in very few sectors e.g. Motorola in secure communications.

Most of the studies looking at the sector therefore concentrate on the role of defence firms, partly because the more developed US security market is dominated by defence firms and partly because of the way that the policy area has been framed within EU politics (this will be covered in greater depth in part 4). It is arguable that non-defence firms have been excluded more than they should have been from the agenda-setting phase of the EU's growing involvement in the security sector. Bigo and Jeandesboz (2010) conclude for example that *"major defense and security companies have played a key role in the definition of the orientation and priorities of the EU's research and development policy for security-related technical systems."* However, this is not to deny that non-defence firms will have to accustom themselves to a very different way of working if, as the European Commission hopes, consolidated governmental customers emerge. This has not proven straightforward in some cases when a non-defence firm has entered the defence market. The selection of Airbus's newly created subsidiary, Airbus Military Company, to build the A400M transporter aircraft was intended to draw on Airbus's commercial experience in building civilian aircraft to bring rigour to the procurement. The problem was that Airbus had no experience in building military aircraft, was heavily distracted by problems with its key civilian aircraft project and had completely underestimated the risks inherent in the project (Masseret and Gauthier, 2009: 46-8). For the moment at least though, it seems that non-defence firms are at a disadvantage outside of certain ICT and communications sectors.

3.4.3 Emerging Trends?

The general sense of the current security market is that the major defence firms have positioned themselves, some more wholeheartedly than others, but are waiting for the emergence of a

[I] According to Masson and Marta (2011) SME start-up innovators, developers and providers of new security technologies, are according to the European Security Directory 2009 are very active in the security field. They suggest around 668 SMEs are involved in one way or another through EU policy actions, trade associations and registration in the directory. In a case study of the Netherlands, Akkermann (2012) also reports high levels of interest among smaller Dutch firms.

consolidated demand side in the EU. At present however, there has been relatively little governmental demand and what there was has slowed down. Masson and Marta (2011) argue that a) existing security contracts are small compared to defence ones; b) most existing large contracts are ending and new ones are not being launched (some large contracts have proved highly controversial politically too notably in the UK with identity cards and e-borders); and c) they are often linked to specific events like the London 2012 Olympics or are reactive following a natural disaster. The highly public failure of G4S to deliver on its contract to provide security for the London 2012 Olympics has also cast doubt on whether the state should outsource security functions to the private sector. The security sector at present therefore, with the exception of those who had been particularly well placed to take advantage of surveillance, screening and identity technology demands, is not a major source of income. Some large defence firms therefore are continuing to concentrate on defence activities, while others have turned to non-EU exports as a stopgap. The decisions made vary but are also affected by the health or otherwise of defence spending in their home markets.

Non-security firms seem less well-placed outside of communications and ICT field. This is in part due to particular EU policy decisions and partly because of the large number of SMEs, which will find the market conditions challenging. Another development that may favour defence firms is that the European Commission has used the security research programme to engage in cooperation with the European Defence Agency. Two projects in particular are seen as success stories by the EDA and the Commission.

- Software Defined Radio which has applications both for military use and use by first responders (police, fire service and so forth).
- a project on the insertion of Unmanned Aerial Vehicles into civil airspace. (James, 2009a)

This ad hoc cooperation led to the May 2009 decision by the European Defence Ministers to task the European Defence Agency to establish a European Framework Cooperation for Security and Defence together with the European Commission with the aim of *"maximising complementarity and synergy between defence and civil security-related research activities"*. The EDA has identified situational awareness (sensor technologies, command and control of networked assets) as an area for cooperation (James, 2009a). Discussions are also underway about the possibility of including defence research in the 8th Framework Programme. All of these developments look likely to intensify the patterns of provision emerging in the new security market, where defence firms are well-placed in most but not all security sectors but not guaranteed success unless consolidated demand emerges. If demand remains fragmented, non-defence firms and even SMEs may well find themselves better placed.

3.5 Demand Side

As has already been discussed in the previous sections, the nature of the demand side in the traditional security, new security and defence sectors are very important in determining the make-up of the supply side and how research and development in the new market segment might be funded. The demand side in Europe is invariably criticised for its fragmentation. Is this a fair criticism and would the replication of the military or defence customer be a positive or negative outcome in the new security sector? This section will briefly outline the main user groups of security and defence products, question the extent to which roles and requirements have been blurred in contemporary security policy and then discuss the ways in which the civilian and military

government customer vary in terms of regulatory culture, procurement practice and requirement needs.

3.5.1 Key User Groups of and Requirements for Defence and Security Technologies: Blurred or Distinctive?

Claims that there has been a blurring of defence and security or more pertinently internal and external security for the users of these technologies tend to start from the premise that their missions have become intertwined. As IRIS et al (2010) point out where military missions are concerned, contemporary crisis management operations are often not purely military. In particular, when the intervention lasts into the post-conflict stage, civilian or NGO missions are often set up to help restore policing, administrative and rule-of-law functions as well as assisting with humanitarian and security sector reform tasks. Similarly military personnel may find themselves assisting with various internal security missions such as counter-terrorism operations, support for civil protection, critical infrastructure protection and border security.[I] The roles that the armed forces may or may not play in these types of missions is often defined in national constitutions, so does vary between the EU states, but it is indubitable that there are fuzzy boundaries between military and civilian functions; this is even more the case in states with paramilitary forces such as gendarmeries.

The crossover though goes beyond 'mission creep' – clearly if military and civilian forces are to cooperate on joint operations then a degree of interoperability is required, be that in terms of training, communications equipment or integrated command structures. There is however, for the purposes of this study, perhaps a more interesting dimension of this crossover where civilian and military personnel might find themselves using similar technologies to carry out similar tasks but in very different environments. For example, unmanned aerial vehicles (UAVs) have been used to great effect in military operations, notably in carrying out targeted killings in Afghanistan and Pakistan, but are also considered to be potentially useful (unarmed) for carrying out policing activities such as observing football supporters. Another example might be the use of Trojans and other malware: while most famously Stuxnet was used to hinder the Iranian nuclear programme, the German police have also been discovered planting malware on their own citizens' computers to spy on them.[II] IRIS et al (2010) concluded that there was functional blurring of this nature in the following areas:

- detection, identification and authentication
- situation awareness and surveillance
- risk assessment and modelling
- communication
- information management
- positioning and localisation

Given that for example, difficulties in communications between first responders to the 7/7 London bombings were criticised, why has this level of commonality not led to more joint procurement? Why does the demand side remain so fragmented?

[I] The British military even had to step in to provide security for the London 2012 Olympics after private security firm G4S failed to train enough security staff.

[II] This was reported widely on the internet. A reliable account can be found here on the New Scientist blog: http://www.newscientist.com/blogs/onepercent/2011/10/german-hackers-find-possible-g.html

3.5.2 Civilian and Military Customers: Irreconcilable Differences in Procurement and Requirement Definition Practice?

Firstly, it is important to stress that while (despite inter-service rivalries) there is one military customer in the shape of each state's Ministry of Defence, internal security users are much more varied. To start with they are not all at the national level: security functions are often devolved down to regional and local operators often with a high degree of autonomy and devolved budgets. Moreover, security customers, although they are not the focus of this report are not all governmental. Corporate and private customers range from large infrastructure operators (like energy suppliers, airport operators) to small domestic customers. Some of these private customers will need to be involved in public disaster planning because they control critical infrastructures. This inevitably means that joined-up procurement, even before military customers are involved, is extremely complex. Moreover, differences between the ways in which EU states organise internal security mean that cross-border procurement is even more complex. It is not surprising that both IRIS et al (2010) and Masson and Marta (2011) identify relatively few examples of this happening even in single states. Two widely cited British examples of joined up procurement, the border security e-Borders initiative and the 'Fire Control' project to concentrate fire service infrastructure in nine regional centres, have both collapsed in failure.

Perhaps more importantly though there are crucial regulatory differences and varying levels of requirements between civilian and military customers even when they are procuring similar products. The military or defence customers and the businesses that supply them operate in a highly unusual environment. Briani and Sartori (2011) summarise these conditions as follows:

- Monopsony structure on the demand-side
- Monopoly/oligopoly structures on the supply-side
- High R&D intensity and long-term production cycles
- Decreasing production costs
- Public subsidies in the R&D phase
- Associated spin-offs

Perhaps most importantly, within the EU context, is the existence of article 346 of the Lisbon Treaty, which, notwithstanding the 2009 'defence package' of the directives on intra-EU transfers of defence and defence and security procurement, still largely protects defence equipment procurement from single market legislation.[I] This permits a degree of protectionism and subsidy that would not otherwise be permitted under competition legislation. As has already been discussed this is such a particular environment, that it is difficult for those used to working within such structures to adapt to more normal business environments and vice versa. Moreover, as interviewees at the European Defence Agency pointed out in 2012, military users do tend to require much more customised and higher-end equipment than other users, even if the equipment is similar, making joint requirement definition complicated.

Given the 2009 procurement directive also covers security procurement, would it make sense for internal security customers to adopt military procurement behaviour insofar as it is legally permitted because like defence technology, this new type of security technology requires special treatment? This after all seems to be the assumption underlying much of the EU activity in this field, for example the commitment to explore limiting firms' liability (European Commission, 2012a). It is though a rather problematic assumption. The report has already discussed the

[I] See Eguren Secades (2011) for a full discussion of the limitations of these directives.

complexity in joined up procurement for internal security users in a single state, but even if this was to be overcome, would a security technology market be more efficient than the existing defence one? It seems unlikely that internal security customers would be prepared to accept the extraordinarily lengthy time from requirement definition to in-service that defence customers are resigned to, particularly if the necessary equipment is available to an acceptable degree off-the-shelf. Similarly, the expense of this model of defence procurement is increasingly decried as unaffordable. Perhaps this lies behind the reluctance of national users to launch the type of coordinated and consolidated demand for security technologies that had been anticipated in 2003 by both the European Commission and GoP report.

3.6 Summary

This section began by discussing the methodological problems of quantitatively defining what a variety of studies had observed to be a new security market segment, closely related to the development of the concept of homeland security as outlined in section 2, but with a close relationship to the defence sector. A working definition of this industrial segment was proposed as firms from a variety of industrial backgrounds offering technological products to governmental customers in response to security concerns. It did not therefore seek to exclude defence firms from the analysis, or to limit security concerns to specific issues, but did limit the products considered to technology-orientated ones and omitted the corporate and private security customer in favour of governmental actors.

The second sub-section looked at the crossover between security and defence technologies. It began by pointing out that trends in defence research and development were likely to be similarly valid in another high tech sector with a government customer, namely that R&D was likely to be concentrated in relatively few states and that EU efforts to foster collaborative R&D to make up for this, were likely to struggle. The discussion moved on to look at the taxonomies developed to classify technologies and their associated equipment. It acknowledged the large degree of crossover between defence and security technologies with some caveats, but argued that the most important issue for the purposes of this study was their joint reliance on generic technologies, which made non-proliferation and export controls more difficult, and raised questions about issues like security of supply for the EU.

The section moved on to consider the supply side. It concluded that defence firms enjoyed certain advantages in accessing the new market sector but that their success could not be guaranteed. The lack of government demand meant that the major systems integrators had developed different strategies, from developing security exports to concentrating on their defence portfolios. They had all positioned themselves to some extent to be able to enter an EU market if demand improved. Second tier suppliers had clearer cut decisions to make, depending on the usefulness or otherwise of their technologies to the new market, whereas for third tier suppliers, while their products could well be relevant, their business was rarely in any case entirely defence dependent. Non-defence firms, except in the areas of secure communications and ICT, were struggling. This was mainly because traditional security suppliers and SMEs were disadvantaged in dealing with government customers, but lack of demand made it difficult to draw lasting conclusions.

Finally, the section discussed the difficulties of the fragmented demand side. While it was accepted that military and civilian security users cooperated on an increasing range of missions, and moreover, used very similar technologies albeit for different purposes, the sub-section argued that

it was not that simple to consolidate demand. Firstly, the complexity of bringing together a diverse selection of internal security users from both public and private sectors, and national, regional and local levels of government was discussed. Secondly, the specificities of the defence procurement environment were outlined, and the different regulatory frameworks for military and civilian procurement discussed. Finally, the question was asked whether consolidating demand was actually an attractive prospect for civilian users, if it meant adopting military customs.

To conclude, although there are undeniably commonalities in terms of user requirements and technologies, substantial difficulties remain in consolidating the fragmented demand side. This means that while defence firms are well-placed to be involved in the security sector if this demand emerges, it may not offer a sufficiently inviting prospect. The question is to what extent member states in fact share the EU's vision of the importance of this sector? The way in which EU activity evolved will shed light on why there is perhaps a mismatch between Commission objectives and those of the member states.

4 Evaluation of EU Policies effecting the Security and Defence Industries

4.1 Introduction

The European Union is a comparative newcomer to the fields of security and defence. Until the advent of the European and now Common Security and Defence Policy and the broadening of internal security activity post 9/11, its involvement was limited. The European Commission has though long aspired to play a role in defence industrial policy regulation. It tried to gain influence via Single Market legislation, competition policy and regional policy. Its success however was decidedly limited and was confined to:

- the administration of the Framework programmes for research and development, some of whose projects were dual-use,
- approving major corporate mergers even if a defence dimension existed,
- allocating regional development funds to areas affected by closing defence bases or failing firms (KONVER), and
- in 1995 setting up a regime for the trade of dual-use goods within the EU (Taylor, 1997).

The Council, prior to the establishment of the ESDP, had two working groups connected with armaments. The first was COARM, established in 1991, which attempted to harmonise export controls policies with respect to third countries. The second was POLARM, set up in 1995, which was an ad hoc working group on armaments policy (Colvin, 1998). The European Parliament was not involved. Historically, therefore European cooperation on issues connected to defence and security industry has taken place outside the EU, in NATO, the Western European Union or in other multi- and bilateral fora.

This section of the report aims to critically assess EU policies to strengthen the competitiveness of European security and defence industries looking at their coherence and effectiveness. Given that EU powers in this area are relatively new, the section first outlines the legal basis for EU action. It then looks at Commission policy, considering the security research programme, sectoral competitiveness action, the defence package of directives and finally, the involvement of DG-Home Affairs in developing homeland security type policies. It then moves on to look at the European Defence Agency. The final substantive sub-section will consider related European activity outside the EU, namely, the Franco-British defence agreements, OCCAR, the Framework Agreement and NATO, and seek to evaluate what if any impact they have on EU policy success.

4.2 Legislative basis for EU action in the area of security and defence

The legislative basis for EU actions in the areas of security and defence is quite complex and so is worthy of attention. This sub-section of the report will briefly outline the essence of the treaty basis for action on security and defence industries and technologies, through both the Common Security and Defence Policy and internal security clauses, and explain the significance of Article 346 of the Treaty on the Functioning of the European Union (formerly Article 296) as a restriction on EU activity. It will also outline several key European Court of Justice rulings on the use of Article 346.

4.2.1 Treaty basis and limitations

The treaty basis for the Common Security and Defence Policy stems from Title V of the Treaty on European Union (TEU)[I] on the "General Provisions on the Union's External Action and Specific Provisions on the Common Foreign and Security Policy (CFSP)", and more specifically Section 2, articles 42 to 46, entitled "Provisions on the Common Security and Defence Policy (CSDP)", as well as protocols 10 (on permanent structured cooperation in defence), 11 (on the WEU) and declarations 13 and 14 (which both stress that CSDP should not prejudice the specific character of the security and defence policies of the member states; 14 additionally states that no new powers are given to the Commission or Parliament). Of particular interest for this report, the provisions on the European Defence Agency say it will oversee the capability definition and development process, including having the aim to *"strengthen the industrial base of the defence sector" and participate "in defining a European capabilities and armaments policy"* (articles 42.3 and 45 TEU).

There is however an important limitation to what the EDA or any EU institution can do to regulate the market in defence equipment, namely article 346 (1) of the Treaty on the Functioning of the European Union, which reads,

"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."

This has been understood liberally as a "general and automatic exemption of hard defence material from the application of the treaty" (Trybus, 2000: 665) in part enabled by the secrecy surrounding a list of the products this exemption was meant to cover, which was compiled in 1958 and updated in 1978.[II] Successive European Court of Justice judgments and a 2008 Commission directive have clarified the situation. These will be discussed in depth later.

[I] The Treaty on European Union is available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF

[II] The article 346 list can now be viewed at http://register.consilium.europa.eu/pdf/en/08/st14/st14538-re04.en08.pdf.

The basis for action on internal security policy stems from the revised Treaty of Rome, now known as the Treaty on the Functioning of the European Union (TFEU)[I], Title V 'Area of freedom, security and justice' (AFSJ). The amendments agreed under the Lisbon Treaty bring the AFSJ into the main body of the treaty and hence under normal community judicial controls. Lawyers, who have been critical of the rapid expansion of the policy area since 9/11, on the grounds that some moves have major implications for civil rights, which they feel have not been taken into account enough, have welcomed this, as the ability to take such measures to the ECJ where they seem to contravene the now legally binding Charter of Rights, will prove a check (Craig, 2010). It is also worth noting that article 4 (2) of the TEU states specifically that *"national security remains the sole responsibility of each Member State"* and that the TFEU refers to internal security instead. This differentiation, viewed as important by some member states, was clarified during the negotiations of the Lisbon Treaty. Article 71 of TFEU states that a *"standing committee shall be set up within the Council in order to ensure that operational cooperation on internal security is promoted and strengthened within the Union."* This committee is known as COSI. Article 72 TFEU however reads *"This Title (Title V) shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."*

4.2.2 ECJ judgments

The European Court of Justice has been asked to rule on a large range of cases[II] where the defendant invoked Article 346 in their defence. The key judgments are briefly discussed below. While this is over-simplistic, the basic position of the Commission has been that derogations under Article 346 should be subject to a test of proportionality like any other derogation, whereas the member states have seen Article 346 as providing an automatic derogation. The position of the ECJ has been in general somewhere between these stances. Firstly, the Court has ruled in a number of cases that member states may use Article 346 to protect their sovereignty. In case C-252/01 relating to a contract for Belgian coastal aerial photography, for example, the ECJ accepted the Belgian argument that the contract required special security measures, without requiring a high standard of scrutiny of whether security measures were needed. Similarly in case T-26/01 regarding Fiocchi Munizioni, it was accepted that member states do have discretion in deciding how to protect their interests and what measures to use.

However, the ECJ has consistently ruled that exemptions under Article 346 are limited. On Case 367/89 Richardt for example it ruled that the derogation must be interpreted strictly and that only products actually listed in the 1958 list were exempt. Moreover in the Augusta Helicopters (Case 337/05) ruling, it was clarified that article 346 only applied to equipment intended specifically for military use, so dual-use or equipment supplied to militaries for civilian use were not exempt. The ECJ has also ruled that there is no automatic exemption; article 346 only applies if the conditions are met (Case 273/97 Sirdar) and that it may only be invoked for reasons of security not economic reasons (Case 414-97 Spanish weapons). The 2009 rulings on the so-called 'own resources' cases (C284/05 and others) whereby member states tried to invoke article 346 as the rationale for their failure to disclose VAT revenue from arms imports to the Commission, also stressed that there was no automatic exemption. These rulings on Article 346 have informed the Commission's action in the area of defence and security in recent years, and have strengthened their position.

[I] The Treaty on the Functioning of the EU is available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF

[II] The judgments mentioned can be found at http://curia.europa.eu/en/content/juris/c2_juris.htm.

4.3 European Commission Policy

The European Commission's actions aimed at strengthening the competitiveness of security and defence industry are not based solely in one Directorate General, although DG Enterprise and Industry has specialist units for both security and defence industry. Work carried out by several DGs needs to be considered here, namely, DG-Enterprise and Industry (security research and sectoral competitiveness), DG-Internal Market and Services (defence package) and DG-Home Affairs (homeland security). DG-Information Society and Media has also some involvement through interests in cyber-security but its work is less relevant for the purposes of this report. Finally, DG-Trade is responsible for the dual-use export legislation. The involvement of so many DGs reflects the need for the Commission to agree a common position on a topic with many facets. In recent years, the Commission has seemed to be more joined up in its approach to policy-making in this area. Earlier attempts in the 1990s to gain competence are thought to have failed because tensions between commissioners on whether it should be framed as an industrial policy or a single market competition issue, made it easier for the member states, who did not want Commission involvement to ignore the communiqués (Mörth, 2000).

The Commission was aided though by two developments in the late 1990s and early 2000s. Firstly, the Prodi Commission included Commissioners Liikanen and Busquin, who were firmly convinced of the importance of the defence industry for Europe's economic future and acted as policy entrepreneurs. The idea that Europe could solve its high technology problems by strengthening its defence industry seems to have been embedded in Commission thinking from this point onwards (Merritt, 2004: 216). This approach strengthened the support of industry for Commission involvement. Two important 2002 reports (STAR21 and ACARE) by lobby groups for aerospace and aeronautics made their case that technological innovation in the defence and aerospace fields was key to wider economic success for the EU. Secondly, the decision to create the ESDP quickly drew attention to equipment and technology gaps and refocused political attention on the transatlantic gap. The crystallisation of the Commission's thinking can be dated to 11 March 2003, when they released a communiqué about the industrial and market issues of European defence. The Commission proposed action in seven areas; standardisation, monitoring of defence-related industries, intra-community transfers, competition, procurement rules, export control of dual-use goods and research (European Commission, 2003a). As we will see the 2003 European Council decision to establish the European Defence Agency curtailed the Commission's freedom of movement in proposing legislation but it is nevertheless clear that they have gained power since then. The announcement on 7 November 2011 by Michel Barnier, the Single Market commissioner, that the Commission had decided to launch a defence policy taskforce, which is likely to include the Internal Market, Research and Development, Industry, Transport, Energy and Legal Services Commissioners plus the EDA and European External Action Service, shows continued ambition.

4.3.1 The genesis and evolution of the security research programme

Parts of the European Commission's DG-Research have long sought to fund defence-related research, but many member states, European parliamentarians and indeed some Commission officials have always opposed this on two grounds: a) defence remained a national prerogative and b) that the EU was a civilian not a military power and that it would therefore be inappropriate. However, while the Framework Research Programmes[l] have never formally been allowed to fund

[l] The EU Research Framework Programmes are the main vehicle through which the EU funds research. The programmes started in 1984. They are multiannual programmes (the first six lasted five years each, the current Seventh Framework Programme

defence-related research, increasingly over the years, dual-use research has been funded.[I] In 2003-2004 though Commission supporters of defence-related research actively, notably Liikanen and Busquin, moved to make this a Commission task. Following a number of communiqués on cognate areas such as defence equipment (European Commission, 2003a) and aerospace industry (European Commission, 2003b), which claimed that the Commission should play a role in defence research. Under the heading "towards a more coherent European advanced security research effort", the Commission (2003a) for example called for increased coordination of security research. It said it would ask national administrations, the business community and research institutions their opinions on what a European agenda for research in this field should look like and would seek *"to launch a preparatory action to coordinate such research at the EU level, focusing on a limited number of concrete technologies linked to the Petersberg tasks"*. At this stage the thinking seemed relatively clear; the Commission was attempting to move into defence research funding as a way of supporting the defence firms it deemed technologically vital to economic competitiveness. One Commission official went on the record to say *"The EU's framework program supports dual-use research in all these areas, so it would make sense to bump things over into the purely military realm… The important thing is to set the precedent"* (Tigner, 2003a). In May 2003, meanwhile, another Commission official seemed to suggest that a major reorientation of the research budget was planned, saying that the development of a stronger European defence identity implied, *"a more flexible use of EU research money in favour of defence-orientated projects"*(Tigner, 2003b). However, the decision was taken by the European Council in summer 2003 to set up the European Defence Agency which inter alia would have responsibility for coordinating defence research. This made it very difficult for the Commission to openly try to fund defence research so instead it moved to security research. The Commission issued a communiqué in March 2004 on security research (European Commission, 2004) and a decision on implementing a preparatory action[II] and on 15 March 2004 the Group of Personalities for Security Research (GoP), set up by the Commission, presented its report to Romano Prodi (see Figure 1 on p44). Edler and James (2012) stress the entrepreneurial role of the Commission in making this move, pointing out that there was no initial demand for this action from either the member states or industry.

Subsequently, the Commission published the first call for proposals for projects and supporting activities under the new 'Preparatory Action on the enhancement of the European industrial potential in the field of Security Research' (PASR 2004) on 31 March 2004. This action spent 65 million euros over three years and served as a pilot phase for the Commission's broader agenda of establishing a separate security research programme to facilitate an EU security culture. The preparatory action was criticised for its lack of consultation with security users[III], failure to map

---

and its successors will last for seven years). Each Framework Programme has differed in the allocation of research priorities and how they should be funded. The current Framework Programme has four programmes: cooperation with ten research priorities (health; food, agriculture, fisheries and biotechnology; information and communication technologies; nanosciences, nanotechnologies, materials and new production technologies; energy; environment (including climate change); transport (including aeronautics); socio-economic sciences and the humanities; space; security), ideas (blue skies research funding allocated by the European Research Council, people (Marie Curie Actions enabling the mobility of researchers) and capacities (improving research and innovation capacity). Non-EU states can participate in the programme if they contribute to the budget. The following are associated with the current Framework Programme: Switzerland, Israel, Norway, Iceland, Liechtenstein, Turkey, Croatia, FYROM, Albania, Montenegro, Bosnia and Herzegovina, the Faroe Islands and Moldova.

[I] The security research priority as initially defined in the Commission's proposals was rather ambiguous about its nature. However, during the co-decision procedure on the Seventh Framework Programme, the UK, France and Germany together with the European Parliament insisted that the civilian nature of the framework programmes be preserved. Formally therefore, the Security Research theme has an exclusively civilian focus (see Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)).

[II] Decision 2004/213/EC

[III] It is worth pointing out that only Austria and Sweden of the member states had felt it necessary to set up a national security research programme at this point – this may well have led the GoP to significantly overestimate demand.

onto agreed anti-terrorism priorities, lack of clarity in its objectives and seemingly rushed implementation (Hayes, 2006; Mawdsley, 2004). The security research priority in the seventh framework programme itself funded projects in four main mission areas backed up by three cross-cutting themes:

Mission areas:

- "**Increasing the security of citizens** - technology solutions for civil protection, bio-security, protection against crime and terrorism;
- **Increasing the security of infrastructures and utilities** - examining and securing infrastructures in areas such as ICT, transport, energy and services in the financial and administrative domain;
- **Intelligent surveillance and border security** - technologies, equipment, tools and methods for protecting Europe's border controls such as land and coastal borders;
- **Restoring security and safety in case of crisis** - technologies and communication, coordination in support of civil, humanitarian and rescue tasks";

Cross-cutting themes:

- "**Improving security systems integration, interconnectivity and interoperability** - information gathering for civil security, protection of confidentiality and traceability of transactions;
- **Security and society** - socio-economic, political and cultural aspects of security, ethics and values, acceptance of security solutions, social environment and perceptions of security;
- **Security research coordination and structuring** - coordination between European and international security research efforts in the areas of civil, security and defence research."[I]

The research is mission-orientated and is largely development-orientated, rather than the type of "blue skies" research funded under the priorities managed by DG-Research. Some projects in fact seem to be more about procurement than research and development in so far that demonstrators have been produced (a late stage in the development of technology). It had an overall budget of €1.4 billion for the period 2007-13. The Commission hoped that the research priority would assist them in their wider aim of reducing fragmentation on both the supply and demand sides of the market, and becoming a market leader globally through EU standardisation exercises.[II] Throughout the preparatory stages and the early stages of the actual priority, the Commission carried out a process of public-private dialogue through advisory groups, which sat alongside the more usual comitology committees[III] for research programmes. These groups and their reports are briefly described in Figure 1 (p44). They are significant, and their composition matters, because the European Commission has largely adopted their recommendations in follow-up communiqués (European Commission, 2004a, 2009). Indeed this public-private dialogue appears to have largely determined funding priorities, although given the aims of security research, one might have expected this to be based on a scientifically rigorous risk assessment process.

The call in the Group of Personalities report to spend at least €1 billion of additional money annually on security research now seems wholly unrealistic. Interviews with industry

---

I The outline of the security research priority can be found at: http://cordis.europa.eu/fp7/cooperation/security_en.html (consulted on 7 March 2011).

II Interviews with Commission officials in April 2008.

III There is also an official Security Research Advisory Group (SecAG) of experts, nominated by the Commission to guide the Commission in planning future security research programmes. Out of twenty members, the composition is seven large defence firms, three security firms, EDA, four end-users (Poland, Malta, Romania and Estonia), three research institutes (Finland, Israel, Netherlands), Swedish defence research agency and the Austrian Red Cross.

representatives suggested that the belief that member states would be prepared to match US homeland security spending and that it would be orientated in certain directions, was grounded in part at least in a 'groupthink' situation, based on shared fears from the Commission and European defence firms that billions of dollars flowing into US defence firms for the foreseeable future would leave European firms in a hopeless situation. In reality this was a misunderstanding (shared then by US firms - Beidel, 2011) of how the US homeland security funding would actually be spent.

Firstly, homeland security in the US has been driven by events. Hurricane Katrina ensured that much of the early spending went to disaster response firms not defence firms. It was not until 2009 that large defence contractors like Lockheed started getting really large contracts (Beidel, 2011). Large amounts are also spent on the Department of Homeland Security itself, which has gone from 13 employees in 2002 to 60,000 in 2010. Secondly, it is now generally accepted that homeland security funding will not continue at the levels of the first decade given the US fiscal crisis. Beidel (2011) also argues that predictions that the security market would rival the defence one are *"unlikely now, in part because of growing fiscal constraints and because the two markets are driven by different factors"*. A combination of the realisation that mass surveillance and detection programmes have been very costly in terms of budgets and to business while providing little added security,[I] coupled with growing citizen resistance to intrusive security measures, has led to the cancellation of programmes such as the Advanced Spectographic Portal programme aimed at detecting smuggled nuclear material and SBI-net, a border control 'virtual fence'. Moreover, Beidel (2011) suggests that with the exception cyber security, future US focuses will be on the integration of existing proven technology rather than the funding of new research. Hayes and Vermeulen (2012) argue that the European Commission is also failing to learn the lessons offered by the US experience in pressing ahead with funding for border surveillance projects, which closely resemble those that have failed at great expense in the US like the SBI-net.

In addition to its own projects the security research programme has led to inter-institutional cooperation between the Commission and the EDA. Two projects in particular are seen as success stories by the EDA and the Commission.

- Software Defined Radio which has applications both for military use and use by first responders (police, fire service and so forth).
- a project on the insertion of Unmanned Aerial Vehicles into civil airspace (James, 2009a).

This ad hoc cooperation led to the May 2009 decision by the European Defence Ministers to task the European Defence Agency to establish a European Framework Cooperation for Security and Defence together with the European Commission with the aim of "maximising complementarity and synergy between defence and civil security-related research activities".[II] The EDA has identified situational awareness (sensor technologies, command and control of networked assets) as an area for cooperation (James, 2009a). Interviews in January 2012 with both EDA and Commission officials suggested that both parties saw this cooperation as positive. For EDA in particular, it was seen as a way of gaining access to additional funding.

[I] Mueller and Stewart (2012: 107) calculate that for US homeland security spending to have been cost-effective, it would have had to "deter, prevent, foil, or protect against 333 very large attacks that would otherwise have been successful every year. That would be about one a day." The article claims that between 2001 and 2012 there were only 50 cases of Islamic extremist terrorism, most of which were small-scale.

[II] Council of the European Union, 2943rd External Relations Council meeting, Conclusion on European Security and Defence Policy (ESDP), Brussels, 18 May 2009

Figure 1: Security Research Advisory Groups and their Reports

Group of Personalities Report 2004

Members - 27 members primarily from defence industrial or military backgrounds. Low representations of users.

Key Recommendations

- Commission security research programme should be established
- 1 billion euro per year should be spent on security research by the Commission in addition to existing spending
- Programme should fund capability-related research projects up to the level of demonstrators
- There should be no division between civilian and military security research – synergies should be encouraged
- Programme should foster industrial competitiveness & stimulate market development

European Security Research Advisory Board Meeting the Challenge Report 2006

Members - 50 members - mixture of government users (18), industry representatives (14) and some security experts - more defence-focused than might have been expected.

Key Recommendations

- Multidisciplinary, mission-oriented research on security should be undertaken covering capability development, system development and system-of-systems demonstration
- Five demonstration programmes were recommended: aftermath crisis management; European-wide integrated border control; logistic and supply chain security; security of mass transportation; and CBRNE threats
- Societal concerns about privacy and ethics should not be ignored in the effort to improve security
- Security research system should be established using *"innovative pre-commercial public procurement, the use of large-scale demonstration programmes, greater SME engagement and the definition and use of European standards"*

European Security Research and Innovation Forum (ESRIF) Final Report 2009

Members - 65 plenary members - all stakeholders represented including EU institutions. Additional members (c.600) mainly industrial figures took part in working groups. Little civil society representation.

Key Recommendations

- The human and societal aspects of security must be at the heart of security research and ethical and legal dimensions must be a part of security solutions.

- Industrial policy – overcome market fragmentation & strengthen security industrial base to become a leader in global security market
- European Security Research and Innovation Agenda – 5 clusters

  - classic security cycle of preventing, protecting, preparing, responding and recovering;
  - countering of different means of attack;
  - securing critical assets/infrastructures;
  - securing identity, access and movement of people and goods;
  - cross-cutting enablers, in particular Information and Communication Technologies.

- Need to consider in addition the external dimension of security in future
- Continued public-private dialogue, coordinated trans-European cooperation and establishment of an Internal Security Fund

Has the security research programme been a success? To answer this question, it is necessary to evaluate it from the Commission perspective, that of industry and that of Commission critics. Firstly, from the side of the Commission the security research programme has to be regarded at least as a partial success. It was popular. Interviews with DG Enterprise and Industry officials and industry representatives in January 2012 confirmed that the programme had been substantially over-subscribed. Moreover, the fact that security research will continue into the Eighth Framework Programme called Horizon 2020, under the heading 'Inclusive, Innovative, and Secure Societies' is indicative of a level of success, although the budget at this point is unclear. There have even been discussions about the possibility of funding defence research through the Framework Programmes.[1] The Commission was less successful in its market shaping aims though, especially on the demand side, as discussed earlier in section 3.

From an industry perspective, interviews carried out in January 2012 had some interesting findings. For industry, the lack of subsequent demand from users was a major problem, as it made little sense to share technologies (or useful contacts to act as the user representative on the project) with project partners in the security research programme, if there was no contract at the end. This was a particular problem for firms based in countries where there was little research funding available but also no procurement, as they could apply for EU funding for the research stage but then there were no obvious continuation routes, as it was difficult to export with no existing customers, raising the question of research and development being wasted. The Commission, not being a customer, is limited in its ability to respond to this. It was also suggested that the need to put together bids that had geographical balance and SME representation, meant that suboptimal partners were being chosen.

The Commission's critics are harsher. For Hayes (2006; 2009; 2010) the security research programme represents a triumph for the lobbying of defence firms, who he claims were over-represented in all of the advisory groups at the expense of genuine civil society voices. Jeandesboz and Ragazzo (2010) agree the public-private dialogue within the advisory groups was closed and

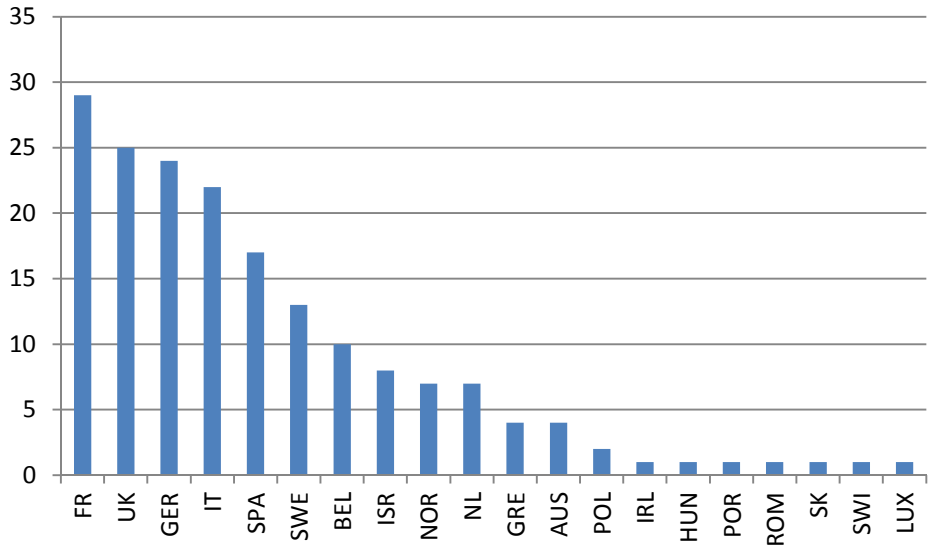
[1] It was proposed that defence research should be funded in the Horizon 2020 programme (the successor to the Seventh Framework Programme) but there was opposition within DG-Research and from member states. Edler and James (2012) suggest that this reverse suggests that there are limits to the Commission's ability to move into this policy area. It is also not really clear that funding for defence research would add value. It is unlikely that sufficient funding would be allocated to make a difference, and the problem that the EDA has faced in not being able to assure procurement of the research it has funded, would also apply to the Commission. It would seem that EU research funding could be used more effectively in other areas.

limited, but have also collected an array of interesting data to support their further criticisms that the programme was geographically biased, was dominated by big defence firms and concentrated on controversial surveillance technologies. They claimed that the beneficiaries were disproportionately based in six countries (UK, France, Germany, Italy, Sweden and Israel). Jeandesboz and Ragazzo (2010) also claimed that big defence firms are the overwhelming beneficiaries of the security research programme, and equate this with their over-representation on advisory groups. Their final claim is that the programme was too heavily focused on surveillance technologies, some of which are highly controversial in terms of civil liberties and privacy. They pointed out that projects for surveillance and detection up until May 2009 had taken up 40.1% of the budget, compared to the 1.09% spent on two projects reflecting on ethical and legal dimensions. They based their claims on an analysis of projects awarded prior to May 2009. This study has created a database of projects awarded up until July 2012 to re-examine the claims with more data. The data was taken from the CORDIS website.[I]

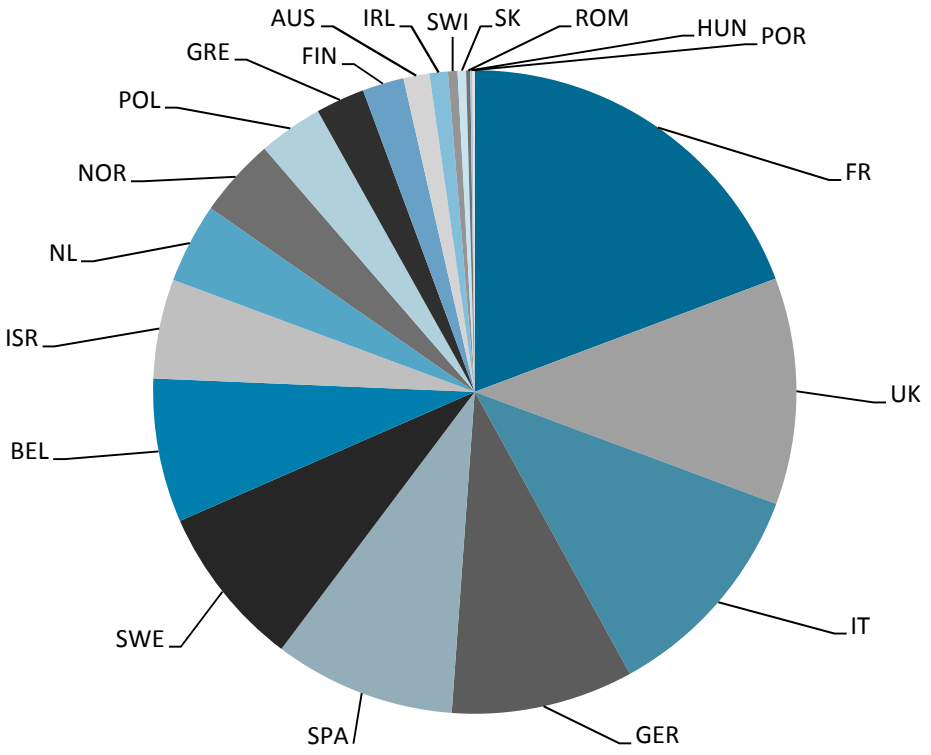
After analysing the total number of projects coordinated by each state and their value (shown in graphs 1 and 2 below), it is clear that there is a concentration. The top six states by July 2012 in terms on number and value of projects funded were France, UK, Germany, Italy, Spain and Sweden. The French have been the most successful coordinating over 19% of the funds awarded thus far. Belgium has also done well, although it should be noted that numerically half of the projects coordinated are being coordinated by European-level organisations based in Brussels like the European Organisation for Security. Israel and Norway (non-EU states may participate in the Framework Programmes if they contribute to the budget) have performed strongly too. As might have been expected, there is a correlation between defence industrial strength and above average coordination rates. The top six are the six members of the Letter of Intent group. This suggests that the concern raised in section 3 about a potential geographical concentration in security research mapping onto the concentration in defence research has validity. The picture of overall participation may be more complex but as the amount awarded to each partner in projects is not given, more in depth analysis was not possible for this report. Given the concerns raised by interviewees from industry that Commission efforts to achieve a better geographical spread were forcing them to choose non-optimal partners, such analysis might also prove misleading about the whereabouts of security research expertise.

[I] CORDIS list of projects funded under the security research priority: http://cordis.europa.eu/fp7/security/projects_en.html

Graph 1: Number of Projects in the Security Priority of the 7th Framework Programme Funded as Project Coordinator by Participating State (up to July 2012)



Graph 2: Value of Projects Funded in the Security Priority of the 7th Framework Programme as Project Coordinator by Participating State (up to July 2012)



Turning to the chief beneficiaries of the programme, the data shows a mixed picture. Four of the five firms in the list are either part of firms with a defence portfolio or are subsidiaries of defence firms. The top two beneficiaries (Thales and Indra) are firms with interests in both the defence and security sectors. Morpho (owned by Safran) and Selex Sistemi Integrati SPA (owned by Finmeccanica) trade in surveillance and detection technologies. Verint also produces surveillance and detection technologies but is associated more with law enforcement than defence. The other top ten recipients are the Swedish defence research agency, the Belgian Royal Military Academy, Germany's Fraunhofer-Gesellschaft and the Dutch TNO research organisations (some of whose groups do defence research) and the French CEA, which does research into civil and military uses of nuclear power (and since 2010 alternative energy). In this sense, the picture is a little more mixed than Jeandesboz and Ragazzo (2010) claimed but given that the security research programme is intended to be civilian in nature, there is a surprisingly high defence presence. It should be noted that again the analysis looks at the funding per coordinator – in various cases, there is clearly a successor project coordinated by a different entity, but this factor could not be taken into account.

Table 5: Top Ten Project Coordinators in Terms of Total Funding from the Security Priority of the 7th Framework Programme (until July 2012)

Project Coordinator	Total Value of Funding (Euros)
Thales Communications and Security SA (France)	37640021
Indra Sistemas S.A. (Spain)	35459846
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung (Germany)	31437774
Totalforsvarets Forskningsinstitut (Sweden)	30806584
Ecole Royale Militaire - Koninklijke Militaire School (Belgium)	30549645
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek – TNO (Netherlands)	22998389
Selex Sistemi Integrati SPA (Italy)	22143064
Morpho (France)	22048026
Verint Systems Ltd (Israel)	21108212
Commissariat à l'Energie Atomique et aux Energies Alternatives (France)	18300468

The final claim made by Jeandesboz and Ragazzo (2010) was that the programme was heavily biased towards surveillance and detection technologies at the expense of only two projects looking at the ethical and legal implications of security technologies. The majority of the projects funded under the categories 'security of the citizen', 'security of infrastructures and utilities' and 'intelligent surveillance and border security' do feature surveillance and detection technologies. These three categories account for 48.5% of spending. While the funding dedicated to primarily social science projects is less, (unsurprisingly as they require less funding than technology projects), there have been fourteen projects funded, which appear to engage with legal or ethical implications. This is possibly an example of the Commission responding to and accepting earlier criticism, but the Commission (2012a: 5) commenting on societal reluctance to accept certain technologies, argues that:

"The problems associated to the societal acceptance of security technologies results in a number of negative consequences. For industry it means the risk of investing in technologies which are then not accepted by the public, leading to wasted investment. For the demand side it means being

forced to purchase a less controversial product which however does not entirely fulfil the security requirements."[I]

This might be taken as evidence in favour of Jeandesboz and Ragazzo's (2010) assertion that the Commission is not really engaging with the ethical and legal implications of security technologies.

As has been argued above, extending the analysis to July 2012 paints a more mixed picture of the nature of the programme. Nevertheless, the Commission's critics do seem to be correct to argue that the programme was heavily slanted towards certain types of technologies, firms and countries with strong defence industrial bases. This is not surprising given the genesis of the programme outlined above, but given the discussion in part 3 of the report about whether it was desirable or realistic to try to construct a homeland security market on the same lines as the defence market, is perhaps cause for concern.

4.3.2 Policy actions taken by DG-Enterprise and Industry under the heading of sectoral competitiveness

Between 2001 and 2004 the European Commission established a number of policy advisory groups looking at different industrial sectors connected with defence: STAR 21 on aerospace,[II] LeaderSHIP 2015 on shipbuilding[III] and the already discussed Group of Personalities on security and defence research and development, which aimed inter alia to strengthen their contacts with industry and thus gain support for Commission action in the defence and security sectors (Slijper, 2005). Even supporters of the Commission's approach admit openly that, it *"has set about recruiting allies in industry to reinforce its message"* (Merritt, 2004: 238). The Commission also works closely with the Aerospace and Defence Industries of Europe (ASD) the main industry lobby group. ASD coordinates Commission funded research projects like SETRAS, a research study about enhancement of critical infrastructure protection measures and security standards. It also manages some cooperation projects with third countries for the Commission. The Commission's work on security and defence industry competitiveness is beginning to be codified in communiqués and action plans.

In July 2012 the Commission issued a communiqué on EU security industrial policy setting out an action plan to improve the competitiveness and innovation of European security industry. The communiqué accepts that there is no clear definition of the security industry and relies heavily on the work by Ecorys (2011) for its statistics on the value of it, even though that study acknowledged the limitations of the data. Contrary to earlier documents there is an acceptance that the security and defence markets are distinguishable as there are different end-users, requirements and applications, although this is rather oddly described as a fragmentation in itself (Commission, 2012a: 8). Interestingly though it describes the industrial basis supplying the two markets only as 'not fully identical' (European Commission, 2012a: 8), whereas (as discussed in section 3) other commentators have suggested a greater diversity. The features of the action plan are:

[I] The original document contains a number of spelling mistakes. These have been corrected in the quotations.

[II] The STAR21 report can be accessed here: ftp://ftp.cordis.europa.eu/pub/era/docs/report_star21_en.pdf

[III] The LeaderSHIP report can be accessed here: http://ec.europa.eu/enterprise/sectors/maritime/documents/shipbuilding/index_en.htm

Overcoming market fragmentation by:

- standardisation road maps
- harmonised certification for airport screening equipment and alarm systems
- exploiting synergies between security and defence technologies through hybrid standards

Reducing the gap between research and market by:

- aligning funding programmes (notably between Horizon 2020 and the Area of Freedom, Security and Justice) and using intellectual property rights to funded projects to test and validate them
- encourage public users to fund technological innovation by the use of pre-commercial procurement rules
- explore ways of limiting third party liability for firms

Better integration of the societal dimension by:

- societal impact checking during the R&D phase
- introducing an industry standard for 'privacy by design' and 'privacy by default' for products.

It is noticeable that the communiqué stresses the importance of export markets and the need to enable trade in security products not just within the EU but globally (the impact of this on export controls is discussed in section 5). It is also clear that the Commission is frustrated by member states' reluctance to purchase the technologies the Commission has decided are necessary. The lack of interest of national administrations in security industrial policy is visible in the fact that only 7% of responses to the consultation prior to the issuing of the communiqué came from member states – with only 59[l] responses in total, this equates to four of the twenty seven member states. The measures outlining the future use of the Commission budget for testing and validation and the pushing of pre-commercial procurement attempt to counter this. The reluctance of citizens to accept some security technologies, and deep differences between member states in attitudes towards privacy and rights is identified as a hindrance to industrial competitiveness as it can lead to wasted research.

This is not just a problem of national differences though. The security research programme has allocated €13 million to the development of a functioning prototype of a "transportable autonomous patrol for land border surveillance" or "Talos." The system comprises two unmanned ground vehicles (UGVs), one to act as a spotter and the other to act as an interceptor of any suspects attempting to cross EU borders. The UGVs are connected to manned command units and the UGVs notify them that suspects have been intercepted and tracked. Non-lethal weapons could be added to the UGVs. The consortium, which includes an Israeli firm (Israeli Aerospace Industries), is seeking further EU funding to further develop the product. According to Nielsen (2012a) a spokesperson for Frontex thought it unlikely that the UGVs would be seen on EU borders but that *"Israel might find them more digestible as border control devices".* This suggests that the societal impact checking proposed at the R&D stage needs to be rigorous.

The Commission's work on strengthening the competitiveness of defence industry has thus far been largely based around issuing communiqués (European Commission, 1996; 1997; 2003; 2007) and commissioning studies like IRIS et al (2010). The one major legislative act has been the directives known as the defence package adopted in 2009, which will be discussed fully in the next

[l] 51 responses came from businesses and business associations and four from NGOs.

sub-section. The Commission though has considerable policy ambition in this field, and the announcement in November 2011 that it was setting up a defence policy taskforce is potentially significant. The taskforce will have four key missions:

- "*Ensuring that an EU defence procurement directive and an intra-EU defence products' transfer directive are transposed into member state legislation*
- *Creating a debate in industry on determining the strategic areas where Europe needs to keep an industrial base and thereby retain strategic autonomy*
- *Exploiting synergies between the security and defence industries*
- *Ensuring coherence on security of supply issues*" (Hale, 2011)

At present though it is only possible to offer a preliminary assessment of the effects of the defence package in the next sub-section.

4.3.3 Action to regulate defence and security procurement and remove barriers to intra-EU trade

Issued in September 2004, the European Commission's Green Paper on defence procurement (European Commission, 2004b) opened wide-ranging consultations with national governments, industry and security policy institutes to frame the best approach to injecting competition into Europe's long-protected national defence markets. It set out two possible approaches:

- A communication to clarify the limits of Article 296
- A binding defence procurement directive to cover the procurement of items not included in the Article 296 list

A third option, pushed initially by the British government but which rapidly gained support from many member states, also emerged during the consultation process:

- A voluntary code of conduct regarding the use of the article, which would involve disclosure of all use of Article 296 and the reasons why a state had chosen to do so, administered by the EDA

The EDA subsequently drafted such a code on behalf of national governments. The majority of the responses reacted rather unenthusiastically to the two Commission proposals, largely because as Schmitt et al (2005) point out, it was unclear how much impact, if any, the measures would have on top-end defence procurement, which is where for the member states the problem lies. The Commission's measures would impact on procurement of those items not covered by the Article 296 list, but the extent to which protectionism in this low-end procurement is really hindering intra-EU trade was and is unclear. Nevertheless the Commission produced first and interpretive communiqué on the application of what was then Article 296 (Commission, 2006) and then produced two directives that have become known as the defence package; Directive 2009/43/EC on intra-EU transfers of defence products[I] and Directive 2009/81/EC on defence and security procurement.[II] The measures were proposed under Article 114 of the TFEU which allows legislation to be proposed to harmonise national legislation to improve the functioning of the common market. While the former should reduce bureaucratic hurdles for business,[III] it is the latter directive

[I] Directive 2009/43/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:146:0001:0036:EN:PDF

[II] Directive 2009/81/EC: http://ec.europa.eu/enterprise/sectors/defence/files/full_text_of_directive_en.pdf

[III] It does however raise some potential problems for the adequate control of exports. This will be mentioned further in section 5. See Depauw (2010) for a full discussion of the directive.

that may have considerable impact on the strength and competitiveness of European defence and security industry. The directive proposes that it establishes a specialist procurement regime for security and defence, which specifically addresses the difficult issues of security of supply and security of information, thus making it unnecessary to derogate from the regime by invoking Article 346. There are two potentially important exemptions where the directive does not apply: government to government sales and multinational collaborative projects: (Eguren Secades, 2011). Moreover, the full extent of the directive is likely to only become clear in some years time through accumulated ECJ case law. There are likely though to be two main impacts, firstly on those countries with strong defence industrial bases and procure most products nationally, and secondly on those countries that are large arms importers and use offset agreements as an industrial policy tool.

The concentration of both defence spending and industry in the same few member states, predominantly Britain, France and Germany means that much of the EU defence procurement in terms of total spend only involves these countries and their defence firms. The directive wishes to encourage open procurement to increase competition and affordability. However, there are two potential problems here. Firstly, research and development are excluded from the directive, but once the development phase is over, the contract should be tendered openly. This may be a disincentive for states to fund research, if there is no guarantee that the procurement contract would go to a firm from their country (Edwards, 2011). Secondly, while it is likely that member states will be able to declare some technologies vital to national security, such as those associated with nuclear weapons or complex weapons, and so make a case for those contracts to remain national, Edwards (2011) suggests that the Commission might insist on contracts being split for large platforms, with the non-sensitive part being openly procured. It is not clear that this would improve efficiency or affordability though. Moreover, if the Commission acts against these states, there is a very real risk that they will undermine European industry by having to open more procurement to American firms as there are few European alternatives.

Secondly, there is an impact on countries who import defence and security products. Within the global arms trade, offsets[I] are commonplace,[II] the Commission, however, feels that they distort the tendering process by shifting the focus for decision from the quality and price of the tenders to the offset deal proposed. While offsets are not forbidden in the directive, the Commission has made it clear that it will challenge their continued use. EU states can be divided into four groups on this matter. France and Germany import very little. Italy, the Netherlands, Sweden and the UK, while net exporters, do import substantial amounts of equipment from the USA and usually attach indirect offset to such contracts. Finland, Greece, Poland, Portugal and Spain import a lot from the EU and expect direct offsets. The rest have little defence industrial capacity and so favour civil indirect offset agreements (Edwards, 2011). It is the third group that has most to lose as they have been using offset to support indigenous and generally uncompetitive defence industry. The Commission has already begun to challenge the use of offsets. Its first challenge[III] was to Greece over the public procurement contract for six submarine battery kits, whose call for tenders

[I] The USA defines offset as "Industrial compensation practices required as a condition of purchase in either government-to-government or commercial sales of defense articles and/or defense services as defined by the Arms Export Control Act and the International Traffic in Arms Regulations." The full definitions can be accessed here: http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/offsets/offsetsdefinitions.html

[II] Direct offset deals are based on products and services directly related to the equipment the purchasing state is buying (e.g., local co-production of parts of the purchased weapon system). These are predominantly military. Indirect offset deals, though, can be based on either military or civilian products/services unrelated to the specific defence equipment purchased. This can include foreign investment and countertrade.

[III] Press release IP/10/1558 can be accessed here: Http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1558&format=HTML&aged=0&language=en&guiLanguage

included a requirement that 35% of the material used in the batteries should be produced in Greece. Although the Greek government claimed national security grounds (Article 346), the Commission decided the Greeks were in breach of EU rules on the basis as they had not explained why the use of standard EU public procurement rules would endanger Greek security interests. It should be pointed out that the case for offset use is not economically proven, but ending its use will probably have a deleterious impact on some defence firms in the countries affected (Mawdsley, 2008a). The second group of countries, who buy from the US, might also lose, as they have often used offset as a way to embed sub-contractors into lucrative US supply chains. The UK though has already abandoned offset for imports entirely (UK MoD, 2012), which suggests that the impact is not thought to be so great.

To summarise, while it is undeniable that the directive may make the market more efficient, it is not clear that it will increase the strength and competitiveness of European defence industry. While the loss of some uncompetitive firms may be beneficial in the long-run, there are two significant risks. Firstly, that the directive has the unintended effect of increasing US market share in the EU, and secondly, that defence industrial capacities will be concentrated in even fewer states with the risk that this increases the number of states uninterested in funding defence R&D. Interviews with industry figures in January 2012 revealed that industry was very anxious about the effects, pointing out that it did nothing to consolidate demand. There is no guarantee that states that lose indigenous defence industrial capacity will 'buy European' subsequently, the US and Russia will be keen to offer their products, which may be more suitable than European alternatives. The directive also applies to sensitive security products but the impact is likely to be less severe on a market that is still immature.

4.3.4 Development of 'homeland security' type policies and their associated technological needs by DG Home Affairs.

In many ways the work of DG Home Affairs complements that of DG Enterprise and Industry. Parallel to the security research programme DG Home Affairs runs a Framework Programme on Security and Safeguarding Liberties, which is composed of two specific programmes: 'Prevention, Preparedness and Consequence Management of Terrorism' and 'Prevention of and Fight against Crime'. The total budget for the 2007-13 cycle is €740 million. This programme aims to support *"operational, highly specific and policy-oriented activities".* In particular the terrorism programme has a focus on protecting critical infrastructure that has commonalities with the aims of the security research programme.

Schengen states can also apply for funding to the External Border Fund, which aims to offer financial solidarity to those member states, for which "the implementation of the common standards for control of the EU's external borders represents a heavy burden".[I] States can apply to upgrade border surveillance equipment including equipment ships and helicopters with the Fund financing up to 90% of some projects although 80% appears to be the most common. Overall, €1 820 million was allocated for the Fund over the financial period 2007–13. Particularly for those states affected badly by the financial crisis, this fund offers a heavy subsidy for the purchase of some internal and external security equipment. For the next budget cycle 2014-20, the Commission has proposed establishing an Internal Security Fund with funding of €4648 million, to assist in the

[I] For information on the External Borders Fund see: http://ec.europa.eu/home-Affairs/funding/borders/funding_borders_en.htm

implementation of the internal security strategy.[I] This is planned to be the financial support instrument for *"police cooperation, preventing and combating crime, and crisis management"* and external borders and visas, so effectively bringing together the two programmes already discussed.

The Commission communiqué on their budget plans specifically aims to fill the gap between the security research programme and procurement. *"In addition, funding is made available for particularly innovative projects which aim at developing new methods or technologies, especially the testing and validating of the outcome of EU funded security research. This will help close the gap between the research results achieved with support from the 8th Framework Programme and their serial application in practice for the benefit of the law enforcement community."* (Commission, 2011: 7) There are also links through the proposed EUROSUR border surveillance system that for instance suggests that *"European research and development programmes could be targeted towards improving the performance of surveillance tools and sensors (e.g. satellites, unmanned aerial vehicles / UAVs, etc.)"* (European Commission, 2008).[II] The European Commission (2012a: 9) communiqué on security industrial policy also explicitly states that the Internal Security Fund can be used to fund the testing and validation of funded security research projects. It appears that even if the member states are not convinced of the need to increase their demand for internal security technologies, as discussed in part 3, the European Commission is doing its upmost to maximise the market.

4.4 European Defence Agency

The European Defence Agency's role is defined as follows:

"The Agency in the field of defence capabilities development, research, acquisition and armaments (hereinafter referred to as 'the European Defence Agency') shall identify operational requirements, shall promote measures to satisfy those requirements, shall contribute to identifying and, where appropriate, implementing any measure needed to strengthen the industrial and technological base of the defence sector, shall participate in defining a European capabilities and armaments policy, and shall assist the Council in evaluating the improvement of military capabilities". (TEU Article 42(3))

It is therefore the EU institution, which is most obviously tasked with ensuring the strength and competitiveness of the European defence industrial and technological base (EDITB). Given that the EDA is intended to give strategic direction to the EU's armaments efforts, it seems worth analysing its statement on the shape of the European defence industrial base of the future (2007) to see whether they have been able to produce coherent and viable policy directions. Accepting that harmonization of the demand side is needed to facilitate consolidation of the supply side, the EDA (2007) states that EDITB should be:

- Capability-driven (that is, focussed on meeting the real operational requirements of the Armed Forces of the future, whilst sustaining the necessary levels of European and national operational sovereignty);
- Competent (denoting in particular the rapid exploitation of the best technologies); and
- Competitive (both within and outside Europe).

[I] EU Internal Security Strategy: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf

[II] For an extremely critical report on both the initiatives and the European Commission's failure to question the claims made by firms about their equipment, see Hayes and Vermeulen (2012).

The EDA suggests that to achieve this, there needs to be more consolidation, work-sharing and interdependence on an EU basis, centres of excellence (with appropriate regional distribution), greater integration into the civilian industrial base, with *"less European dependence on non-European sources for key defence technologies"* but without resorting to a Fortress Europe approach (EDA, 2007). However, while these aims may be laudable it is clear that significant further consolidation will produce monopolies rather than competition (Hartley, 2006), and that regional distribution (while desirable) ignores the realities of the state of the EDITB (Mawdsley, 2008b). In reality as Hartley (2011) points out there is still excess defence industrial capacity in the EU, and these firms should not be artificially shielded. In many ways the EDA has inherited the almost impossible task of reconciling the ambitions of big and small arms producing states and between Fortress Europe and free market enthusiasts, which stalled progress within WEAG. They must also do this in a time of financial austerity, where increasing numbers of member states no longer carry out defence research according to EDA's own statistics, and where defence expenditure is falling. The EDA is also hampered by trying to develop a policy without adequate data; as Hartley argues there are *"major data limitations: gaps in the data mean that it is not possible to obtain the statistics needed for an adequate economic evaluation of the individual sectors of the EDTIB."* (Hartley, 2011: 96-7)

The EDA's biggest problems though are twofold. Firstly, it lacks the budget to really provide the incentives for member states to get involved.[I] Secondly, British support has been lukewarm from the start and the country is currently evaluating whether to remain a participant. As early as November 2006 when the EDA Steering Board launched a three year €54.23 million force protection research programme, the UK declined to take part. France too seems less convinced that the EDA can deliver what it deems vital for its own DITB. Without the active support of the two biggest spenders on defence research and procurement, it is difficult to see how the EDA can be expected to make substantial progress. Like the Commission, the EDA is not a customer, so it suffers from the same problem that even if it sponsors technology development to demonstrator stage, it cannot force member states to procure the equipment, thus dis-incentivising stronger firms from sharing technologies. It is therefore limited in what it can really do to strengthen the EDITB. This is not to say that the European Defence Agency has achieved nothing useful. It has set in play various projects with real military utility. In establishing a voluntary code of conduct on opening up defence procurement, it paved the way for the Commission directive. Moreover, its work on offsets has injected some valuable transparency into European practices.

While Commission and EDA cooperation has now been codified in the European Framework Cooperation for Security and Defence, and generally appears to be working well, there are also problems in reconciling the Commission's 'European Defence Equipment Market' (EDEM) approach, which aims to apply as much single market logic as possible to the defence market (as has already been discussed with the procurement directive), and the need to retain an EDITB. Hartley (2011) summarises the key difficult choices that need to be made thus:

"i) ***Conflicts between the EDEM and EDTIB.*** *Choices are needed either to restrict competition to firms from Member States only or whether to allow other firms from the rest of the world to enter EU defence markets (e.g. US defence firms). Competition might also threaten key defence industrial capabilities and the appropriate regional balance of capabilities needed for the EDTIB. In the absence of competition, privately-owned monopoly defence firms will have to be treated as regulated firms with the associated problems of determining prices, efficiency and profitability.*

[I] Although the budget has risen steadily, in 2010 it was still only €31 million.

ii) ***Maintaining key specialised defence industrial capabilities during troughs in development and production work.*** *These are specialist firms with no alternative uses for their plant and human capital but which are needed in the future (e.g. capability in nuclear-powered submarines; main battle tanks; aircraft carriers). Such specialist capabilities might be prime contractors or small and medium enterprises in the defence industry supply chain. Selecting which key capabilities to retain is only the starting point. Further issues arise about how to retain such capabilities (e.g. interim orders; mothballing of plants, etc.), the costs of alternative retention policies, who decides and who will pay." (Hartley, 2011: 111)*

These are decisions that will be politically very difficult, and will require a level of intra-institutional cooperation that will not be easy.

4.5 EU Member States

Although for some, the European Union is now regarded as the natural home for defence and security industrial policy-making, it is challenged by a number of other actors. Firstly, a growing number of important states like Germany, the UK and France have made it clear that they regard CSDP as a vehicle for crisis management rather than for defence (Auswärtiges Amt, 2012; Haine, 2011). The 2010 Franco-British Lancaster House agreements in particular have the potential to reshape the defence industrial scene. Secondly, there are a number of multilateral initiatives that remain outside the EU such as OCCAR (Organisation Conjointe pour la Coopération en matière d'Armement) and the Framework Agreement. Finally, NATO is involved in counter-terrorism cooperation and countering cyber warfare.

4.5.1 Key Bilateral and Multilateral Agreements

It is important to stress the continuing presence of multilateral and bilateral defence cooperation. There are a number of formal groupings like the highly developed Northern Defence Cooperation (NORDEFCO) and the increasingly active Visegrad Group, which aim to improve capabilities by closer cooperation between a small number of like-minded states. The 2010 Franco-British agreements on defence cooperation appear though to be particularly important as they seem to set certain parameters for future European armaments cooperation. It is worth outlining the extent of what was agreed because of the focus on conventional and nuclear weapons. Within the framework of two legally binding treaties, both states committed themselves to extending the cooperation between their armed forces and to joint development of their nuclear weapons technology, marking a step change in the level and depth of their bilateral cooperation. Alongside the ground-breaking treaty on nuclear cooperation, the establishment of a joint expeditionary force and various pooling and sharing measures, London and Paris also agreed extensive defence industrial cooperation.

The agreed cooperation in the fields of defence technology and industry is also based on congruent strategic considerations that have been developed over many years.[l] The ten year plan for cooperation in the field of complex weapons, to be started in 2011 with the development of the anti-surface missile FASGW(H)/ANL, an assessment of enhancements to the Scalp/Storm Shadow

[l] An Innovation and Technology Partnership was launched in 2007 by both countries to look at synergies in complex weapons research and requirements.

cruise missiles, and a joint technology roadmap for short range air defence technologies, showed the importance for both states of improved industrial cooperation. In order to develop cooperation between British and French defence firms, funding for joint research and development projects of €100 million annually has been agreed. Chick (2011) suggests that maintenance of defence industrial capacities is central to the Franco-British cooperation. Further agreements in both 2010 and 2012 on cooperation on MALE drones and on Future Air Combat Systems could lead to a government-sponsored consolidation of that market segment, leaving other European states outside (Kempin, Mawdsley and Steinicke, 2012).[I]

Paris and London could have decided to carry out the agreed projects within the EU framework of permanent structured cooperation, which offers the possibility for member states to cooperate flexibly in the defence field. Their decision not to shows the low level of expectations both countries have of meaningful progress in CSDP capabilities cooperation, and particularly the frustration that France has felt since they failed to secure adequate progress during their 2008 EU presidency and in the aftermath of the Chad mission (Haine, 2011). This attitude will also have consequences for the European Defence Agency (EDA). It seems that both states' unhappiness with the level of progress made by the EDA in the realisation of urgently needed military capabilities, has led them to cooperate outside the EU institutions. This decision by France, in particular, which until now has been the leading nation in its consistent support of the EDA's work, is likely to weaken the EDA. Britain and France have not rejected EU armaments cooperation but have made it clear, that it must be on their terms. It is also to be expected that they will be resistant to any involvement of the Commission in defence if it is seen to risk their defence industrial capacities.

It is also worth considering the Framework Agreement on defence industrial restructuring (UK, France, Germany, Italy, Sweden and Spain) and the Organisation Conjointe de Coopération en matière d'ARmement (OCCAR – UK, France, Germany, Italy, Belgium and Spain), not because they are likely to significantly impact on EU action, but because their experience in this area is illustrative of some problems that the EDA and potentially the Commission will face. The Framework Agreement came to fruition through what was known as the Letter of Intent (LoI) process, signed up to in July 1998 by the Defence Ministers of France, Germany, Spain, Italy, Sweden and the UK. This process tried to develop a framework of co-operation to facilitate the restructuring and operation of the West European defence industry as well as assisting an industry-led restructuring of both the aerospace and defence electronics sector. In 2000, the same Ministers signed the Framework Agreement which agreed measures for improving co-operation on harmonisation of military requirements, security of supply, export procedures, research and technology, handling of classified information and the treatment of technical information. Work within the Framework Group has continued since the establishment of EDA and some useful steps agreed, but the cooperation has not led to joint procurement projects. Interestingly even among the states with the most defence industrial activity, a 2005 report to the Framework Agreement states found little evidence of fragmentation and duplication and moreover, that only 7% of defence technologies considered were common priorities for all six states. There was though bilateral commonality in 74% of technologies (UK MoD, 2006:35).This brings into question whether the EU analysis of market fragmentation and duplication is accurate but perhaps more importantly shows how difficult it will be to find research and procurement projects that all the large arms-producing states would be prepared to sign up to.

OCCAR is a management agency for collaborative defence procurement programmes. An agreement establishing administrative arrangements for cooperation between EDA and OCCAR and

[I] Italian protests to the Commission about the Franco-British cooperation being anti-competitive were rejected (Kington, 2011).

on the exchange of classified information has been blocked by Greece and Cyprus in the Council since 2009. OCCAR was intended to manage collaborative defence procurement projects on a much more commercial basis, drawing on best practice in procurement from the private sector and as an arms length agency essentially depoliticising the process. The A400M was the first project to be subjected to this commercial approach and results have not been good. This has led the British and the French to conclude that the sustainability of their DITB is not something to be risked by cooperation with partners less serious about it than themselves (House of Commons, 2010; Masseret and Gautier, 2009). Although OCCAR itself is still thought worthwhile, the experience of the A400M project might make it difficult to persuade key states to participate in large scale procurement projects for CSDP if they are open to all EDA member states.

4.5.2 Is NATO relevant?

As Haine (2011) points out NATO remains of central relevance to discussions of European security and defence, as despite US ambivalence, it, with Franco-British leadership, rather than the EU, became the central actor in the Libyan operation of 2011. More specifically for the purposes of this report, it is also involved in counter-terrorism cooperation and countering cyber warfare. This short overview seeks to outline what overlap there is between NATO and EU actions with regards to the role of industry and technologies in these areas.

One obvious area of overlap is between NATO's Smart Defence, which tries to enable states to jointly purchase equipment and the EU Ghent Initiative on pooling and sharing of military capacities. Both aim to improve European military capabilities. However, Maulny (2012) argues that unless the modalities of cooperation between the different schemes are agreed, then there is a risk that they undermine each other. Maulny (2012) offers competition between the EU and NATO on air-to-air refuelling pooling as an example.

As far as counter-terrorism is concerned there also appears to be potential overlap between NATO's Defence Against Terrorism (DAT) programme and European Commission and EDA initiatives in the field of security and defence technology development. The DAT programme is based on scientific research and testing of counter-terrorism technologies. NATO and the EDA do though work together to avoid duplication of research and DAT is a purely military programme. It is focused on ten areas, each led by a lead nation, where analysis suggests technology can help:

- Reducing the vulnerability of wide-body civilian and military aircraft to man-portable air defence missiles (MANPADs) (UK)
- Protecting harbours and ships using sensor nets, electro-optical detectors, rapid reaction capabilities and unmanned underwater vehicles (Italy / Portugal)
- Reducing the vulnerability of helicopters to rocket-propelled grenades (RPGs) (Bulgaria / Greece)
- Countering improvised explosive devices (IEDs), such as car and road-side bombs, by their detection and disruption or neutralization (Spain)
- Detecting, protecting against and defeating chemical, biological, radiological and nuclear (CBRN) weapons (Czech Republic).
- Technologies for intelligence, reconnaissance, surveillance and target acquisition (IRSTA), with the goal of developing improved tools for early warning and identification of terrorists and their activities (Germany)
- Explosive ordnance disposal (EOD) (Slovakia)
- Technologies to defend against mortar attacks (DAMA) (Norway)

- Protection of critical infrastructure – now an overarching project within the DAT programme, integrated into the Portugal-led harbour protection programme
- non-lethal capabilities (Canada)[I]

This work programme was approved in June 2004 and should not overlap with current Commission activity on security research, as this is intended to be civilian. However, as the Commission's security industrial policy and its Defence Task Force both intend to draw on synergies between security and defence industries in the future, the potential for conflict exists. There are also areas of overlapping interest in cyber security and cyber warfare. One area where NATO could be useful, is if it was to be used as a forum for the exchange of technological information between the US and EU on which homeland security projects were viable. The US Department of Homeland Security is currently prevented from engaging in such exchanges, but if this were to change, NATO might be an acceptably secure arena (Committee on Homeland Security and Export Controls, 2012). As some of the research funded by the European Commission looks similar to projects cancelled by the US as ineffective, this could save money (something that given the financial crisis is crucial).

4.6 Summary

This section of the report has first outlined the legal basis for EU action. It then looked at Commission policy, considering the security research programme, sectoral competitiveness action, the defence package of directives and finally, the involvement of DG-Home Affairs in developing homeland security type policies. It then moved on to look at the European Defence Agency. The final substantive sub-section considered related European activity outside the EU, namely, the Franco-British defence agreements, OCCAR, the Framework Agreement and NATO, and sought to evaluate what if any impact they might have on EU policy success.

The Commission, despite long aspiring to be active in the sector, has only really become an actor in the last decade, and the first directives are only now being transposed into national law. At present, it is not clear whether the member states will allow it to expand its role further (despite its clear intentions to do so), and opinions are divided on whether there is a legal basis for it to move further onto the terrain of national security. Equally, its actions on internal security are both enabled and challenged by the Lisbon Treaty, as it seems likely that the hitherto emphasis on surveillance technologies is likely to meet legal challenges. The Commission seems to have the same diagnosis for both the defence and security markets, namely:

- The supply side is too fragmented. Industrial consolidation and mergers are required in all sectors
- The demand side is also too fragmented and both national procurement regimes and requirements need to be harmonised.

It is these beliefs that guide its actions. However, its critics argue that it should not assume that the security and defence markets are essentially interchangeable, and that policy needs to be more nuanced. They also argue that the Commission has been guilty of taking a technology-centric and defence industry focussed approach to the more nuanced needs of the internal security user community (and paying insufficient attention to ethical concerns about its agenda). The overestimation of the demand from users, given the Commission cannot (despite its best efforts

[I] For more information on the DAT programme, see http://www.nato.int/cps/en/natolive/topics_50313.htm.

through the External Borders Fund) act as a customer, suggestions that such interactions need to be strengthened in the next Framework Programme if research is not to be wasted. The main problem with the emergence of the security research field, is potentially that the Commission's entrepreneurial attempts to extend its policy competences, have led to a disconnect between what the Commission and industry would like to see, and what member states and EU citizens are prepared to countenance. This could lead to unintended consequences. Similarly, it is possible that its efforts at reforming the demand side of the defence market, through the procurement market, may have detrimental impacts on the EDITB depending on how it is enforced.

The European Defence Agency has been set a near impossible task of reconciling contradictory member state wishes, without an adequate budget, and without the support of one (and increasingly more) key member states. Unsurprisingly, while some of its projects are undeniably useful, it has not been able to reconcile these differences. The questions of how to reconcile the contradictions between market-driven and protectionist approaches, and how to maintain key EDITB capacities when there is little demand, cannot remain unanswered for much longer despite the difficult political compromises that will inevitably need to be made. As Hartley (2011) points out, European defence firms are not particularly competitive when compared to their US counterparts. Nor can it be assumed, as some have optimistically thought that security industry and demand will offer an easy diversification route.

The biggest challenges to the EU's capacity to make policy to strengthen the competitiveness of European security and defence industries come from outside the EU institutions. Here there are two main issues. Firstly as NATO becomes more active in counter-terrorism, there is a risk that an alternative transatlantic agenda emerges, which could potentially duplicate or contradict Commission actions, although as argued above, it could also be helpful in avoiding duplication and wastage. Secondly, the Franco-British agreements on defence open up the possibility of an even more concentrated state of procurement and research expenditure and industrial power in both defence and security, which will be antagonistic to any attempts at regulation. However unpalatable this might be however, to those preferring action at the EU level, it might also be the case that the two states are correct in their calculations that this is the only way to preserve sufficient industrial, technological and military capabilities to make any European security action feasible.

It is though that the Commission is the pivotal actor at present. If it is to continue to expand its competence unchecked though, it needs to be more realistic about what member states can spend on security and defence in a time of fiscal crisis, and to be much more aware of the ethical issues surrounding security. In questioning the negative emphasis that supporters of the EU as a civilian power put on the development of ESDP, Bailes argued that:

"The real issue is not so much about 'militarization' of the Union as about an increasingly salient securitization of its entire identity and image, which the EU as a conscious organism is not yet equipped to recognize, let alone to handle maturely, and from which the ESDP's small do-gooding adventures can come almost as a relief." (Bailes, 2008: 119)

There is a real sense that this might be an accurate description of the Commission's activities in the security field, in that there seems to be a failure to consider the acceptable balance between human rights and security, which leads to a growing gap between the EU's activities in this area and its foreign policy statements. This is immediately visible when we consider the question of export controls on security technologies.

5 Security Technologies and their Impact on Strategic Goods Export Controls

5.1 Introduction

The Arab Spring raised new questions about the adequacy of EU arms export control regulations, but as Bromley (2012: 14-5) puts it *"some of the more damning revelations concerning exports from EU member states to the Middle East and North Africa in the wake of the Arab Spring uprisings have concerned transfers of surveillance software and other types of technology for monitoring regime opponents"*.[I] These reports have turned policy-makers' attention to the question of how one might monitor and control such technologies. The European Parliament's efforts in 2011 to amend Council regulation 428/2009 on the export of dual-use technologies,[II] to include such technologies were only partially successful, but the inclusion of restrictions on the export of telecommunications technology and equipment to enable surveillance in 2012 EU sanctions on both Syria and Iran, suggests that the issue has continued political salience.

The renewed debate around the control of security technologies has reopened a difficult issue for the EU. The Code of Conduct on arms exports, which later became a Common Position, was initially intended to contain a third list (alongside the military list and the dual-use list) covering security and police equipment. Bauer (2003) claims that arguments over legal competence, definitions and methods of control meant that this list was not added. Instead a weaker (in terms of the equipment covered) and more specific regulation, known as the Torture Regulation, was agreed in 2005. This means that security technologies and products are partially covered – some fall under the military or dual-use list and others are covered by the Torture Regulation – while others are controlled at a national level only, but the legal situation is not as clear as it might be. Bromley (2012) claims that one group of security technologies used for surveillance and detection is not covered at all, which has enabled their export and misuse during the Arab Spring.[III]

Although attention was drawn to the problematic nature of the trade in surveillance technologies as early as 1995 by Privacy International (1995), prior to the Arab Spring the export of surveillance and other security technologies had not attracted much attention from either civil society or legislators, with the exception of a few reports from NGOs like Amnesty International and the Omega Foundation who have campaigned on the issue (Amnesty International and Omega, 2010; Amnesty International, 2011). Indeed, rather than being seen as a problem, some states, particularly Germany, have come to view the security technology sector as a major export

---

I See inter alia Wagner (2012a) and Timm and York (2012).

II This defines dual-use items' as "items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices", Council of the European Union, Regulation 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, Brussels, 5 May 2009: Article 2 (1)

III It is not entirely clear whether this is correct. In August 2012 in a response to a letter from Privacy International the UK government stated that it had informed Gamma International, the makers of Finspy surveillance software, that it requires licences for all non-EU exports as the product used controlled cryptography covered by category 5 part 2 of the dual-use legislation. It seems likely that this would apply to other similar products (Privacy International, 2012)

opportunity (Bundesministerium für Wirtschaft und Technologie, 2010).[I] Indeed, the European Commission (2012a: 2) even after the Arab Spring states, in support of its view that there needs to be an EU brand for security technologies, that: *"the central future markets for security technologies will not be in Europe but in emerging countries in Asia, South America and the Middle East."*

Indeed, the communiqué on security industrial policy suggests a desire to liberalise trade still further rather than restrict it (European Commission, 2012a). This clash of approaches to this matter suggests that political agreement will be difficult to find. The rest of this introduction will briefly outline how and why the issue of the control of security technologies has regained political salience.

While more conventional policing technologies such as water cannon and tear gas are often used to suppress political demonstrations, political attention has been drawn recently to software used to track activists or disrupt communications technologies. The terms twitter / facebook / wikileaks revolutions have been applied to a number of protests and uprisings since 2009, notably with respect to the 2009 Moldovan civil unrest, the Iranian election protests in 2010 and the Tunisian and Egyptian uprisings in 2010 and 2011, which formed part of the group of uprisings known as the Arab Spring. The use of social media to both exchange information within the states and to publicise what was happening to the outside world, was feted in the media, almost to the extent that the underlying causes of the protests were neglected.[II] However, the media attention to the use of social media also meant that attention was paid to the way in which the internet was censored, and surveillance technologies used to track protestors in the regimes' attempts to stop the demonstrations. As Wagner (2012a) details there is a growing evidence base to show how deep packet inspection technology is used to censor the internet across a large number of states in the Middle East and North African (MENA) region (and beyond). Additionally, there is evidence that many states in the region maintain surveillance infrastructures (Wagner, 2012a). Use of both types of technology was made during the Arab Spring to filter the information available to citizens (e.g. external news coverage) but more worryingly to identify and imprison social media activists. A Bloomberg investigation uncovered evidence that some activists caught through these methods were tortured (Elgin Silver and Zschiegner, 2011).

Much of this technology and the technical expertise to maintain it had been exported to the MENA region by US and EU firms. The Bloomberg investigation implicated the following EU firms: Nokia Siemens Networks (Finland), Ericsson AB (Sweden), ETI A/S (Denmark), AdaptiveMobile Security Ltd (Ireland), Creativity Software Ltd (UK), Amesys (France), Qosomos SA (France), Trovicor GmbH (Germany), Ultimaco Software AG (Germany) and Area SpA (Italy) (Elgin, Silver and Zschiegner, 2011). Wagner (2012) also identifies the activities of French firm Wanadoo in Tunisia and Gamma International (UK) in Egypt as problematic. A New York Times report also implicated Gamma International in sales of surveillance software, known as Finspy, used to monitor activists in Bahrain, Brunei and Turkmenistan (Perlroth, 2012). Recent Wikileaks releases have also shown that Italian firm Finmeccanica sold communications technologies to the Syrian police until 2012 (Clark, 2012). As the negative press coverage spread, it initiated discussions in the EU member states and in the European Parliament about how and if the export of such technologies should be regulated.

[I] Germany chose security technologies to be one of four fields to benefit from a export market expansion support programme for SMEs starting in 2012: Auslandsmarkterschließung für kleine und mittlere Unternehmen – official document accessed 21 July 2012 at: http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Aussenwirtschaftsfoerderung/aussenwirtschaftsfoerderunginstrumente,did=193980.html

[II] Other more analytical accounts have stressed the need not to overstate the contribution of social media (Comninos, 2011; Morozov, 2011).

This background has meant that the renewal of the debate on how and whether to control the export of security technologies has had a particular focus on surveillance technologies.

It is helpful at this juncture to return to the discussion on security technologies in section 3 of this report. The report has already argued that military and security products increasingly draw on the same range of generic technologies, particular ICT technologies, which are in wide use within the civilian sector. This does blur the boundaries around both knowledge production and the application of the technologies, not just between military and non-military security products, but with wider civilian and commercial technology innovation (James, 2009b). It clearly also brings new challenges to non-proliferation agendas, and to the design of effective control regimes for both tangible and intangible exports. This is in effect a classic example of the difficulties in regulating the exports of dual-use items.[I] However, this group of technologies and products is even more complex as they do not necessarily fit the definition of dual-use, as they can be used for human rights abuses and internal repression without there being any involvement of military forces. Finally, as Edler and James (2012) point out the Commission has deliberately kept the concept of security research, firms and technologies ambiguous for their own purposes. This ambiguity makes it difficult to define the sort of boundaries needed for security technologies to be added to the list-based systems of export controls that exist for military and dual-use goods.

It has already been pointed out that security technologies and products are partially covered by three separate EU regimes, namely the Common Position on arms exports, the dual-use regulation and the torture regulation, and additionally national controls. All three appeared to be under review at the time of writing. The report will assess each of these regimes, outline which security technologies are covered and what the strengths and weaknesses are, and discuss the potential reforms proposed. It will also look at the effectiveness of sanctions and embargos and of industry-led voluntary codes. Finally, it will assess the strength of claims that rather than controlling them, there is a need to enable such exports, looking in particular at the external aspects of the EU's Internal Security Strategy.[II] Firstly though, the next sub-section of this debate will outline how the European and latterly EU position on the control of strategic goods has evolved, the different ways in which the debate can be framed, and point to emerging trends, which may have an impact on the discussion about the control of security technologies.

5.2 The Control of Strategic Goods: Framing the Debate

While the synergies between defence and security technologies, firms and products can be overstated (IRIS et al, 2010), the similarities are such that it is understandable that policy-makers wishing to restrict exports of security technologies have turned to the framework governing defence exports and in particular the dual-use legislation. It is perhaps worthwhile at this point to consider the potential rationales for arms export control and see how they apply to security technologies and products. Governments have deemed it desirable to restrict exports of arms for the following reasons:

[I] Although Wagner (2012a: 7) points out that that "typical censorship and surveillance technologies are sold as systems and are not typically used for multiple overlapping purposes. Although the base hardware is theoretically capable of performing multiple diverse tasks, the systems themselves are typically built and maintained for one specific purpose: limiting individual human rights."

[II] The US Committee on Homeland Security and Export Controls (2012) for example argues that US export controls on homeland security technologies are preventing the DHS from engaging in international cooperation.

1. Non-proliferation of certain types of technology – here we think particularly of controls on the exports of technologies enabling nuclear, biological and chemical (NBC) weapons, but also certain types of missile technology. The proliferation of such technologies is deemed to endanger global security and stability.
2. Maintenance of strategic superiority – countries may decide to forbid the export of technologies that allow them to maintain a strategic edge over their competitors.
3. Maintenance of control over 'their' defence firms – concerns about security of supply may lead states to prevent key defence firms from building up substantial business in other states to ensure that they retain power over that firm and thus defence supplies.
4. Prevention of human rights abuses or escalating conflict situations – states may have ethical reasons to forbid arms exports e.g. they have reason to believe the recipient state would use the equipment to perpetuate human rights abuse. Equally they may decide that arms exports would escalate a regional conflict.

Realistically, the only argument that is likely to really apply to security products is human rights concerns. On the other hand governments may decide arms exports are desirable for the following reasons:

- Pursuit or maintenance of influence – governments may permit arms exports to regions or states where they wish to increase or maintain their strategic influence on the recipient state.
- Wealth – arms exports are usually considered to be profitable for the exporting state (although export subsidies make this assertion questionable).
- Maintenance of indigenous weapons programmes – substantial exports increase the affordability of indigenous weapons programmes through economies of scale.

These arguments in favour are all made implicitly or explicitly with respect to the export of security products by the Commission in their security industrial policy communiqué (European Commission, 2012a), suggesting that convincing the EU of the necessity of export controls on security technology will be difficult.

Equally, it is necessary to ask whether arms export controls are effective and whether they could be easily applied to security technologies. Cooper (2006) points out there is already a substantial difference in effectiveness between arms control regimes aimed preventing the proliferation of key technologies (especially NBC technologies) and controls on conventional arms, which he suggests are largely tokenistic. The former are largely successful because of three factors. Cooper (2006: 119) argues that firstly there are *"relatively high technological barriers to entry"* coupled with *"scarce availability of key materials"*, secondly, that the disciplinary mechanisms in the regimes are both severe and enforced, and thirdly, that the regimes are underpinned by a *"powerful (and almost universal) norm against NBC proliferation"*. Conventional arms export control regimes in contrast frequently suffer from a lack of political will to overcome strategic and commercial interests. Moreover, the increasingly global nature of the defence industry undermines national controls. Finally, the growing importance of dual-use technologies in defence equipment and pervasive *"globalised illicit arms networks"* have eroded the strength of existing conventional weapons transfer controls as proliferation is significantly harder to prevent (Cooper, 2006: 118). Certainly the EU Common Position on conventional arms exports has been criticised for failing to prevent exports to problematic recipients (Poitevin, 2011). The dual-use export controls are also viewed as inadequate where conventional weapons are concerned as attention has concentrated on stopping nuclear proliferation.

What does this tell us about the likely effectiveness of a regime aimed at controlling the export of security technologies? Let us first examine the factors that underpin the success of the NBC regimes. Are there high technological barriers to entry or reliance on hard to obtain materials? In the case of security (and much conventional military) equipment the answer is increasingly no. Neither is expertise confined to the EU and allied states. This immediately limits the ability of the EU to limit the proliferation of security equipment, particularly where complex systems integration has not been involved. Secondly, as with conventional arms exports, the international penalties for states failing to enforce dual-use legislation and sanctions are not particularly severe (Cooper, 2006). Thirdly, there is no universal or powerful norm against the export of security equipment; indeed the global logic of the 'War on Terror' would suggest that such exports would be desirable.

Finally, we have to consider how the debate on the control of strategic goods is being framed at present. Cornish (1995) points out that the rationales for enabling or preventing weapons sales within Europe have not been consistent, but rather reflected the status of international relations at the time. While during the Cold War arms exports from Western Europe were often tied to ideals of furthering Western ideas and influence and preventing sales to those who did not share these aims, at the end of the Cold War political restrictions vanished, and there briefly a near free market in arms emerged (Cornish, 1995). Economic rather than balance of power considerations became important. It could also be argued in the 1990s that political and NGO attention turned away from the task of general controls on conventional weapons, and towards ensuring non-proliferation of nuclear, biological and chemical weapons and to stopping the trade in what became known as 'pariah' weapons such as cluster bombs and landmines. Following a series of scandals in the 1990s though, political will in the EU emerged to agree a system of arms export controls, that would take into account the recipient state's human rights record. As Bailes (2004) has argued, the Code of Conduct started a virtuous circle of pressures to improve consistency and transparency between EU member states through annual reporting and mutual pressure. Rather than a race to the bottom, it seemed that a new era of responsibility was emerging.[I] When in 2008 the French dropped their long-standing opposition (in return for the acceptance of the directive on intra-community transfers (ICT) of defence products), and the Code of Conduct became a legally binding Common Position, the EU broke new ground. However, as Poitevin (2011) and Depauw (2010) point out, the Common Position has been rather disappointing in the way it has been implemented thus far. There has been delayed and substandard reporting from member states, the Position is inconsistently implemented (especially problematic given the ICT directive), and arms export scandals are still occurring. Moreover, there are signs that one important state, Germany, is seeking to loosen arms export controls through NATO. The German media has reported that Germany presented a paper to the 2012 Chicago summit calling for agreement on a list of strategically important states for the NATO partners, to whom arms sales would be permitted even if their human rights records were weak (Steinmann and Dierks, 2012). The Financial Times Deutschland names the members of the Gulf Cooperation Council as among those proposed. While the initiative was apparently coolly received by other NATO states, this marks both a substantial shift in Germany's own restrictive approach to arms export controls, but also a potentially problematic step for NGOs pushing for improvements in the EU Common Position.

These shifts in attitudes on conventional arms export also play into the framing of the initial debate on the control of security technologies. Early discussions, notably in the European Parliament about the updating of the dual-use regime in 2011,[II] together with the media reports from the Arab Spring, focussed attention on surveillance and detection technologies. They revealed both a lack of

[I] Although France, Germany and the UK continued to feature regularly in the top five of annual lists of arms exporting states.

[II] These will be discussed fully in the sub-section on dual-use.

political will in some quarters. Although there is some support, notably in the Netherlands (the Dutch Foreign Minister Uri Rosenthal supported export controls on technologies that filter Internet content for example) and to some extent in the UK, the German government lobbied heavily against the inclusion of stricter measures on telecommunications technologies in the revised dual-use legislation. In 2010 the then German Economics minister, Rainer Brüderle, declared the civilian security area to be a future market for German industry and warned against burdening industry with legal impediments.[I] Despite the growing evidence of misuse of EU and German exports of surveillance technologies to repressive regimes,[II] his successor Rösler is determined to maintain this position (Schumann, 2011). Similarly, Sweden softened sanctions against Syria in 2011 by blocking the inclusion of two Syrian telecommunications firms with commercial links to Swedish firm Ericsson on the sanctions list (Brunnstrom and Ringstrom, 2011). The discussion on security technologies is also being played out against a backdrop of Commission attempts to liberalise dual-use controls, which will be discussed in the sub-section on dual-use controls.

The case for the EU acting as a normative or virtuous international actor, which therefore restricts exports of security technologies on human rights grounds, is less clear-cut than it has been in the past on conventional arms exports, allowing policy space for different conceptions such as the EU as a trading power or security provider to emerge. The concentration on surveillance technologies has meant that the debate has been orchestrated by internet freedom NGOs (and human rights NGOs) rather than those who have specialised in the arms trade (possibly because their energies were devoted to the UN Arms Trade Treaty negotiations). The continuing economic troubles affecting most EU member states also do not favour agreement on controls. Moreover, there is also a precedent for disagreement in that the EU has failed in the past to agree a list of security and police equipment for control. Neither, if we recall table 1, can it be realistically argued that all security technologies should be controlled for export purposes. All states need to invest in critical infrastructure protection and given global interdependence, it is desirable, for example, that all states have adequate passenger and baggage screening equipment at airports. Global interdependence means that homeland security requires international cooperation and where necessary technology sharing (Committee on Homeland Security and Export Controls, 2012). Export controls can also have other unintended human rights impacts: expanding the definition of dual-use goods to include all potentially problematic cases can lead to humanitarian crises, as US abuse of the concept during the UN sanctions on Iraq between 1990 and 2003 showed (Gordon, 2010). It seems therefore more fruitful in the rest of this section, rather than proposing the control of all security technologies, instead to consider the way in which existing and potential control regimes could be amended or improved to close loopholes in this area, or to extend coverage to the most problematic technologies.

[I] The German position is significant as the German export control office (BAFA) is mandated by the EU to carry out projects aimed at enhancing international cooperation on dual-use controls. An overview of their activities can be found here: http://www.eu-outreach.info/eu_outreach/

[II] See 'Security made in Germany' for details of the more controversial German exports: http://www.german-foreign-policy.com/en/fulltext/57919?PHPSESSID=snktg8f7sg5f55goenjjb9lol4

5.3 Existing and Potential Control Regimes

The initial debate about controlling the exports on some types of security equipment has focussed on the EU dual-use regime. This is probably the most likely type of regime to be used in these circumstances and some progress has been made in the 2011 update process. Moreover, there is an ongoing consultation and review process of the regime. However, as has already been argued the classification of these technologies and products as dual-use is problematic under the current legislation and it may be that other types of regulatory framework are more appropriate. Similarly, it is already clear that there is some opposition to using the dual-use regime as a regulatory framework. While this sub-section looks in depth at the position with the dual-use regime, it also considers the relevance of the Common Position on arms exports, the Torture regulation, sanctions and embargos and industry-led self-regulatory frameworks.

5.3.1 EU Dual-Use Regulation

Technologies and goods that can be used for both civilian and military purposes are described as dual-use. The EU has agreed a dual-use export regime to control the export, transfer, transit and brokering of such items (Council Regulation 428/2009 which was amended in 2010, 2011 and 2012). Under the regime controlled items may not leave EU territory without a licence. With the exception of those items listed in annex 4, dual-use items can be traded freely within the EU. There are four types of export authorisation: community general export authorisations, national general export authorisations, global authorisations and individual licences. The EU list of controlled items is derived from the control lists adopted by the international export control regimes to prevent the proliferation of certain types of weapon – namely the Australia Group (biological and chemical weapons), the Nuclear Suppliers Group (nuclear weapons), the Wassenaar Arrangement (conventional weapons) and the Missile Technology Control Regime (unmanned delivery systems capable of delivering WMD). There are two aspects of the regime worthy of analysis; the listing system and the EU implementation procedures. As the EU lists represent a consolidated list, it is important to consider how the decisions on inclusion and deletion are taken. The sub-section will then look at the implementation system and efforts to reform it to counter some of the problems than emerged with exports to MENA.

While some types of unmanned aerial vehicles (and associated technologies) and some sensor technologies are covered by the MTCR, the most important regime for the purposes of this report is the Wassenaar Arrangement. The Wassenaar Arrangement is often neglected in accounts of the dual-use regime, as the political priority for some time has been the prevention of WMD not conventional weapons proliferation (Wetter, 2009) The criteria for the selection (or deletion) of goods for the Wassenaar lists are:

"Dual-use goods and technologies to be controlled are those which are major or key elements for the indigenous development, production, use or enhancement of military capabilities. For selection purposes the dual-use items should also be evaluated against the following criteria:

- *Foreign availability outside Participating States.*
- *The ability to control effectively the export of the goods.*
- *The ability to make a clear and objective specification of the item*
- *Controlled by another regime."* (Wassenaar Arrangement, 2005)

Immediately, the problems raised earlier about the control of security technologies as a group become clear. The concept is ambiguous, the technologies based largely on globally available generic technologies and they may not contribute to military capabilities. Evans (2008) argues that Wassenaar listing decisions are marked by a tension between those who view dual-use technologies as a problem of control and those who see them as a new market to exploit rather than control. Participating states agree to maintain export controls on all listed items but they make the decision whether to issue a licence or not. Information sharing modalities are also used to increase transparency. The Wassenaar dual-use lists are divided into the following categories:[I]

Category 1 Special Materials and Related Equipment
Category 2 Materials Processing
Category 3 Electronics
Category 4 Computers
Category 5 - Part 1 Telecommunications
Category 5 - Part 2 "Information Security"
Category 6 Sensors and "Lasers"
Category 7 Navigation and Avionics
Category 8 Marine
Category 9 Aerospace and Propulsion

Obviously, only a small percentage of the items that could be covered by these categories are controlled – most would fail to meet the criteria for listing. Nevertheless, some of the security technologies that were listed by ESRAB, such as hyperspectral and multispectral sensors, some encryption technologies and much of the technology and materials involved in the production of larger UAVs are included. Wagner (2012b) argues that EU cooperation with the Wassenaar partners could get more technologies included. This is probably possibly the case despite the listing criteria working against such inclusions. Moreover, national controls on additional technologies further to the EU lists are permitted.[II]

Attempts within the EU to strengthen the implementation of the dual-use regime have centred on the European Parliament. After the Lisbon Treaty came into force, updates to the dual-use lists, Community General Export Authorisations and any review of the regulation are subject to the co-decision procedure. In 2011 following reports of the misuse of surveillance and detection technologies in the Arab Spring, some MEPs[III] tried to use the update to the regulation to insert text into the Commission's legislative proposal strengthening the controls over these technologies. Jörg Leichtfried, the rapporteur for the International Trade committee on the Commission 2010 proposals to amend the dual-use legislation, proposed a number of amendments some to the text and some to strengthen parliamentary oversight of the dual-use regime,[IV] one of which was particularly important as far as surveillance technologies are concerned, and was accepted by the Council. The EU General Export Authorisation for telecommunications was amended to read that

[I] The Wassenaar Agreement also includes the munitions list which is the equivalent of the EU Common Military List, and two annexes - the sensitive and very sensitive lists. These annexes represent nested sub-sections of the main categories and include technologies that it is agreed are critical and where greater levels of information sharing on licensing decisions are required, and in the case of the very sensitive list participating states agree to exercise extreme vigilance.

[II] Article 8 of Council Regulation 428/2009 allows member states to unilaterally impose restrictions on unlisted items on the human rights or public security grounds. France, Germany, Latvia and the UK have taken advantage of this measure. Details are available in the Official Journal of 6 March 2012.

[III] Some of the most active were Dutch MEPs Marietje Schaake and Lambert van Nistelrooij, Jörg Leichtfried from Austria and Vital Moreira from Portugal.

[IV] A proposed general export authorisation for computers was also deleted. The full list of amendments can be viewed at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2011-0028&language=EN

the export was not authorised if the exporter was aware that the equipment could be used for (or had been warned that this was the case by the member state):

"for use in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use (e.g. via Monitoring Centres and Lawful Interception Gateways);" (Regulation 1232/2011 Annex IIe Part 3 1(1)(d))

While the destinations that the general export authorisation applies to do not include any of the Arab Spring countries, it does include countries like Russia and China, who are known to engage in such practices. It also sets a useful precedent for further changes. Leichtfried claims to have been surprised at the extent of the hostility towards some of his other amendments.[I]

In June 2011 the Commission issued a Green Paper on the reform of the dual-use regime and launched a consultation. The thrust of the Green Paper is towards greater harmonisation and for general export authorisations to be at the EU not the national level. It is argued that firms whose states preserve stricter understandings of catch-all clauses are disadvantaged. Broadly speaking the Commission approach is towards greater liberalisation rather than restriction. Greater harmonisation has been opposed by both the UK and Germany in their submissions as unnecessary. According to the Gemeinsame Konferenz Kirche und Entwicklung (GKKE) group (2012), which contributes an annual report on German arms export policy, the only measure that the German government supported with enthusiasm in the Green Paper was speeding up the updating procedure for the regulation, which would diminish the ability of the European Parliament to amend the legislation. The Netherlands is also sceptical about the need for major change and the extension of EU general export authorisations, but would favour the introduction of an EU level catch-all clause to harmonise implementation (Bleker, 2011).

The consultation has seen a number of proposals that may help tighten export controls of security technologies if accepted. The UK has proposed in its submission that the definition of military end-use in Article 4(2) of Council Regulation (EC) 428/2009 be amended to read *"intended for military, paramilitary, security or police forces in a destination subject to an arms embargo or to an entity involved in procurement, manufacture, maintenance, repair or operation on their behalf."* Their justification is that the current control is too narrow. Their legal advice suggests that under the current wording they cannot prevent the export of complete items which are to be used as complete items. *"For example, we could prevent the export of an unlisted item intended to be used as a component in a military vehicle but we could not prevent the export of a complete civilian vehicle that was to be used by the military or internal security forces of the destination country even where that country is subject to arms embargo. It is also unclear whether the military end-use control permits us to prevent the export of an unlisted item that is to be modified for military purposes, either in the destination country or in an intermediate destination"* (House of Commons, 2012). Such an amendment would extend the understanding of military end-use to include internal security forces, which could be helpful. Vranckx, Slijper and Isbister (2011) make a similar suggestion arguing that an unlisted item that was to be converted for military or security use should be covered if either the state or the firm knew about it. This is however a complex problem as one recent case shows. Engines made by German firm 3W Modellmotoren appear to have been resold by dealers, without the firm's knowledge, to Belarus where they are being used to power

[I] Leichtfried's comments in 2012 can be viewed here: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20120208-1630-COMMITTEE-AFET

spy drones, despite an EU embargo from 2011 preventing the sale of technologies that could be used for internal repression (Nielsen, 2012b). Bromley (2012) has recommended new controls on exports of surveillance technologies within either the dual-use regime or common position reviews. All of these suggestions would potentially enable action to be taken on the exports of some types of security technologies, but these suggestions are only suggestions and run contrary in some cases to the Commission proposals.

5.3.2 Common Position on Arms Exports

Since 2008, the EU has had a Common Position outlining the rules on the control of exports of military technology and equipment across the EU. This is the successor to the Code of Conduct on arms exports agreed in 1998. The harmonisation of arms exports controls during the last fifteen years has not just been about establishing minimum standards throughout the EU but also about greater information exchange and transparency between member states. In comparison to the Code of Conduct the Common Position is legally binding. Goods named in the EU Common Military List[I] require licenses if they are to be exported. Decisions on licensing must consider the eight criteria detailed in table 5.1.[II]

Table 6 Common Position Criteria

Criterion	Description
1	Respect for the international commitments of EU member states, in particular the sanctions decreed by the UN Security Council and those decreed by the Community, agreements on non-proliferation and other subjects, as well as other international obligations
2	Respect of human rights in the country of final destination
3	Internal situation in the country of final destination, as a function of the existence of tensions or armed conflicts.
4	Preservation of regional peace, security and stability
5	National security of the Member States and of territories whose external relations are the responsibility of a Member State, as well as that of friendly and allied countries
6	Behaviour of the buyer country with regard to the international community, as regards in particular its attitude to terrorism, the nature of its alliances and respect for international law.
7	Existence of a risk that the military technology or equipment will be diverted within the buyer country or re-exported under undesirable conditions.
8	Compatibility of the exports of the military technology or equipment with the technical and economic capacity of the recipient country, taking into account the desirability that states should meet their legitimate security and defence needs with the least diversion of human and economic resources for armaments

Source: Cooper (2012: 11)

Member states must consider any denials of licenses for the same equipment within the last three years, and must provide an annual report on their licensing decisions. The Common Position is

[I] The Common Military list can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:069:0019:0051:EN:PDF

[II] Article 12 of Regulation 428/2009 (dual-use regime) states that licensing decisions on dual-use exports must also respect these criteria.

considered an advance on the Code of Conduct because in addition to being legally binding, it also includes measures on brokering, transit transactions and intangible technology transfers. While the Common Position applies to military not security technologies (unless listed as dual-use) it is interesting for several reasons.

Firstly, there is Article 6, which makes it clear that exports to internal security forces and similar entities are covered as well as the military:

"Without prejudice to Regulation (EC) No 1334/2000, the criteria in Article 2 of this Common Position and the consultation procedure provided for in Article 4 are also to apply to Member States in respect of dual-use goods and technology as specified in Annex I to Regulation (EC) No 1334/2000 where there are serious grounds for believing that the end-user of such goods and technology will be the armed forces or internal security forces or similar entities in the recipient country. References in this Common Position to military technology or equipment shall be understood to include such goods and technology." (Council of the European Union, 2008c)

Secondly, a small number of technologies listed in table 1 as security technologies figure in the common military list, with the caveat that they are only covered if specifically designed or modified for military use. The most obvious examples are unmanned aerial vehicles and some types of CBRN equipment. If the Commission (2012a) pushes forward its plans for hybrid military and security standards for some types of products as suggested in its security industrial policy communiqué, presumably products intended for civilian users would also be covered. Similarly, the joint research work between the EDA and Commission under Framework Cooperation could have similar results. Thirdly, and perhaps most straightforwardly, it does not preclude member states from adopting stricter national controls. The UK, for example, has added some items of equipment that it describes as security, paramilitary and police goods to its national military list.[I] This is an avenue that concerned member states could follow if there is no consensus at the EU level.

The Common Position is also undergoing a review process as foreseen in the initial decision. While this need not necessarily entail revisions, Bromley (2012) states that a number of items have been placed on the agenda as a result of EU states aligning their positions on the proposed UN Arms Trade Treaty, including enhanced consultation mechanisms for problematic destinations; how data for the EU annual report should be submitted; the national implementation of controls on transit, transhipment and brokering at the national level; how COARM functions; what information should be shared on license denials and the use of global and general licences. Many of the NGO proposals for reform share these concerns, centring in particular on the need for more uniform

[I] The UK has added the following goods to its military list for example: "Other security and para-military police goods as follows:

a. Acoustic devices represented by the manufacturers or suppliers thereof as suitable for riot control purposes, and specially designed components therefor;

b. Anti-riot and ballistic shields and specially designed components therefor;

c. Shackles designed for restraining human beings having an overall dimension including chain, when measured from the outer edge of one cuff to the outer edge of the other cuff, of between 240mm and 280mm when locked;

d. Electric–shock belts designed for restraining human beings by the administration of electric shocks having a no-load voltage not exceeding 10 000 volts;

e. Water cannon and specially designed components therefor;

f. Riot control vehicles which have been specially designed or modified to be electrified to repel boarders and components therefor specially designed or modified for that purpose;

g. Electric-shock dart guns having a no-load voltage not exceeding 10,000 volts;

h. Components specially designed or modified for portable devices designed or modified for the purposes of riot control or self-protection by the administration of an electric shock (e.g., electric-shock batons, electric-shock shields, stun-guns and electric-shock dart-guns)." (BIS, 2012)

implementation and greater transparency about licensing approvals and denials. Depauw (2010) for example points out that with the introduction of the ICT directive, it is unclear how states will be able to prevent re-exports of military equipment initially sold to other member states if they disapprove of the re-export. If all states are not using the criteria in the same manner then problems of undercutting are likely to arise. Analysts have also been keen to draw lessons from the questions raised during the Arab Spring about the robustness of EU arms export procedures, proposing that a new criterion could be added to explicitly consider poor governance as a risk factor, that a list of countries of concern could be agreed and that special arrangements could be made after the lifting of an embargo (Vranckx, Slijper and Isbister, 2011; Bromley, 2012). While these may not cover security technologies, there are connections between the regimes, and changes in one setting may prove helpful precedents in other debates.

The EU also could lobby for some technologies to be added to the Wassenaar lists. Where surveillance technologies of the type used in the Arab Spring are concerned Munitions List 11a (c) *"Electronic systems or equipment, designed either for surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purposes or for counteracting such surveillance and monitoring;"* would seem to be potentially useful as a starting point for discussion. Within the EU context given the concerns of the Commission and some member states about regulation in this context disadvantaging EU firms, attempts to add some technologies to the Wassenaar regime might be more acceptable.

5.3.3 The EU Torture Regulation

As had already been mentioned, initial plans to include a security and police equipment list in the Code of Conduct on arms exports failed. There was however agreement to accept a Commission proposal to regulate the exports of items that could be used for torture of other cruel, inhuman and degrading treatment. This was in line with guidelines on policy towards third countries committing acts of torture agreed in 2001. These guidelines did not create legal obligations but rather expressed a political commitment on the part of the EU to the global campaign against torture. While early reviews (Council of the EU, 2008a) suggested that the effect of the guidelines had not been as comprehensive as hoped, one result was the adoption of EC Regulation 1236/2005, generally known as the Torture Regulation. The regulation banned trade in some goods used to restrain or execute humans, and introduced controls on the export of other items which could be used for torture. While the lists in both cases are short, it remains a good example of a decision to restrict exports of certain security-related products even though there is no military connection and thus is of interest to this report. The regulation's scope is outlined below and then the strengths and weaknesses are discussed.

The regulation, revised in 2011, prohibits the import and export of the following items listed in Annex 2:

1. **Goods designed for the execution of human beings, as follows:**

    1.1. Gallows and guillotines
    1.2. Electric chairs for the purpose of execution of human beings
    1.3. Air-tight vaults, made of e.g. steel and glass, designed for the purpose of execution of human beings by the administration of a lethal gas or substance
    1.4. Automatic drug injection systems designed for the purpose of execution of human beings by the administration of a lethal chemical substance

2. **Goods designed for restraining human beings, as follows:**

2.1. Electric-shock devices which are intended to be worn on the body by a restrained individual, such as belts, sleeves and cuffs, designed for restraining human beings by the administration of electric shocks having a no-load voltage exceeding 10 000 V

3. **Portable devices allegedly designed for the purpose of riot control, as follows:**

3.1. Batons or truncheons made of metal or other material having a shaft with metal spikes

The rationale for banning these products from export is that they cannot be used for any purpose other than torture or inhuman, cruel or degrading treatment. NGOs successfully argued for the 2011 addition of spiked batons and truncheons on this basis (Amnesty International and Omega Foundation, 2010). Annex 3 contains a list of specific products under the following headings:

- Goods designed for restraining human beings
- Portable devices designed for the purpose of riot control or self-protection
- Portable equipment for dissemination of incapacitating substances for the purpose of riot control or self-protection and related substances
- Products which could be used for the execution of human beings by means of lethal injection.

These products must be licensed on a case-by-case assessment basis for export and licensing authorities should consider the likelihood of misuse by the recipient state. Member states should also take into account any refusal of a license by other member states in the preceding three years in making their decision. This information is not made public by most member states, but from a sample of six states that did, Amnesty International and Omega (2010) point out that between 2006 and 2008 both the Czech Republic and Germany have supplied security-related equipment that could be used for torture to countries that are known to commit human rights abuses.

There are known problems with the regulation. Alongside the lack of transparency, the regulation suffers from the problems of all list-based controls. As an NGO report points out;

"List-based systems provide clarity for exporters and importers, but on their own can have inherent weaknesses, including:

- *Not controlling a range of products even though they fall within the intended scope of the agreement, because they are not specifically named on the control lists;*

- *The delay often experienced between the manufacture, transfer and use of newly designed equipment, and the time taken for it to be added to a control list;*

- *The potential for suppliers to evade controls simply by re-naming or re-specifying their products." (Amnesty International and Omega Foundation, 2010: 28)*

Since 2008, the UK has been a supporter of the introduction of a torture end-use catch-all clause at the EU level, which would allow a member state to license and thus ban any item that could be used for torture. Correspondence between the UK government and Baroness Ashton from 2011, published by the UK House of Commons Committees on Arms Exports Controls in 2012, suggests a review of the scope of the legislation is taking place (House of Commons, 2012 – written evidence

142). However, there is growing NGO and parliamentary pressure, particularly in the UK, for supportive states to introduce such measures unilaterally, in the belief that there is not sufficient support for the measure across the EU.[I] While not unproblematic, the Torture Regulation nevertheless does offer a precedent in the restriction of non-military security-related goods at the EU level, and could serve as a model for banning what Wagner (2012b) describes as the worst of the worst technologies: single use technologies whose only purpose is repression.

5.3.4 Sanctions and Embargos

Since late 2011 the EU has increasingly included specific clauses in its sanctions and embargos to cover surveillance technologies. In December 2011, the Council of the European Union passed additional sanctions, to ban "equipment and software intended for use in the monitoring of the Internet and telephone communications" (17985/11) from entering Syria. Moreover on 23 March 2012, in response to the use of the technologies in acts of repression, the EU broadened sanctions on Iran by adopting Council Regulation 264/2012, which prohibits the sale, supply, transfer or export to Iran of equipment and technology that could be used for monitoring and interception of internet and telephone communications. This includes the provision of technical assistance. The US White House went a step further in April 2012 by announcing targeted financial sanctions against firms selling surveillance technologies to Iran and Syria.[II] These moves have almost certainly come in response to sustained media and parliamentary pressure on the issue.

Do sanctions offer a satisfactory answer to this problem? Wagner (2012b) suggests that they are best seen as a short-term solution to stopping the worst types of surveillance technologies reaching regimes actively engaged in internal repression. It is generally faster to agree a sanction than it is to amend a multilateral export control regime. However, the grey areas between acceptable and unacceptable technologies make such sanctions permeable and difficult to police. Another potential issue is that crackdowns of this nature often appear dependent on the vigour of the media, politicians and NGOs in exposing abuses. The disadvantage here is that this means disproportionate attention can be paid to some abuses deemed newsworthy, while others, equally as severe, go unnoticed. Had the Arab Spring and Iranian protests not been framed as being about the use of social media to organise protest, would surveillance technology exports have gained such attention? This may also mean that only certain countries are targeted leading to problems of inconsistency. For example, Reporters without Borders (2012) named Vietnam (along with Syria and Iran) as one of the twelve countries deemed to be enemies of the internet, but in June 2012 the EU signed a Partnership and Cooperation Agreement with Vietnam marking an upgrade in the relationship. Country-specific rather than general bans also mean that it is difficult to prevent re-exports from third countries.

5.3.5 Industry-led Voluntary Codes

Despite much negative publicity about firms exporting arms to inappropriate recipient states, the firms involved appear to take the view that so long as their trade is legal and government-supported, then public reputational damage through association with human rights abuse is less

[I] In response to NGO and media pressure the UK has introduced unilateral controls in 2011 on the supply of drugs to the US that could be used to carry out the death penalty, and previously on sting sticks and electro shock devices (House of Commons, 2012).

[II] The White House Executive Order of 23 April 2012 can be viewed at: http://content.govdelivery.com/attachments/USTREAS/2012/04/23/file_attachments/108232/2012iransyria.eo.rel.pdf

important. After all their business is with governments not the general public. Reputational damage for firms that do rely on their brand perception to support non-governmental sales is much more serious. For example, allegations in July 2011 that British newspaper 'News of the World' had illicitly accessed the mobile phone voice messages of a murdered schoolgirl led to a highly successful social media campaign to force other firms to withdraw advertising from the paper. Israel (2009) suggests that ICT companies are particularly vulnerable to reputational damage because their most valuable assets are their brand and human capital. Given this, and an industry preference for avoiding government intervention, it is unsurprising that various government-backed stakeholder initiatives on ICT and human rights have emerged in a similar vein to the Kimberley Process on conflict diamonds. They also form a response to the UN Guiding Principles on Business and Human Rights which were endorsed by the UN Human Rights Council in 2011.

Perhaps the most visible of these efforts is the Global Network Initiative (GNI). This was launched in 2008 after two years of collaboration between three leading ICT companies (Microsoft, Yahoo and Google), human rights investigators, academics and investors to agree an approach. It represented a response to criticism of ICT firms for restricting internet freedom especially in China and to what at the time looked like potential legislation in the US Congress (Israel, 2009). Membership commits a firm to the GNI principles and to independent assessment of its compliance. However, GNI has met with criticism from Amnesty International, which was involved in the talks but did not join claiming the regime was too weak, and from business commentators who point to the fact that no other major ICT firms have joined claiming the regulatory burden is too onerous (Downes, 2011). A group of predominantly European telecommunications companies are also engaging in an Industry Dialogue on issues of privacy and free expression. Finally, in response to the issues raised about ICT and repression during the Arab Spring the European Commission is developing a 'No Disconnect' strategy based on the following four aims:

1. ***"Developing and providing technological tools*** *to enhance privacy and security of people living in non-democratic regimes when using ICT.*

2. ***Educating and raising awareness of activists about the opportunities and risks of ICT****. In particular assisting activists to make best use of tools such as social networks and blogs while raising awareness of surveillance risks when communicating via ICT.*

3. ***Gathering high quality intelligence about what is happening "on the ground"*** *in order to monitor the level of surveillance and censorship at a given time, in a given place.*

4. ***Cooperation****. Developing a practical way to ensure that all stakeholders can share information on their activity and promote multilateral action and building cross-regional cooperation to protect human rights." (EU press release, 2011)*

Wagner (2012b) points to the Institute for Human Rights and Business which is developing self-regulatory stakeholder guidance on the respect of human rights for the ICT sector on behalf of the Commission as an example of the work behind this approach.

While corporate social responsibility is to be encouraged, and guidance for firms exporting all manner of security technologies (not just ICT) on human rights issues is to be encouraged, given the current unclear legal situation on export controls, these initiatives are unlikely to be sufficient. Wagner (2012b) argues that they should be seen as helpful steps in conjunction with legislative action. Reputational damage is recoverable, and there are ways to minimise it such as the use of

subsidiary companies to do business that may prove problematic. Without the fear of legal consequences, and greater transparency around exports, scandals are likely to reoccur.

5.4 Is Control Needed?: The External Aspects of the EU Internal Security Strategy

The 2010 EU Internal Security Strategy states that:

"A concept of internal security cannot exist without an external dimension, since internal security increasingly depends to a large extent on external security. International cooperation by the EU and its Member States, both bilaterally and multilaterally, is essential in order to guarantee security and protect the rights of our citizens and to promote security and respect for rights abroad."(Council of the European Union, 2010: 16).

This statement implicitly recognises the interdependence of contemporary global security. If international passenger flights are to be made secure for example, it is clear that the more sensible option is, rather than banning flights from any country deemed a terrorism concern, instead to ensure that the country can acquire advanced passenger and freight screening technology. The same logic applies for much counter-terrorism, migration and international crime cooperation with third countries – technology will need to be shared if the EU is to meet its policy objectives. However, while the Internal Security Strategy's goals and indeed those of the Stockholm Programme are dependent on agreements with third countries, as Monar argues, *"The negotiation of such agreements can be difficult because third countries often do not meet EU standards in terms of respect of fundamental rights, judicial procedures and data protection."* (Monar, 2010: 32)

This tension is at the crux of the difficulties that the EU faces regarding the export of security technologies. It is further intensified by the EU's neighbourhood policies, which have put emphasis on stability in the EU neighbourhood at the expense of democracy promotion (Youngs, 2002) meaning that the EU has had to and will have to deal regularly with problematic actors, where human rights are concerned. Finally, in line with the EU's general stance on free trade, insofar as the EU and its member states can be said to have a common policy towards the security industry, it has been assumed that export potential would be strong (Schumann, 2011; European Commission 2012a).

Let us unpack the nature of these dilemmas by drawing on an example. Counter-terrorism cooperation with third countries, whose human rights records are problematic, is always a difficult balancing act between the desire for security and the desire to promote human rights. For example, the EU-Egypt Action Plan from 2010 stated that the EU and Egypt would cooperate on fighting *"the use of the internet for terrorist purposes"* and that the EU would support capacity building in the *"technological capabilities of law enforcement institutions"* (European Commission, 2010: 31). But this inevitably means internet filtering and blocking and it was widely known that Egypt suppressed freedom of expression through surveillance across communications mediums (Wagner, 2012b). It is not clear in this case that EU human rights and counter-terrorism aims are compatible.

The European Commission (2012b) has also defined cybercrime as a major security issue. Recognising it as the ultimate borderless crime, the need for international partners is clear.

Commission proposals over the last decade to improve the policing of terrorist radicalisation on the internet or to prevent the sharing of internet child pornography are often dependent on internet filtering or forcing internet providers to share the browsing history of their subscribers. These technologies are available and in use in the EU itself.[I] If cybercrime is to be successfully countered, then third countries would need to be enabled to access such technology. This would seem to legitimate the export of such security technology, but it is precisely the usage of these systems to track activists during the Arab Spring that has proved so controversial (Valentino-Devries et al, 2011).

Another example is border management. The EU's own proposed border management plan, EUROSUR and the Smart Borders initiative, involves mass use of surveillance technologies including the use of UAVs for monitoring the Mediterranean. A driving aim behind the initiatives is a response to the border 'crisis' caused by the Arab Spring, when many people sought refuge from the fighting in the EU. The aim is not just to track migration and visa abuses much more strictly but also to create buffer zones for the policing of migrants outside EU territory. It is therefore dependent on the cooperation of third countries and the sharing of personal data about migrants and the technology to monitor migration with them. In an extremely critical report on the proposals for EUROSUR and Smart Borders, Hayes and Vermeulen (2012) allege that the plans contravene the Universal Declaration of Human Rights as EU cooperation agreements with third states amount to a ban on unauthorised departure and thus a negation of the right to seek asylum. It is also a questionable use of development aid. Vranckx, Slijper and Isbister (2011) also point out that there is an impact on related export licensing decisions as supplying sophisticated and integrated border surveillance systems has become important for firms like EADS, who, for example, have won the initial contracts for such a system in Saudi Arabia, supported by training from the German police. It is suggested that gaining an export licence for such systems is fairly straightforward as a relatively small percentage of the technology needs a licence and not much of it is military. Vranckx, Slijper and Isbister (2011: 34) argue that licensing sales of "*border control technology is perceived in many of the licensing countries as supportive to their attempts to control migration and influxes of refugees"* and thus to support FRONTEX, the EU border control agency, in its work. This means that human rights concerns, such as the treatment of migrants and refugees in that state, might be deemed less important in licensing decision-making. These are not dilemmas unique to the EU. The US is also facing problems reconciling the need to cooperate internationally and share technology to meet its homeland security goals, with its preference to operate a restrictive export control system (Committee on Homeland Security and Export Controls, 2012).

[I] A European Court of Justice ruling in 2011 banned the use of generalised internet filtering but more targeted activity is still taking place.

5.5 Summary

This section has argued that the introduction of export controls on security technologies is going to be difficult even after the publicity given to the misuse of surveillance and detection technologies during the Arab Spring. It has argued that the concept of security technology is ambiguous and so difficult to classify, based frequently on globally available generic technologies and in some cases there is no need for control. It also argued that there were few grounds beyond human rights concerns for governments and the EU to favour restrictions and arguments in favour of avoiding them. It was pointed out that the way the debate was framed was very different to the framing of discussions on arms exports, and that this could make it more difficult to draw on those frameworks as the basis for legislation.

The section went on to discuss the existing coverage and the potential for changes / introduction of controls in the following frameworks:

- EU dual-use regime
- Common Position on arms exports
- Torture regulation
- Sanctions / embargos
- Industry-led initiatives

While the legal position on the controls of security technologies is undeniably patchy and unclear, it seemed that there was no straightforward solution. The major gap emerging from the Arab Spring appears to be the lack of controls on exports of surveillance technologies, but the older disagreement around export controls on policing equipment means that items used for repression such as water cannons and electro shock guns are only controlled if a member state chooses to do so nationally. While sanctions offered a short term solution, it appeared that the best way in the medium term to control exports was through the dual-use regime. The Torture Regulation offered a precedent for a regulation to ban what Wagner (2012b) describes as single-use products whose only purpose was repression.

Finally, the section discussed the external requirements of the EU's internal security policy commitments particularly on transnational crime, counter-terrorism and border management. These require cooperation and technology sharing with third countries to be successful. Some of these countries do not have good human rights records. The technology needed is the sort of surveillance and detection equipment that is prone to misuse. This means that any controls on the exports of security technologies could potentially lead to the EU being unable to implement some of its internal security plans (whether this is a bad thing is a different question).

6 Conclusions

As Edler and James (2012) argued, the European Commission has acted as a policy entrepreneur in opening up a new EU policy field around security industry and technological development. Initially, its mandate was unclear and it did not enjoy full support from either industry or member states. The interviews carried out for this report showed that although the security research programme was a success in many ways, there is a residual discomfort about the Commission's activism. Edler and James (2012) have suggested that the failure to agree on funding defence research in the Horizon 2020 research funding programme indicates limits to the Commission's ability to expand their role further. Moreover, the Commission claims that there is no real difference between security and defence industry, technologies and user requirements have been questioned by a number of reports (including this one), which have suggested that particularly among users' requirements there are still significant differences. There are though clearly linkages between security and defence (or internal and external security) technologies and industries, not least because of EU policy actions, which have tried to increase the blurring between the two. One under-researched linkage is the question of export controls: the Arab Spring drew public and political attention to the inadequacy of controls over EU exports of security technologies.

The report began by posing the following research questions:

- How has the concept of security changed in the post Cold War era? And how has this been interpreted in the EU?
- What is the security market? What are the parameters that determine its technologies and supply and demand side? Can these be differentiated from the more established defence technologies, firms and customers/ users?
- What are the European policy initiatives in this area and what is driving them? What impact are they having on the market? Who are the policy entrepreneurs – the EU institutions or the member states? Are the different policy aims coherent? Is it beneficial or problematic to conflate defence and security? What impact do the security industrial and technological issues have on other EU policies?
- Finally, the place of security technologies in the strategic export control system needs analysis. Do existing regimes cover security technologies? Should security technologies be controlled? What are the ethical issues?

It is worth briefly reviewing the findings of each section in response to these questions.

In response to the first group of questions, it is undeniable that the concept of security has changed following the end of the Cold War. An academic debate on the concept of security has been picked up by policy-makers and the definition of security threats is no longer confined to external military threats. One highly important development in this context has been the emergence of the concept of homeland security. This US concept has been adopted within the EU as a whole, but most particularly within the European Commission's agenda. Arguably, the emergence of homeland security gave the Commission another potential entry point into the security and defence field, which member states have preferred to keep intergovernmental. This has led to some unusual policy dynamics, whereby it has been in the Commission's interests to stress the extent of blurring between internal and external security needs, suppliers and technologies.

The Commission has chosen to define the security market fairly narrowly, concentrating on certain types of products thought to be attractive to government customers. This has led to policies that critics argue favour defence firms over non-defence suppliers. The report asked whether you could still differentiate between defence and security technologies, firms and customers. Both types of technologies draw heavily on the same generic civilian technologies and there is a degree of overlap, although this can be overstated. Moreover, even the European Commission (2012a) now accepts that the firms researching and producing defence and security technologies are not identical. Although the type of security market that the Commission thought would emerge, would resemble the defence market, which would favour the defence firms, this has not yet emerged and at present there are non-defence firms involved in the security market, particularly in areas like telecommunications and surveillance. Additionally, not all defence firms see the security market as the most promising area to diversify into, while others have adopted holding strategies rather than committing themselves. Thirdly, the report argued that although there were overlaps between military and civilian security tasks and thus requirements, there were few signs of a unified government customer emerging (not even in the shape of a single national civilian security customer). This was because requirements and expectations are not identical, and there was little to tempt civilian customers to adopt the military procurement model, which was viewed as inefficient. Finally, it was suggested that high profile failures of large security projects in both the US and UK, might make other states cautious about embarking on such projects, particularly at a time of cuts to government spending. This meant that the demand side was not as strong as the Commission had thought.

Section 4 outlined the current policy initiatives in Europe concerning security and defence industry. With the exception of the Franco-British agreements, these were being pursued by the EU institutions. The balance of the evaluation was that the EDA was hampered by having been given a near impossible task of reforming the EDITB without sufficient funding or support, while the Commission's policies seemed to vacillate between liberalisation of defence and security trade internally and externally, and active industrial policy measures to support industry. The report argued though that the Commission's inability to act as a customer meant that they could not manage the sector as effectively as they might like. There are limits to their ability to counter the lagging demand in member states for these technologies. The Commission's entrepreneurial approach to policy development was evident by their activism in a number of policy fields, particularly border controls that could be linked to security and defence technologies in an effort to overcome this. It was also noted that internal security policies seemed to be developing certain emphases that did not fit well with the human rights-based approach of EU foreign policy. Similarly, the Commission appears to be overly optimistic about the enthusiasm for security technologies from the member states and EU citizens. These problems mean that the global export market plays a larger role in Commission plans for the security industrial sector than might have been expected.

Finally, the report considered security technologies and export controls, an issue that had gained political salience following media coverage of the misuse of surveillance and detection technologies during the Arab Spring. The emergence of these 'remote' technologies is arguably the most important part of the new security sector, as it is in these technologies that the potential for the blurring of internal and external security or security and defence is at its strongest. They also constitute the group of technologies that are crucial to the growth of the homeland security state. This raises many ethical dilemmas for internal policies, but the report has concentrated on the dilemmas they pose to EU external relations.

The externalisation of the EU's internal security concerns through the external dimension of the Area of Freedom Security and Justice means that policy success in areas such as border control

depends on the export of these technologies to neighbouring states. The report argued that this inevitably led to difficult ethical problems in finding a balance between concerns about misuse and policy effectiveness. These ethical dilemmas were vividly portrayed in the Arab Spring where regimes trying to repress protesters misused surveillance technologies sold to them by European exporters.

Turning to the question of controlling the export of security technologies, the report argued that this was an issue where an EU consensus would be hard to reach. Some member states share the Commission's view that security technologies should be a growing export market for European firms. Others are keener to extend export controls. There is a longstanding division on whether policing equipment that could be used for repression and human rights abuse should be controlled, which is why such items were not included in the initial Code of Conduct on arms exports, and instead a shorter list became the basis for the Torture Regulation. The report noted however, that legally there were a number of possibilities for member states to take unilateral action, and that some had. The issue is made more complex in that it is not possible to treat all of the technologies designated by ESRAB (2006) as security technologies as one group. Some are already covered by the military or dual-use lists. Others offer little potential for misuse. The biggest gap appears to be around remote or surveillance and detection technologies.

The report considered the following alternatives for extending export controls to cover these security technologies:

- EU dual-use regime
- Common Position on arms exports
- Torture regulation
- Sanctions / embargos
- Industry-led initiatives

It concluded that while this new group of remote technologies also highlights the growing complexity of the dual-use regime and how dual-use could and should be interpreted, that this was the best medium-term option for control. It also suggested that the Torture Regulation offered a model for banning the export of some surveillance technologies that Wagner (2012b) argued could only be used for repression. The report found that sanctions and industry-led initiatives were unlikely to be robust enough to offer long-term solutions.

In summary, it can be argued that while the Commission's starting point was that security and defence industry, technology and requirements were essentially interchangeable, this is in fact not the case. The Commission's policy entrepreneurship has enabled it to open up a new policy field with speed, but there seems to be a disconnect between the Commission and the member states on the question of what technologies are wanted, and a more serious potential gulf between the Commission and EU citizens on what security technologies are acceptable. This mirrors the situation in the US, and it is hoped that transatlantic lessons can be learnt to avoid wastage of scarce resources. The Arab Spring has also reminded the EU that certain gaps were left in its export control regime, and that one of them is the control of some types of security technologies. While the external needs of the EU internal security policy field are undoubtedly important, the ethical issues that they raise cannot be ignored by sensible policymakers.

7 Bibliography

Akkermann, Mark (2012) Militarisering van Security Inventarisatie Nederlandse bedrijven, Amsterdam, Campagne tegen Wapenhandel, November 2012: available at http://stopwapenhandel.org/sites/stopwapenhandel.org/files/cybersecurity_final.pdf (accessed 14 November 2012)

Amnesty International (2011), Arms for Internal Security: Will they be covered by an Arms Trade Treaty?, London, Amnesty International

Amnesty International and Omega Research Foundation (2010), From Words to Deeds: making the EU Ban on the Trade in 'Tools of Torture' a Reality, London, Amnesty International

Archick, Kristin (2011) US-EU Cooperation against Terrorism, CRS Report for Congress RS22030, Congressional Research Service, Washington

ASD-Europe (2011) Facts and Figures 2010, available at: http://www.asd-europe.org/site/fileadmin/images/publications_thumbs/FF2010.pdf

Auswärtiges Amt (2012) Deutsch-Französische Erklärung: Für eine stärkere europäische Sicherheit und Verteidigung, Paris, 6 February 2012 http://www.auswaertigesamt.de/cae/servlet/contentblob/608180/publicationFile/164316/120206-D-F-Sicherheitserklaerung.pdf

Ayoob, Mohammed (1997) 'Defining Security: A Subaltern Realist Perspective', in Keith Krause and Michael Williams (eds.) Critical Security Studies: Concepts and Cases, UCL Press, London: 121-147

Baldwin, David (1997) The Concept of Security, Review of International Studies, 23(1997): 5-26

Bailes, Alyson (2008), 'The EU and a 'Better World': What Role for the European Security and Defence Policy?', International Affairs, 84(1): 115-30

Bailes, Alyson (2004), 'Preface', in Sybille Bauer and Mark Bromley, The European Union Code of Conduct on Arms Exports, SIPRI Policy Paper No. 8, Stockholm: SIPRI

Bauer, Sibylle (2003) The EU Code of Conduct on Arms Exports-Enhancing the Accountability of Arms Export Policies?, European Security, 12(3/4): 129-48

Beidel, Eric (2011) Homeland Security Market Vibrant despite Budget Concerns, National Defense, September 2011: http://www.nationaldefensemagazine.org/archive/2011/September/Pages/HomelandSecurityMarket%E2%80%98Vibrant%E2%80%99DespiteBudgetConcerns.aspx

Bellavita, Christopher (2008) Changing Homeland Security: What is Homeland Security?, *Homeland Security Affairs*, 4(2): 1-30

Bigo, Didier (2002) Security and Immigration: Toward a Critique of the Governmentality of Unease, *Alternatives,* 27(1): 63-92.

Bigo, Didier and Julien Jeandesboz, (2010), *The EU and the European security industry questioning the 'public-private dialogue'*, INEX Policy Brief no. 5/February 2010.

BIS (Department for Business, Innovation and Skills), (2012) *UK Strategic Export Control Lists: The consolidated list of strategic military and dual-use items that require export authorisation*, London, August 2012, available at: http://www.bis.gov.uk/assets/biscore/eco/docs/control-lists/12-1014-uk-strategic-export-control-list-consolidated.pdf (accessed 13 August 2012)

Bleker, Henk (2011) *Kabinetsreactie Groenboek exportcontrole dual-usegoederen*, Ministerie van Economische Zaken, Landbouw en Innovatie, Den Haag, 20 September 2011

Bossong, Raphael (2008) The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance, *Journal of Common Market Studies*, 46(1): 27-48

Briani, Valerio and Nicolo Sartori (2011) Transatlantic Industrial Policies in the Security Sector, in *EU-US Security Strategies: Comparative Scenarios and Recommendations*, Issue 3: 156-66 Available at: http://csis.org/files/publication/110614_Conley_EUUSSecurity_WEB.pdf

Bromley, Mark (2012) *The review of the EU common position on arms exports: prospects for strengthened controls*, Non-Proliferation Papers No. 7 January 2012, EU Non-Proliferation Consortium, Available at: http://www.sipri.org/research/disarmament/eu-consortium/publications/publications/non-proliferation-paper-7 (accessed 7 May 2012)

Brunnstrom, David and Anna Ringstrom, (2011) Sweden blocked an effort by other EU states to add two telecoms firms in Syria with commercial links to Swedish firm Ericsson to an EU sanctions list this week, EU diplomats said, Reuters, 2 December 2011, available at: http://www.reuters.com/article/2011/12/02/us-eu-syria-sweden-idUSTRE7B120J20111202 (accessed 7 May 2012)

Bundesministerium für Wirtschaft und Technologie (2010), *Zukunftsmarkt zivile Sicherheit: Industriepolitische Konzeption des Bundesministeriums für Wirtschaft und Technologie*, Berlin, November 2010

Buzan, Barry (1991) People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, Lynne Rienner, Boulder

Buzan, Barry, Ole Waever and Jaap de Wilde, (1998) *Security: A New Framework for Analysis*, Lynne Rienner, Boulder

Chandler, David (2008) Human Security: The Dog that didn't Bark, *Security Dialogue*, 39(4): 427-38

Chick, Claire (2011) *2011 Franco-British Council Annual Defence Conference Report*, French Embassy, London 31 March 2011

Clark, Liat (2012), Wikileaks' Syria files will be 'embarrassing' for Syria and the West, *Wired*, 5 July 2012 Available at; http://www.wired.co.uk/news/archive/2012-07/05/wikileaks-syria-files (accessed 16 July 2012)

Coats, R Morris, Gökhan Karahan and Robert Tollision (2006) Terrorism and Pork Barrel Spending, *Public Choice*, 128(1): 275-87

Cohen, Dara et al (2006) Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates, *Stanford Law Review*, 59(3): 673-760

Colvin, Michael (1998) European armaments restructuring and the role of WEU: Report submitted on behalf of the Defence Committee to the WEU Assembly, *Document 1623*, Paris, 9 November 1998

Committee on Homeland Security and Export Controls, (2012) *Export Control Challenges Associated with Securing the Homeland*. Washington, DC, The National Academies Press

Comninos, Alex (2011) *Twitter revolutions and cyber crackdowns: User-generated content and social networking in the Arab spring and beyond*, Association for Progressive Communications, available at: http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf (accessed 21 July 2012)

Cooper, Neil (2012) *The Arms Trade Treaty in the Context of Post-Cold War Conventional Arms Trade Regulation*, 10 July 2012, Available at: http://www.caat.org.uk/issues/att/att-neil-cooper.pdf (accessed 13 August 2012)

Cooper, Neil (2006) What's the point of arms transfer controls?, *Contemporary Security Policy*, 27(1): 118-37

Cornish, Paul (1995) *The Arms Trade and Europe*, Chatham House Papers, London, Royal Institute of International Affairs

Council of the European Union (2010) *Internal Security Strategy for the European Union: Towards a European Security Model*, Brussels, 23 February 2010, 5842/2/10

Council of the European Union (2008a), Implementation of the EU Guidelines on torture and other cruel, inhuman or degrading treatment or punishment - Stock taking and new implementation measures, *Note 8407/1/08 from the General Secretariat to the Political and Security Committee*, Brussels, 18 April 2008

Council of the European Union (2008b) The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to improve their Protection, *Council Directive 2008/114/EC*, Brussels, 8 December 2008

Council of the European Union (2008c) *Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment*, Brussels, 8 December 2008

Craig, Paul (2010) *The Lisbon Treaty: Law, Politics and Treaty,* Oxford, OUP

Curtis, Polly (2011), Government faces legal action by US firm over e-border system, *Guardian*, London, 25 August 2011: http://www.guardian.co.uk/uk/2011/aug/25/government-legal-action-e-border

DePauw, Sara (2010) *The Common Position on arms exports in the light of the emerging European defence market*, Background Note, Brussels, Flemish Peace Institute.

Downes, Larry (2011) Why no one will join the Global Network Initiative, Forbes, 30 March 2011, available at: http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/ (accessed 3 August 2012)

Dunne, J Paul (1995) The Defense Industrial Base, in Hartley, Keith and Todd Sandler, (Eds.), *Handbook of Defense Economics*, Oxford, Elsevier: 399-430

Ecorys et al, (2009) Document ENTR/06/054, Study on the Competitiveness of the EU Security Industry, Study produced for DG-Enterprise and Industry within the Framework Contract for Sectoral Competitiveness Studies, Brussels, DG-Enterprise and Industry, 15 November 2009

Edler, Jakob and Andrew James (2012) Understanding the Emergence of STI policies in the EU: the Genesis of EU Security Research and the Role of the EU Commission as Policy Entrepreneur*, Manchester Business School Working Paper No. 630,* Manchester, June 2012

Edwards, Jay (2011) The EU Defence and Security Procurement Directive: A Step Towards Affordability?, *International Security Programme Paper ISP PP 2011/05*, London, Chatham House

Eguren Secades, Santiago (2011) Openness in the European Defence Market and Company Competitiveness, in Bailes, Alyson and Depauw, Sara (Eds.) *The EU defence market: balancing effectiveness with responsibility*, Brussels, Flemish Peace Institute: 29-36

Elgin, Ben, Vernon Silver, and Hermann Zschiegner, (2011) *Wired For Repression.* Bloomberg, Available at http://www.bloomberg.com/data-visualization/wired-for-repression/ (accessed 16 July 2012)

ESRAB (2006) *Meeting the Challenge: the European Security Research Agenda*, European Security Research Advisory Board Report, September 2006, Luxembourg, Office for Official Publications of the European Communities

Euractiv (2006) Critical Infrastructure, http://www.euractiv.com/en/security/critical-infrastructure/article-140597

European Commission (2012a) *Security Industrial Policy: Action Plan for an innovative and competitive Security Industry*, COM (2012) 417 final, Brussels, 26 July 2012

European Commission (2012b) *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels, 28 March 2012

European Commission, (2011) *Building an open and secure Europe: the home affairs budget for 2014-2020*, COM (2011) 749 final, Brussels, 15 November 2011

European Commission (2010) EU-Egypt Action Plan, available at: http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146097.pdf (accessed 13 August 2012)

European Commission (2009) *A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations*, COM (2009) 691 final, Brussels, 21 December 2009

European Commission (2008) *Examining the creation of a European Border Surveillance System (EUROSUR)*, COM (2008) 68 final, Brussels, 13 February 2008

European Commission (2007) *A Strategy for a Stronger and more Competitive European Defence Industry*, COM (2007) 764 final, Brussels, 5 December 2007

European Commission (2006) *Interpretive Communication on the application of Article 296 of the Treaty in the field of defence procurement*, COM (2006) 779 final, Brussels, 7 December 2006

European Commission (2004a), *Security Research: The Next Steps*, COM (2004) 590 final, Brussels, 7 September 2004

European Commission, (2004b), *Green Paper: Defence Procurement*, Document COM (2004) 608 final, Brussels, 29 September 2004

European Commission (2003a) *European Defence - Industrial and Market Issues - Towards an EU Defence Equipment Policy*, COM (2003) 113, Brussels, 11 March 2003.

European Commission (2003b) *A Coherent Framework for Aerospace: A Response to the STAR 21 Report*, COM (2003) 600 final, Brussels, 13 October 2003.

European Commission, (1997), *Implementing European Union Strategy on Defence-Related Industries*, COM 97/583, December 1997, Brussels

European Commission, (1996), *The Challenges facing the European Defence-Related Industry: Contribution with a View to Actions at European Level*, COM 96/10, January 1996, Brussels

European Council, (2003) *A Secure Europe in a Better World* Brussels: European Union

European Defence Agency, (2007) *A Strategy for the European Defence Technological and Industrial Base,* Brussels: European Defence Agency, May 2007

European Organisation for Security (2011) Security Market Evaluation and Recommendations for Funding Future EU Security Activities, March 2011, Available at; http://www.eos-eu.com/LinkClick.aspx?fileticket=y0rpzCaYh7o=&tabid=318

European Union Press Release (2011) Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=EN&guiLanguage=en (accessed 13 August 2012)

Evans, Samuel, (2009), *Technological ambiguity & the Wassenaar Arrangement*, DPhil. Thesis, University of Oxford

Flechtner, Stephanie (2006) European Security and Defense Policy: Between 'Offensive Defense' and 'Human Security'**,** *Internationale Politik und Gesellschaft*, 4/2006: 157-73

Gemeinsame Konferenz Kirche und Entwicklung (2012) *Rüstungsexportbericht 2011 der GKKE*, January 2012, Bonn/Berlin

Gordon, Joy (2010) *Invisible War: The United States and the Iraq Sanctions*, Harvard, Harvard University Press

Hale, Julian (2011) EU to Establish Defense Policy Task Force, *Defense News*, 7 November 2011 http://www.defensenews.com/article/20111107/DEFSECT04/111070302/EU-Establish-Defense-Policy-Task-Force

Haine, Jean Yves, (2011) The Failure of a European Strategic Culture – EUFOR CHAD: The Last of its Kind?, *Contemporary Security Policy*, 32:3, 582-603

Hallsworth, Simon and John Lea (2011) Reconstructing Leviathan: Emerging contours of the security state, *Theoretical Criminology*, 15 (2): 141-157

Hartley, Keith (2011), Creating a European Defence Industrial Base, *Security Challenges*, 7(3): 95-111.

Hayes, Ben and Mathias Vermeulen (2012) *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals,* Berlin and Brussels, Heinrich Böll Stiftung

Hayes, Ben (2010) 'Full Spectrum Dominance' as European Union security policy: On the trail of the 'NeoConOpticon', in Kevin Haggerty and Minas Samaras (Eds) *Surveillance and Democracy*, Routledge, Abingdon: 148-70

Hayes, Ben (2009), NeoConOption: The EU Security-Industrial Complex, Transnational Institute, Amsterdam (http://www.statewatch.org/analyses/neoconopticon-report.pdf)

Hayes, Ben (2006), Arming Big Brother; the EU's Security Research Programme, Statewatch-TNI Report: http://www.statewatch.org/analyses/bigbrother.pdf

House of Commons Committees on Arms Export Controls (2012), *Committees on Arms Export Controls - First Joint Report Scrutiny of Arms Exports 2012*, London, House of Commons

House of Commons Defence Select Committee (2010) *Defence Equipment,* Sixth Report of Parliamentary Session 2009-10, London, House of Commons

ICISS (2001) The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty, International Development Research Council, Ottawa

International Institute for Strategic Studies (IISS), (2012) *The Military Balance 2012*, London, Routledge

IRIS, Instituto Affari Internazionai and University of Manchester, (2010) Study on the Industrial Implications of the Blurring of Dividing Lines between Security and Defence Final Report June 2010 http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf

Israel, Brian (2009) “Make Money Without Doing Evil?” Caught Between Authoritarian Regulations in Emerging Markets and a Global Law of Human Rights, U.S. ICTs Face a Twofold Quandary, *Berkeley Technology Law Journal*, 24(1): 617-55

James, Andrew (2009a), Defence and Security R&D in Europe: SANDERA Background Report: www.sandera.net

James, Andrew (2009b) Introduction and Synthesis Paper, www.sandera.net

Jeandesboz, Julien and Francesco Ragazzi, (2010), *Review of Security Measures in the Research Framework Programme*, Study for the European Parliament Committee on Civil Liberties, Justice and Home affairs, European Parliament, Brussels http://www.statewatch.org/news/2010/nov/ep-review-security-research-programme.pdf

Katzenstein, Peter (1997), Introduction, in Katzenstein, Peter (Ed.), *The Culture of National Security: Norms and Identity in World Politics*, Columbia University Press, New York: 1-32

Kempin, Ronja, Jocelyn Mawdsley and Stefan Steinicke (2012) *Entente Cordiale: Eine erste Bilanz französisch-britischer Zusammenarbeit in der Sicherheits- und Verteidigungspolitik*, Deutsche Gesellschaft für Auswärtige Politik, Berlin

Kington, Tom (2011) Anglo-French Deal Upsets Neighbors: Germans, Italians Warn of '2-Tier Europe', *Defense News*, 13.6.2011, available at: http://www.defensenews.com/article/20110613/DEFFEAT04/106130301/Anglo-French-Deal-Upsets-Neighbors (accessed on 23 July 2012).

Lodge, Juliet (2004) EU Homeland Security: Citizens or Suspects? *Journal of European Integration*, 26(3): 253-79

Marti Sempere, Carlos (2011) The European Security Industry: A Research Agenda, *Defence and Peace Economics*, 22 (2): 245-64

Masseret, Jean-Pierre and Jacques Gautier, (2009) ‘L’Airbus militaire A400m sur le «chemin critique» de l’Europe de la défense’, Rapport d’information, No. 205, *Sénat français*, February 2009

Masson, Hélène and Lucia Marta (2011), The Security Market in the EU and United States: Features and Trends, in *EU-US Security Strategies: Comparative Scenarios and Recommendations*, Issue 3: 111-26 Available at: http://csis.org/files/publication/110614_Conley_EUUSSecurity_WEB.pdf

Maulny, Jean-Pierre (2012) *The Franco-British Treaty, the European Union's 'Pooling and sharing' and NATO's 'Smart Defence': How can the different initiatives in terms of pooling capabilities be coordinated?* Paris, IRIS

Mawdsley, Jocelyn (2011) Towards a Merger of the European Defence and Security Markets?, in Bailes, Alyson and Depauw, Sara (Eds.) *The EU defence market: balancing effectiveness with responsibility*, Brussels, Flemish Peace Institute: 11-19

Mawdsley, Jocelyn (2008a) European Union Armaments Policy: Options For Small States?, *European Security*, 17 (2-3): 367-86

Mawdsley, Jocelyn (2008b) L'industria europea degli armamenti nel contesto dell'integrazione europea: alcune contraddizioni" in Chiara Bonaiuti e Achille Lodovisi (Eds.), *Industria militare e difesa europea: rischi e prospettive*, Annuario La Pira Armi e Disarmo n. 3, Milano, Jaca Books: 75-82

Mawdsley, Jocelyn (2004) The Commission Moves into Defence Research, *European Security Review* 2004, (22), 6-8.

Mérand, Frédéric (2008) *European Defence Policy: Beyond the Nation State*, Oxford University Press, Oxford

Merritt, Giles (2004), Industrial Aspects of European Defence and Concrete Measures, in von Wogau, Karl (Ed.), *The Path to European Defence*, Antwerp, Maklu-Publishers: 215-40

Molas-Gallart, Jordi (1999), Measuring Defence R&D: A Note on Problems and Shortcomings, *Scientometrics*, 45(1): 3-16

Monar, Jörg (2010) The EU's Externalisation of Internal Security Objectives: Perspectives after Lisbon and Stockholm, *The International Spectator*, 45(2): 23 -39

Morag, Nadav (2011) Does Homeland Security Exist Outside the United States?, *Homeland Security Affairs,* 7(September): 1-5

Morozov, Evgeny (2011) *The Net Delusion: The Dark Side of Internet Freedom,* New York, Public Affairs

Mörth, Ulrika and Malena Britz (2004) 'European Integration as Organizing: The Case of Armaments', *Journal of Common Market Studies*, 42(5): 957-73

Mörth, Ulrika, (2000), 'Competing Frames in the European Commission - the Case of the Defence Industry and Equipment Issue', *Journal of European Public Policy*, 7(2): 173-89

Mueller, John and Mark Stewart (2012) The Terrorism Delusion: America's Overwrought Response to September 11, *International Security*, 37(1): 87-110

Nielsen, Nikolaj (2012a) EU-funded consortium unveils border-control robot, *EUObserver*, 10 May 2012: http://euobserver.com/22/116223 (accessed 10 May 2012)

Nielsen, Nikolaj (2012b) EU components used in Belarus spy drones says NGO, *EUObserver*, 10 September 2012: http://euobserver.com/foreign/117489 (accessed 20 September 2012)

Pawlak, Patryk (2009) Made in the USA? The influence of the USA on the EU's Data Protection Regime, Centre for European Policy Studies, Brussels

Perlroth, Nicole (2012) Software Meant to Fight Crime Is Used to Spy on Dissidents, *New York Times*, 30 August 2012

Poitevin, Cedric (2011) A European export control regime: balancing effectiveness and responsibility, in Bailes, Alyson and Depauw, Sara (Eds.) *The EU defence market: balancing effectiveness with responsibility*, Brussels, Flemish Peace Institute: 47-52

Privacy International (2012) British government admits it has already started controlling exports of Gamma International's FinSpy, Press release 10 September 2012, available at: https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma (accessed 21 September 2012)

Privacy International (1995) *Big Brother Incorporated 1995*, London, Privacy International: available at: https://www.privacyinternational.org/reports/big-brother-incorporated-1995 (accessed 13 June 2012)

Rees, Wyn and Richard Aldrich (2005) Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence?, *International Affairs*, 81(5): 905-23

Relya, Harold (2002) Homeland Security and Information, *Government Information Quarterly*, 19(2002): 213-23

Reporters without Borders (2012) *Beset by Online Surveillance and Content Filtering Netizens fight on*, Paris, 29 March 2012, available at: http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html (accessed 5 August 2012)

Schmitt, Burkard et al, (2005), *Defence procurement in the European Union: The current debate*, Report of an EUISS Task Force, Paris, May 2005

Schumann, Harald (2011) Die Schnüffel-Industrie unterstützt autoritäre Staaten, *Der Tagesspiegel*, 29 October 2011

Slijper, Frank, (2005), *The Emerging EU Military-Industrial Complex: Arms Industry Lobbying in Brussels*, TNI Briefing Series 2005/1, Amsterdam, The Transnational Institute

Stankiewicz, Rikard et al (2009), Knowledge Dynamics Scoping Paper, www.sandera.net

Steinmann, Thomas and Benjamin Dierks (2012) Deutschland will NATO für Panzerverkäufe einspannen, *Financial Times Deutschland*, 31 July 2012

Taylor, Trevor (1997) Arms Procurement, in Howorth, Jolyon and Anand Menon (Eds.) *The European Union and National Defense Policy,* London, Routledge: pp.121-40

Thorleuchter, Dirk and Dirk van den Poel (2011) Semantic Technology Classification - A Defence and Security Case Study**,** *2011 International Conference Proceedings on Uncertainty Reasoning and Knowledge Engineering*: available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06007833

Tigner, Brooks (2003a) EU moves to directly fund research, *Defense News*, 6 January 2003

Tigner, Brooks (2003b) EU to shift research funds into defense: move mixes national, EU money for global security, *Defense News*, 5 May 2003

Timm, Trevor and Jillian York (2012) Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators, *The Atlantic*, 6 March 2012,

http://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/

Trybus, Martin (2000) On the application of the EC Treaty to Armaments, *European Law Review*. 25(6): 663-68

Ullman, Richard (1983) 'Redefining Security', *International Security,* 8(1): 129-153.

United Kingdom Ministry of Defence (2012) *National Security through Technology: Technology, Equipment and Support for UK Defence and Security*, Cm 8278, The Stationery Office, London, February 2012

United Kingdom Ministry of Defence (2006), Defence Technology Strategy, London: http://www.mod.uk/NR/rdonlyres/27787990-42BD-4883-95C0-48BB72BC982/0/dts_complete.pdf

United Nations Development Programme (1993) *Human Development Report 1993: People's Participation*, available at: http://hdr.undp.org/en/reports/global/hdr1993/

United States Commission on National Security in the 21st Century (2000) *Seeking a National Strategy: A Concept for Preserving Security and Promoting Freedom*: available at http://www.au.af.mil/au/awc/awcgate/nssg/

Valentino-Devries, Jennifer et al. (2011) Document Trove Exposes Surveillance Methods, *Wall Street Journal,* 19 November 2011

Vranckx, An, Frank Slijper and Roy Isbister (2011) *Lessons from MENA: Appraising EU Transfers of Military and Security Equipment to the Middle East and North Africa: a Contribution to the Review of the Common Position,* Ghent, Academia Press

Wagner, Ben (2012a) *Exporting Censorship and Surveillance Technology*, HIVOS Report January 2012, Humanist Institute for Co-operation with Developing Countries (HIVOS), The Hague, Accessed 28 April 2012: http://www.hivos.nl/eng/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Exporting-Censorship-and-Surveillance-Technology

Wagner, Ben (2012b) *After the Arab Spring New Paths for Human Rights and the Internet in European Foreign Policy*, European Parliament Directorate-General for External Policies Briefing Paper EXPO/B/DROI/2011/28, July 2012, Brussels

Wassenaar Agreement (2005) Criteria for the Selection of Dual-Use Items, Available at http://www.wassenaar.org/controllists/2005/Criteria_as_updated_at_the_December_2005_PLM.pdf (accessed 13 August 2012)

Wetter, Anna (2009) *Enforcing European Union Law on Exports of Dual-Use Goods*, SIPRI Research Report 24, Oxford, OUP

Wolfers, Arnold (1952) National Security as an Ambiguous Symbol, *Political Quarterly*, 67 (December): 481-502

Youngs, Richard, (2002) *The European Union and the Promotion of Democracy: Europe's Mediterranean and Asian Policies*, Oxford, OUP

COLOPHON

Author:
Jocelyn Mawdsley

Project guidance Flemish Peace Institute:
Sara Depauw

Publisher:
Tomas Baum (Leuvenseweg 86, 1000 Brussels)

Brussels, 8 January 2013
ISBN 9789078864554

The Flemish Peace Institute was founded by decree of the Flemish Parliament as an independent institute for research on peace issues. The Peace Institute conducts scientific research, documents relevant information sources, and informs and advises the Flemish Parliament and the public at large on questions of peace.

Flemish Peace Institute
Leuvenseweg 86
1000 Brussels
tel. +32 2 552 45 91

vredesinstituut@vlaamsparlement.be
www.flemishpeaceinstitute.eu