Newcastle University e-prints

Date deposited: 24th April 2012

Version of file: Published

Peer Review Status: Peer reviewed

Citation for item:

Further information on publisher website:

http://www.flemishpeaceinstitute.eu/

Publisher's copyright statement:

Use Policy:

Towards a Merger of the European Defence and Security Markets?

Dr. Jocelyn Mawdsley, Newcastle University

Since the terrorist attacks of 9/11 much attention has been paid to the United States' homeland security programme, but it has been less widely noted that the EU has also developed a series of initiatives aimed at enabling the development and production of security technologies, focused around the security research priority of the EU's Seventh Framework Programme (FP7). These policy initiatives are slowly creating an identifiable security market within the EU. The question underpinning this chapter is the extent to which this is a distinct entity, or whether it is in fact simply an offshoot of the well-established defence market.

This chapter makes the assumption that security refers to the homeland security agenda developed in the post 9/11 era. It is difficult, however, to completely separate defence and security issues even in this limited time period. Defence is sometimes viewed as being military and focussed on external security, whereas contemporary homeland security is predominantly internally focussed and civilian. The reality is that divisions are not clear cut. Policing, intelligence and border control customs vary considerably within the EU as does the role of the military in internal security. States like Britain and France have merged both concepts in recent strategic reviews (the French 2008 White Book and the British 2010 Strategic Defence and Security Review). For some commentators, it is merely a matter 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."[1] For others, the blurring of the boundaries of military and civilian is a worrying development with concerning implications for civil liberties in Europe.

This chapter aims to offer an analysis of the interconnectedness (or otherwise) of the security and defence markets in the European Union (EU) by considering firstly, how the security market has come into existence and then questioning whether providers and products differ substantially between security and defence. It will then ask whether security products are subject to controls as strategic goods and whether these controls are fit for purpose. It will conclude by discussing whether the merging of security and defence markets is real, problematic or useful.

The Beginning of an EU Security Market?

The first analytical problem facing the researcher keen to consider the EU security market is one of definition. What is the security market and what firms are involved? It is not entirely clear. Ecorys et al (2009) emphasise this difficulty in their report for DG-Enterprise and Industry on the competitiveness of the security industry in Europe. Their model for scoping the sector differentiates between the traditional security market, based around the largely private provision of protection for persons and property, and the market that is responding to 'new' security threats such

---

as terrorism, organised crime, cyber-crime and protection from and response to major catastrophes.[2] This latter market is immature, arguably only having been called into existence since 9/11 and the subsequent US launch of a major Homeland Security programme. 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.[3] The demand side is still highly fragmented. The nature of this market and the firms operating within it will be shaped by early funding programmes, so it is worth taking some time to consider the genesis and character of the EU security research programme, which has the aim of creating such a market within the EU.

DG-Enterprise and Industry itself claims on its website to trace the evolution of security research to 2003,[4] citing the European Security Strategy as the rationale for Commission activity to increase European security. Concrete development of what became security research seems, however, to date from July 2002 with the report of the Strategic Aerospace Review for the 21st century, or STAR 21, and the Commission's response.[5] STAR 21 was somewhat controversial. The report was the product of an unusually high-level working group of European aerospace industry figures, European Commissioners, Javier Solana and Members of the European Parliament. It emphasised the view that European civil and defence aerospace were both complementary and interdependent and needed considerable investment to match the American competition. The report had two particular priorities: (1) rapid progress in developing a more coherent European market in defence equipment; and key to this paper, (2) major improvements to the structure of European research and technology in civil aeronautics, defence and space. Another 2002 document is also worthy of note: the Strategic Research Agenda for aeronautics released by the Advisory Council for Aeronautics in Europe (ACARE).[6] Like STAR 21, the ACARE report also pointed out that defence companies in the United States are now spending considerably more on research than their European Union counterparts. A uniting theme of the two reports was the stress laid on the belief that technological innovation in the defence and aerospace fields was key to wider economic success for the EU.

According to DG-Enterprise and Industry, the next key document for the development of security research was the March 2003 Commission Communiqué 'Towards an EU Defence Equipment Policy'. 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 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".[7] 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

2   Ecorys et al, 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.

3   Interviews carried out with German officials in 2008.

4   http://ec.europa.eu/enterprise/security/documents_en.htm consulted on 7 March 2011.

5   European Commission, STAR21 Strategic Aerospace Review for the 21st Century, Brussels, European Commission, July 2002.

6   Advisory Council for Aeronautics Research in Europe, Strategic Research Agenda, Brussels, ACARE, October 2002.

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

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".[8] 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".[9]

This however was complicated by the decision in June 2003 of the European Council to launch an intergovernmental agency, to be known as the European Defence Agency (EDA), which was finally agreed in a July 2004 joint action. The EDA was specifically tasked with coordinating EU defence research and development. It was at this stage that the Commission documents became some-what ambiguous as they tried to find a way to continue with their plans without openly funding defence research, which they had no legal basis for doing. The Commission's 2004 communiqué and decision, which launched a preparatory action in the field of security research (PASR), drew inspiration from the 2003 European Security Strategy and the priorities were rather broad.[10]

PASR was to spend 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 facili-tate an EU security culture. PASR funded projects in the following priority mission areas:
– Improving situation awareness
– Optimising security and protection of networked systems
– Protecting against terrorism
– Enhancing crisis management
– Achieving interoperability and integrated systems for information and communication.

PASR is noteworthy as it was a particularly large preparatory action, operating for the maximum budget (€65 million) and time span (3 years) permitted in the relevant procedural framework. Although dubbed a research programme and initially launched by DG-Research, the funding approved for PASR was provided under the then Article 157 of the EC Treaty (Title XVI -Industry) rather than under Title XVIII (Research) as ordered in Article 163(3) of the Treaty. Later the PASR group was moved into DG-Enterprise and Industry, which also manages the security research priority in the 7th Framework Programme. There was no question of PASR failing. The first call for projects had hardly been made before the decision of whether to continue with a security research priority in the 7th Framework Programme was taken, in a September 2004 communiqué called 'Security Research: The Next Steps'.[11]

The Group of Personalities whom the Commission asked to produce a report on security research was heavily biased towards defence industry and defence officials, and had very little represen-tation from any users of civilian security research. Unsurprisingly, their report contended that there should be no division between military and civilian research and argued for €1 billion per year (minimum) to be spent on security research, thus helping to meet the Lisbon target of 3% of

8   Tigner, B, EU moves to directly fund research, Defense News, 6 January 2003.

9   Tigner, B, EU to shift research funds into defense: move mixes national, EU money for global security, Defense News, 5 May 2003.

10   European Commission, COM (2004) 72 final and Decision 2004/213/EC, On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, Towards a programme to advance European security through Research and Technology, Brussels, European Union, 3 February 2004.

11   European Commission, COM (2004) 590, Security Research: The Next Steps, Brussels, European Union, 7 September 2004.

GDP spent on research.[12] Its primary claim for doing this appeared to be that as the US has chosen to invest this much in Homeland Security so must the EU, to ensure that US industry should not have a competitive advantage – scarcely a particularly convincing argument given the widespread domestic criticism of the USA's own homeland security research programme.

The Commission's communiqué 'Security Research: The Next Steps' committed it to setting up a European Security Research Advisory Board (ESRAB) "to advise on the content of the ESRP and its implementation, paying due attention to the proposals of the Group of Personalities". ESRAB should include "experts from various stakeholder groups: users, industry, and research organizations".[13] The research priority eventually agreed within the 7th Framework Programme maps fairly closely onto the findings of the ESRAB report, with the following activities being funded (€1.4 billion over the lifetime of FP7):
– **"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;
– **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."[14]

The research is mission-orientated and in many ways is 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. A good example of this is the Seabilla project: according to one firm involved, Mondeca, "Seabilla will define the architecture for cost-effective European Sea Border Surveillance systems; integrate space, land, sea and air assets, including legacy systems; apply advanced technological solutions to increase performances of surveillance functions; as well as develop and demonstrate significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels"[15]. Interviews with DG-Enterprise officials in 2008 made it clear that they were predominantly interested in running the priority as a internal security market creation scheme, to push for standardisation of security practices and procedures across the EU (through end-user involvement in all projects) and thus to increase the competitiveness of the EU security industry.

12   European Communities, EUR 21110, Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research, Luxembourg, Office for Official Publications of the European Communities, 2004.
13   European Commission, COM (2004) 590.
14   http://cordis.europa.eu/fp7/cooperation/security_en.html consulted on 7 March 2011.
15   http://www.mondeca.com/index.php/en/research/projects/seabilla_european_union_ict_fp7_sec_2009_1_2010_2014 consulted on 7 March 2011.

The EU Security Market Features: Supply Side

Ecorys et al have identified three types of supplier in the security market: the traditional security industry supplying general security applications e.g. protective clothing, access control, fire detection, CCTV; the security-orientated defence industry, based on applying defence technologies to security problems or where defence firms have acquired or adapted civilian technologies for use in the security market; and finally, new entrants either from other civilian industrial sectors spinning in their technologies for security use or start-up companies.[16] However, within the high end of the 'new security' market, as fostered in the EU Security Research programme, Ecorys et al see a fairly limited involvement of the traditional security firms, except in some surveillance technological areas. They also point 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, and the specificity of their demands, which combine to produce a corresponding concentration in the supply of security equipment.[17] They also argue 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;
–   High costs in securing markets (lobbying, marketing and government relations) – this is related to 'the need to 'educate' clients on technological possibilities and choices.[18]
This means that there is little involvement by small and medium-sized enterprises (SME), and when SMEs do develop technologies, they tend to either be acquired by the large equipment integrators or licensed out to them to develop the technology.

Does this add up to a convergence of security and defence providers? If one takes the security market as a whole, then no, the spectrum of suppliers is still relatively diverse. However, when the high end of the 'new security' market, as supported by the EU security research programme, is considered then the picture is rather different.[19] Here there is a concentration of defence contractors who have entered the security market by acquiring companies specialising in areas such as x-ray scanning, biometrics and mobile communications, or by applying existing defence technologies to internal security problems. 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 with the acquisition of L-1 Intelligence Services group. Ecorys et al noted that firms originating in the civilian market were major players in very few sectors e.g. Motorola in secure communications.[20] Looking at the history of the security research programme, this is perhaps unsurprising. This tendency looks likely to be strengthened by the Commission's response to the European Security Research and Innovation Forum report, when it notes the need to strengthen the complementarity and cooperation between defence and civilian technologies, and to increase its mandate to include the external dimension of security in future research programmes.[21]

---

16   Ecorys et al, Document ENTR/06/054.

17   Ibid.

18   Ibid p. iv.

19   The area of European maritime security is the only sector at the high-end of this market to show much diversity in suppliers according to Ecorys et al.

20   Ibid.

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

The European Commission has also 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.[22]

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".[23] The EDA has identified situational awareness (sensor technologies, command and control of networked assets) as an area for cooperation.[24] 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.

Is there a Convergence of Military and Non-Military Products supplied to the market?

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.[25] Aircraft-carriers, fighter jets and advanced missile technology for example remain clearly military products. Stankiewicz et al insist that this division will be maintained, as ministries of defence will be careful to retain control over and privilege investment in some defence technologies for reasons of national security and security of supply.[26] Where there is less difference is in the technologies underpinning the products. If we consider the STACCATO taxonomy of technologies of interest to security and defence users, then James 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)."[27] Most defence and civilian security products however are heavily reliant on a wide range of generic technologies.

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

22   James, A (2009a), Defence and Security R & D in Europe: SANDERA Background Report: www.sandera.net consulted 7 March 2011.

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

24   James, A (2009a).

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

26   Stankiewicz, R et al (2009), Knowledge Dynamics Scoping Paper, SANDERA Scoping Paper www.sandera.net consulted 7 March 2011.

27   James, A (2009a) p. 7.

"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."[28]

In other words, the Cold War defence innovation model is breaking down. Because both military and non-military security products draw on generic technologies, 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 vis-à-vis wider civilian and commercial technology innovation.[29] 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. This means that there are new challenges for those concerned about defence and security technology proliferation.

Security Products and Strategic Goods Trade Restrictions

During the Cold War when the Western export control organisation COCOM was engaging in economic warfare with the Soviet Union, strategic goods were seen as goods that were relatively inefficient to produce domestically, but were needed for the pursuit of a particular strategy. Since the end of the Cold War, controls over exports of a strategic but not necessarily military nature have been handled in a more limited fashion by regulating the export of dual-use goods. These legal boundaries also potentially apply to security technologies, and DG-Enterprise and industry warns security research programme applicants that they need to consider whether their application falls into these categories. The most recent EU legislation on this is Council regulation 428/2009, which 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".[30] The list of items covered by this regulation is likely to cover some non-military security equipment and technology, particularly technologies in the area of telecommunications, information security and unmanned aerial vehicles. The export of some types of non-military security equipment is also controlled under Council Regulation (EC) No. 1236/2005 or the 'Torture' Regulation (the Commission is currently working on proposals to tighten this regulation). Individual member states may also have stricter national regulations on the export of certain products, but so long as security technology exports comply with these regulations then the trade is legal.

Should these controls be further extended? A case might be made for this, given the difficulty in establishing whether or not the export will have a military end-use and thus be used in a way the exporting country does not find acceptable, and that there is a further risk that exports of

---

28   Stankiewicz R et al (2009) p. 21.

29   James, A (2009b) Introduction and Synthesis Paper, www.sandera.net consulted 7 March 2011.

30   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).

security products could be used by recipients to perpetuate human rights abuses and other forms of internal repression. The UK's working group on arms 2009 report to the Quadripartite Committee on arms exports, for example, reports on the use of armoured Land Rover-based vehicles by IDF forces in Operation Cast Lead. The UKWG suggests that these were initially supplied as non-military utility vehicles but subsequently adapted into armoured vehicles by Israeli based company M.D.T. Protective Industries Ltd, part of the US company Arotech.[31] In another example, Amnesty International and Omega 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.[32] Similarly, there was considerable criticism of EU exports to North African and Arab states in Spring 2011, when such exports were potentially used in an attempt by regimes to crush popular uprisings. Critics of the EU's security research programme have also questioned the levels of funding that Israeli firms and researchers are receiving from the programme, and in particular the funding of firms like Elbit Systems, which was involved in the construction of the controversial separation wall.[33] Given these loopholes and the potential for problematic usage of EU security exports, should restrictions be tighter, especially given that DG-Enterprise and Industry's vision for the strengthening of the security technological and industrial base clearly implies a vigorous export strategy?

On the other hand, more extensive or restrictive controls potentially ignore the issue of global interdependence. If international passenger flights are to be made secure, is the more sensible option to ban flights from any country deemed a terrorism concern, or to ensure that the country can acquire advanced screening technology? Does the exclusion of problem states from the group of states allowed to be 'secured by technology' simply increase feelings of inequality and unfairness in global politics, which in turn can fuel terrorism? Moreover, 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.[34] It seems that the option of simply imposing greater restrictions on these items is not entirely straightforward.

Is the merging of security and defence markets real, problematic, or useful?

Although real gaps still exist between military and civilian users of security and defence products in their practices, requirements and legal constraints, there has undoubtedly been a blurring of the boundaries. In part, this is because of technological dynamics: the opening up of a previously closed system of defence innovation because of the need to draw upon more advanced civilian technology, which has lessened the "silo mentality" conviction that defence is different. In part too, it reflects a belief on the part of policy-makers that technology can offer answers to the 'new security' problems that have emerged, and a willingness particularly at the EU level to open up a funding stream. Defence manufacturers have been well-placed to expand into this new funding pool - which has high entry barriers for firms not accustomed to high research and development outlays and to the extensive government relations needed when the user group is so small - and

31   UK Working Group on Arms, Memorandum to the Committees on Arms Export Controls, 8 December 2009: http://www. publications.parliament.uk/pa/cm200910/cmselect/cmquad/memo/arms_exp/caec%2008.htm consulted 7 March 2011.

32   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.

33   Hayes, B, Should the EU subsidise Israeli security?, European Voice, 18 March 2010.

34   Gordon, J (2010) Invisible War: The United States and the Iraq Sanctions, Harvard, Harvard University Press.

have been strongly encouraged to do so by policy-makers. It is important not to overstate the case: the security and defence markets have not merged, but the boundaries are more blurred than once was the case.

Is this useful or problematic? Clearly it raises some problems around export regulations as outlined above, but the really problematic issue is in fact an internal issue, namely the future of internal security within the EU. Several worrying trends seem to be emerging. It is not simply a question of militarisation. The involvement of defence firms so long as they understand the very different policy terrain is not necessarily problematic. As Bailes points out,

> "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." [35]

More and more issues are being portrayed as security problems to which security technologies can offer solutions, but the mere definition of issues as security problems legitimises reactions that would otherwise be viewed as problematic. The rights of both EU citizens and non-citizens seem to play second fiddle to the overarching goal of security. But there needs to be a better balance struck. The second problem is that the rapid advances in technology are running ahead of legislation on their legitimate use. Current discussions on deploying unmanned aerial vehicles for civilian surveillance would be a good example of this. Is it appropriate? What limitations should there be? The EU security research programme has been criticised for a lack of attention to transparency and concerns about citizens' rights. It is to be hoped that these are teething pains rather than a harbinger of what is to come in any extension of the programme in future.

35   Bailes, A (2008), 'The EU and a 'Better World': What Role for the European Security and Defence Policy?' International Affairs, 84:1:pp. 115-30: here p. 118.