

ISSUE 3
INDUSTRY TOWARD SECURITY



INTRODUCTION

Nicolò Sartori, *Junior Researcher, IAI*

Since the end of the Cold War, the collapse of the Soviet Union and the advent of structural modifications within the international system, the security perceptions and strategies across the Western world have witnessed radical change and development. Nowhere else is this more evidenced than by defense spending trends over the last half century.

As concerns for large-scale conventional warfare, nuclear attack and the spread of communism fell by the wayside, so too did the age of bi-polarity. With the rise of U.S. leadership, the international community also bore witness to the enhancement of the European Union and other international organizations. Reflective of this downturn in global military conflict, the 1990s defense budgets in both the United States and in the EU countries, experienced sharp reductions and cuts, while national defense industrial bases underwent extreme reorganization and consolidation.

Today, the economic, political and technological landscape of the 21st century has ushered in new security concerns and progressively influenced the politics of modern-day warfare. The terrorist attacks of September 11, 2001, on the World Trade Center illustrates the level of danger new-age technologies and warfare techniques pose to both civilian and military personnel. It also clearly depicts the central role national security has to play in ensuring the safety and well-being of citizens.

As a result of the 9/11 attack, defense budgets of the major transatlantic players once again began to experience growth, and for many, this budgetary increase continues to rise. . The funding for military efforts in Afghanistan and Iraq and crisis management operations by the United States, EU and/or NATO frameworks account for the majority of this expenditure.

Defined as multifaceted, interrelated and increasingly transnational, modern-day threats have shaped a new approach to national security policy and agenda setting. Risks associated with technological development, the rise and empowerment of non-state actors and the possibility of domestic attack must all be taken into account. As a result, activities such as counterterrorism and the fight against organized crime, border control, critical infrastructure protection and preparedness and recovery in times of crisis, now represent fundamental aspects of national security policy.

The emphasis placed on these new challenges has established security as a viable and pertinent market and represents an expansion of a traditionally defense-oriented industry. Although defense-related issues continue to constitute significant portions of governments' budgets, the United States and the EU are actively seeking to build a comprehensive approach to the security sector by way of

legislation and regulations, collaboration with the commercial sector to build industrial and commercial strategies as well as by expansion of the public-private dialogue and partnership programs.

This paper seeks to provide not only a clearer definition of the security market, but will describe the strategies, policies and procedures adopted by both the EU and the United States in efforts to establish an efficient security market and a thriving security industrial base. Additionally, the political, economic and technological drivers and constraints with the potential to influence the development of a competitive transatlantic security industrial sector will be discussed and possible policy recommendations for EU and the United States will be proposed.

The first section, by H  l  ne Masson and Lucia Marta of the Fondation pour la Recherche Strat  gique (FRS), provides a complete picture of the current security market from both the demand and supply sides. The analysis focuses on the main industrial actors and procurement agencies operating in the security sector and pays particular attention to the transatlantic dimension of the market. A high level of fragmentation, both in terms of customer base and industry, has been established as the characterizing feature of the security markets in the EU and the United States.

In the second part of the paper Jan Joel Andersson and Erik Brattberg of the Swedish Institute of International Affairs (UI) focus on the rise of the public-private dialogue. Specifically, this section seeks to determine whether the partnerships between governmental agencies and the private sector reflect an adequate level of collaboration capable of fostering a fruitful exchange of ideas between stakeholders. As UI illustrates, the diversity of buyers' profiles and the unstable/volatile nature of demand within the security market continues to pose significant challenges for the industry.

The third section by David Berteau, Guy Ben-Ari and Priscilla Hermann of the Center for International and Strategic Studies (CSIS), and Sandra Mezzadri of the Istituto Affari Internazionali (IAI), analyses the regulatory environments for security in the United States and the EU. Their investigation identifies different kinds of regulatory shortcomings in both the United States and the EU and highlights a series of common regulatory weaknesses, such as the unclear distinction between the security vs. defense industries, barriers to the security market and insufficient public-private dialogue, all of which areas that can benefit from common transatlantic development.

The final section of the paper written by Valerio Briani and Nicol   Sartori of the Istituto Affari Internazionali (IAI), analyses the different economics characteristics of the defense and the security industrial sectors and their effect on transatlantic cooperation. In addition, IAI discusses the two very different approaches adopted by the United States and the EU in terms of industrial security policy. With the help of collaborating international partners, this section also highlights the differences between the EU's European-centric or multinational-focused industrial policy and the institutionally centered U.S. approach.

This paper concludes with a set of policy recommendations, applicable both to the EU and the United States, aimed at improving the industry's engagement in the governance of the security sector, the enhancement of the regulatory environment and the avoidance of protectionist practices.



THE SECURITY MARKET IN THE EU AND THE UNITED STATES: FEATURES AND TRENDS

Hélène Masson, *Senior Research Fellow, FRS*, and
Lucia Marta, *Researcher, FRS*

Introduction

This section aims to provide a general overview of the structure and dynamics of the security market in Europe and in the United States as well as assesses the opportunities for cooperation at the transatlantic level. Taking a look at the demand-side of the market, this paper will discuss the main actors and security functions identified at the institutional level as well as provide estimations of governmental funding for R&D and the procurement of security solutions and systems. On the supply-side, this paper describes the competitive structure of the security market and its dominant characteristics as well as market segmentation and the strategic orientations of the most prominent competitors.

Security Market: Demand Side

In Europe

Fragmentation in the European security procurement environment

While the defense market is mature and well-structured at the national level, the security market is relatively new and undeveloped. The juxtaposition of these two sectors reveals two fundamental differences with regard to the procurement of security solutions.

First, in the security sector more than one customer can procure security systems. Customers at the national level can be public (several ministries, agencies and institutions) or private (banks, but also owners or managers of critical infrastructures). Moreover, public customers can be found at the central, regional or local level.

Consequences of such fragmentation include the following:

- The security demand is varied and, therefore, many relatively small/medium contracts are issued (when compared to the defense sector) ;

- Security requirements are not harmonized, except for those solutions for which public regulation (in terms of requirements, standards, etc.) exists;
- The size of the security market is hard to ascertain, unlike the defense market

Second, unlike the United States, the demand-side has not established a “European Homeland Security Agency.” As a result, procurement of security equipment does not occur at the EU level, yet at the national level.¹

Besides the fragmentation of European security procurement across all 27 member states, demand for security is also highly split across national lines. With security-related activities occurring primarily at the national and subsequent regional and local levels, the EU requires a high degree of coordination, which currently is insufficient. For example, in France the budget allocated by the Ministry of Interior for the national police and gendarmerie in 2010 concerning investments in new technologies was around 192.6M€, but it does not include the procurement of security solutions related to border control (included in the Coast Guard budget) or airports and ports security solutions, which are under the responsibility of private companies. Official statistics, in this respect, do not exist. Therefore, a complete overview of the budgets allocated for investments in technological solutions is very hard to assess, even at the national level.

We can identify a few examples of countries trying to reduce fragmentation and centralize procurement activities, at least in the communications and biometrics industries. Notably, the acquisition of a single radio system for Federal and Lander first responders in Germany and the National Resilience Extranet System providing national responders with access to the same web-based information system in the UK.

When looking at some security contracts awarded by the main European countries, we can observe the following features:

- They are quite small compared to the defense sector, in terms of costs;
- They have been completed in the past few years, and apparently no new expensive contracts have been recently issued in all the security segments, although some of them, communications and biometrics in particular, are the center of public attention;
- They are often linked to specific events for example, in the UK, the Home Office manages the project “Olympic Safe and Security,” which costs around 600M£. Similarly, if a natural disaster or a terroristic attack occurs in Europe, the security market is able to quickly react.

To conclude, European procurement remains in the hands of single member states, the market is fragmented among different players (public and private, national and local) and demand appears to be experiencing a slowdown across the market, except for in a few key sectors and following specific events.

The European Union: a crucial player in the field of security R&D

While the EU cannot be considered a security procurer, it, nevertheless, plays a very important role in coordinating the security research agenda across 27 EU member states and Associated countries.

The ESRAB report,² in particular, is the first and only comprehensive European effort to highlight security needs in terms of capabilities and technologies for European security and indicates the necessary R&D track. The ESRAB report adopted a capability-related approach, moving in a linear fashion from threats to missions, to functions, to capabilities and lastly to technologies. Identified technologies are meant to address the needs of the following four security missions: border security; protection against terrorism and organized crime; critical infrastructure protection; and recovery following times of crisis.

Following the efforts put in place by the Commission (GoP, PASR, ESRAB), the Seventh Framework Program on research includes, for the first time, a budget line dedicated to security, which is inserted in the Cooperation Program. It covers the period 2007–2013 and allocates 1,4B€ for the Security theme (around 4 percent of the FP's cooperation program), which accounts for an approximate 200M€ per year. This figure is somehow misleading however, as there are security-related projects within other themes, like Information and Communication Technologies, Transports and Space. Although, the overall European funding for security research is hard to calculate, the specifically allocated 1.4B€ is an important figure contributing to the development and expansion of the security market.³

Beyond the 7FP, other agencies at European level are developing security programs with the potential for future procurement. European agencies like EUROPOL, EUROJUST, FRONTEX, EDA are catalysts for demand harmonization in R&D sector and the future procurement of security systems. Equally, they are often involved in missions requiring collaboration with the United States and thus have led to the establishment of operational and technical transatlantic capabilities.⁴

At the national level, security R&D appears weak compared to those made by the EU. In Germany, the Federal Ministry of Education and Research allocated around 123M€ for the period 2007–2011 for civil security research. In France, the D el egation G en erale 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.

The significant level of R&D funding for security at the EU level, rather than at the national level, is creating the good basis for future common procurement. Whether resources for procurement will be available, however, remains unknown. Many experts question the growth of the security market in Europe and the capacity of national institutions to benefit from the established R&D programs.

Estimation of the European security market size and trends

Some estimations of the size of the European security market are made available by research centers and consultancies.

The European Commission⁵ and ECORYS⁶ have stated that the EU security industry had an estimated value ranging from 26 to 36B€ in 2008. This figure represents a large range, confirming the difficulty in acquiring a precise idea of the market size. Moreover, it includes "low level" security systems, like video surveillance and fire detection systems.

According to ECORYS, the following sectors account for the major market share:

- Physical security protections, from 10 to 15B€;
- Border security as well as counterterrorism intelligence, 4.5B€ at least; critical infrastructure protection from 2.5 to 3.5B€;
- Aviation and maritime security sectors from 1.5 to 2.5B€.

Moreover, according to ECORYS, the public sector is the main purchaser of security equipment and services accounting for approximately 80 percent of the market, which places global public spending between 13 and 17B€.

Demand at the European and the national level exist as security concerns are, and will continue to be, high on the political agenda. The public sector will continue to stimulate demand from the private sector through the establishment of security procedures, particularly with regard to aviation security and critical infrastructures protection. Moreover, European agencies are working on the definition of new common and interoperable solutions. Nevertheless, the current economic slowdown and public budget cuts, besides the growing costs of technological solutions which require long term investments, do not guarantee adequate investments for the procurement of security solutions. It is very hard to assess how fast and for how long the security market will grow. At the moment, the level of growth is not being sustained or increasing as quickly as expected in the past years.

In the United States

The Department of Homeland Security and other actors in the security procurement

In the United States, demand in the security market is mainly led by the government (federal, state and local level). Also private companies play a role, but this is limited when compared to the public spending.

The Department of Homeland Security (DHS) brings together, under one agency, activities that were previously spread across the federal government, centralizing the competences in the security domain and improving coordination and effectiveness. Agencies that are now part of DHS include the Coast Guard, the Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA) and activities previously performed by the Immigration and Naturalization Service (INS) and Customs and Border Protection (CBP).

It is worth noting that most of the DHS acquisition budget is spent on services rather than on products (for a more detailed view on DHS procurement see section 3 in this paper). Moreover, not all the resources allocated to DHS are spent on core homeland security activities: part of it (the CBO estimates about 35 percent of the total budget in 2004)⁷ financed non-homeland security functions that were performed by their original agencies (for example, Coast Guards task in marine safety and navigation support).

At the same time, other federal agencies perform tasks related to homeland security although their budget is not part of DHS, the CBO estimates that in 2004 about 17M\$ were allocated for non-DHS homeland security activities. For example, DoD spending for systems and operations was approximately 10B\$ for FY 2006. Additionally, more than 2B\$ per year is spent on Improvised

Explosive Devices (IED) along with substantial investments in counter Weapons of Mass Destruction (WMD) technologies.⁸

Also in the United States, demand appears fragmented as DHS and other federal agencies are involved in security R&D and procurement. Indeed, DHS has fewer large programs than DoD and pushes a significant share of the acquisition money to states and local authorities through a variety of relatively small grant programs.

As in Europe, developments and shifts in policy as well as the occurrence of either natural and or terrorist-related events can lead rapidly to new priorities and budget allocation. The security market is therefore maturing comparing to 10 years ago, and is certainly more mature than the EU market, but still volatile and dynamic.

U.S. R&D in the security sector

The Quadrennial Homeland Security Review identifies the threats and hazards that challenge the U.S. interests from a homeland security perspective such as, the dangers of weapons of mass destruction; Al Qaeda and global violent extremism; risks posed by wide-scale cyber-attacks, intrusions, disruptions, and exploitations; pandemics, major accidents and natural hazards; illicit trafficking and related transnational crime; smaller-scale terrorism.

Those new threats, combined with traditional responsibilities in terms of security, represent the core homeland security missions, for which a set of objectives and capabilities are identified. As in the EU, DHS calls for compatible architecture and standards among the different end-users.

R&D in early stages is funded mainly through the Homeland Security Advanced Research Projects Agency (HSARPA), part of the Science and Technology (S&T) directorate of DHS, and the Defense Advanced Research Projects Agency (DARPA), which is dedicated to defense and has at its disposal a more significant budget (54B€ in defense R&D in 2008). HSARPA “*performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and universities.*”⁹

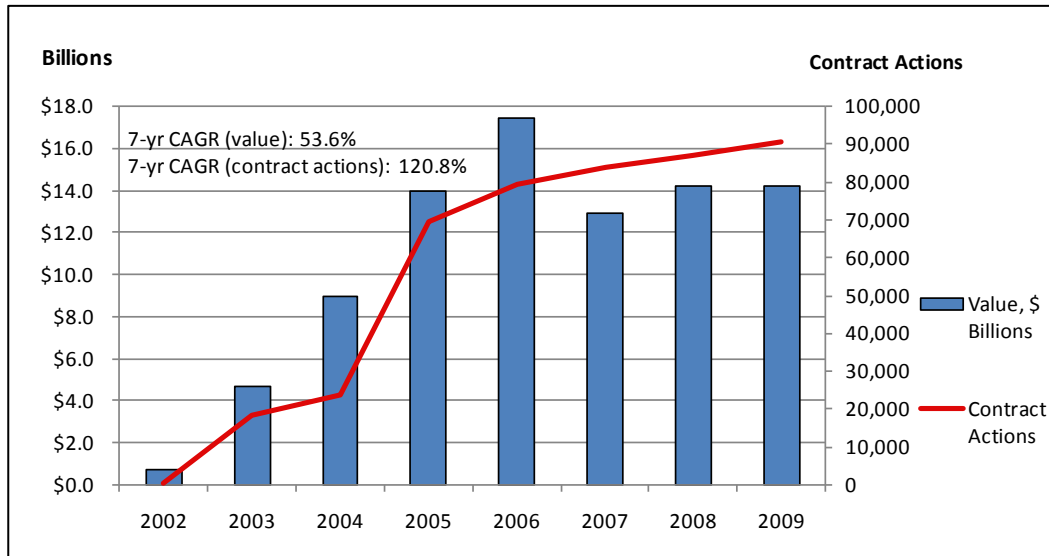
The budget request for the Science & Technology directorate is about 1.02B\$ for FY2011 (less than 2 percent of the total DHS budget, but certainly larger when compared to the EU plus national R&D resources). The R&D funding is allocated among the S&T directorate’s divisions, 6 of them correspond to the 6 areas HSARPA primarily focuses its activities on border and maritime security with 44.2M\$ in FY2010 funds; 206.8M\$ for chemical and biological programs and 120.8M\$ for research on explosives.¹⁰

Estimation of the U.S. security market size

From a historical perspective, federal funding for homeland security activities has constantly increased since 2002 with a light inflection in 2009. The total budget request for DHS in the FY 2011 budget is about 56.3B\$,¹¹ confirming an increasing trend (+2 percent of discretionary funding compared to FY 2010 levels). DHS resources are distributed among its components and agencies, for example, 20 percent to the Customs and Border Protection; 18 percent to the Coast Guard; 14 percent

to the Transportation Security Administration. Each of these bodies allocates part of the budget for procurement, although the FY2011 budget document does not specify the amount.

The following graphic illustrates DHS acquisitions by value and contract actions for the period 2002–2009. Despite the exclusion of the resources coming from other federal agencies, state and local authorities and the private sector, this graph shows the trend wherein more contracts are issued for less value. The large increase in 2006 reflects activity in the security market following Hurricane Katrina.



Source: Federal Procurement Data System, CSIS analysis.

CIVITAS Group, in 2006, published a study that estimates the total size of all federal government expenditure for homeland security (including expenses by other Departments and agencies) to more than 18.2B\$ as of 2006.¹² Moreover, they estimate that the state and local government spending on homeland security, which is accessible to the private sector at approximately 3.5B\$ for the same year, 2.7B\$ of which comes from a variety of federal grant programs.

Additionally, CIVITAS Group found that the private sector and quasi-governmental authorities spent about 9.3B\$ in 2006 on homeland security-related products and services.

Governmental reports and consultancies seem to agree that the increase in DHS spending, particularly the spending that will be captured by industrials and service providers, will only rise in the years to come. The Homeland Security Research Center report reveals that, over the next five years, the homeland security and homeland defense market, from the federal, local and nongovernmental levels, including the private sector, will grow at a CAGR of at least 5 percent from 69B\$ in FY2010 to 85B\$ in FY2014 with increased funding in some key market sectors such as cyber-security, bio-defense, information technology, C3I, perimeter and border security.¹³

Such analysis is, however, questioned by experts¹⁴ who consider that the economic slowdown and the federal budget deficit will have a relevant impact on the budget for security procurement.

Finally, with regard to the distribution of the homeland security and homeland defense budgets among customers, the report highlights the leading role played by state and local security authorities, with a share of 23.7 percent. The Department of Defense (DoD) follows with 22.5 percent and DHS takes the third position with 18.3 percent. This trend seems to create a certain paradox, as the procurement of security solutions remains somewhat decentralized. Despite the creation of DHS, the trend of increased funding to state and local grant programs started in 2001, ranging from 0 to 3.4B\$ in only 4 years.

Despite the existence of a more structured security market in the United States, the demand-side nevertheless, suffers from fragmentation, making the assessment of the overall security market's size difficult to ascertain. Resources allocated for R&D and procurement are more relevant than in Europe, making the United States the dominant world market in the security field.

EU-U.S. Security Market: The Supply Side

First Picture

A wide range of submarkets

The security market is not easy to define because it is an aggregation of market niches. It encompasses a wide range of product and services, from “traditional” security products such as physical access controls, CCTV, anti-intrusion and anti-fire detection/alarm, electronic surveillance tools, physical security measures and security guarding, passenger-screening or cargo-screening systems, biometrics ID systems, video surveillance systems, RFID, cyber-security systems, CBRN detection equipment. On both sides of the Atlantic, the current security solutions address the following key submarkets: aviation security, mass transit security, maritime security, critical infrastructure protection, telecommunications, data management, cyber-security, border security, counter-terrorism intelligence, disaster response and recovery.¹⁵

<i>Submarkets</i>	<i>Leading Technologies</i>
Aviation security	Screening Systems (Millimetre Wave Systems, Terahertz Systems, Backscatter X-Ray Systems)
Mass transit (public transport) security	Biometrics ID Systems
Maritime security (Cargo and port security)	RFID-Based Systems
Critical infrastructure protection (Electricity, Oil, Gas, Water Infrastructures; CBRN Detection Systems)	Cybersecurity Systems
Telecommunications, data management and cybersecurity	Counter-Terrorism Intelligence (Video surveillance systems, Databases)
Border security	CBRN Detection Systems
Counter-terrorism intelligence	
Disaster response and recovery	

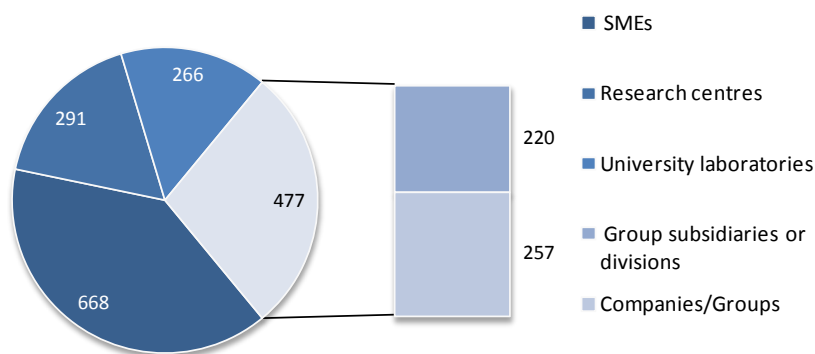
Source: Homeland Security Research Corporation, Jane's Information Group, and Security Industry Association; synthesized by authors Masson and Marta.

Competitor profiles

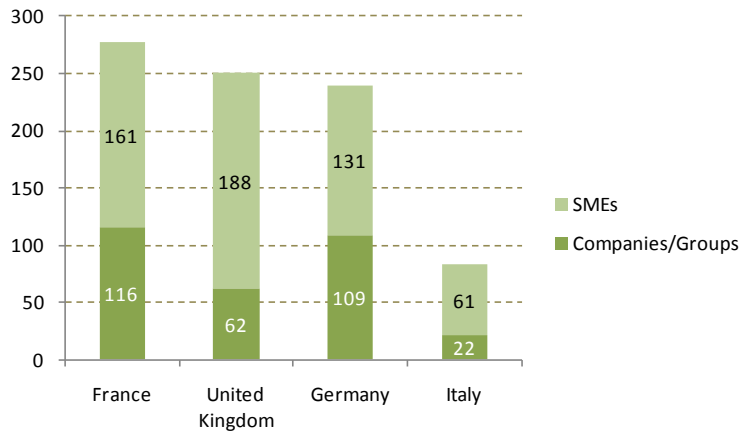
Regarding the suppliers profile, we can distinguish different types of competitors:

- **Suppliers of “traditional” security products.**¹⁶ The traditional private security industry is represented by well-structured trade associations, such as the British Security Industry Association (BSIA), or the Security Industry Association (SIA) in the United States representing electronic and physical security product manufacturers, distributors, integrators, and service providers.
- **Defense industry.** A number of defense business segments can address the capability requirements within security markets. According to Gert Runde, ASD Director Security and Defense: “Both future and current security solutions can derive important advantages from a spin-in of technologies that were developed by the European defense industry.”¹⁷ In this context, big defense companies realign their position for further growth in new and adjacent markets, drawing on their know-how and experience in the defense, electronics and aerospace markets.
- **ICT companies** (i.e. Sun Microsystems, Oracle, IBM, HP, Cisco, MacAfee). ICT companies that previously paid little attention to government contracts, look for business opportunities in the security market, seeking to respond to the growing needs within IT sector as expressed by the public administration, both in Europe and the United States.
- **Specialized Providers** (Mid-sized companies). As noted by Civitas Group “the growing homeland security market has encouraged the creation of many companies focused solely on this sector,” mainly in the United States.
- **A very large number of small innovative companies.** Start-up innovators,¹⁸ developers and providers of new security technologies, are addressing the security market, on both sides of the Atlantic. The *European Security Directory 2009* underlines that European SMEs are very active in the security field. Trade and industry bodies with “security capabilities/technologies,” definitions based on the ESRAB report, and excluding security guardian companies, represent around 668 SMEs. Also represented are 477 companies/groups (including 220 group subsidiaries or divisions with specific security technological or industrial capabilities and 257 Companies/Groups), and 557 research centers and university laboratories.¹⁹

European Security Industry

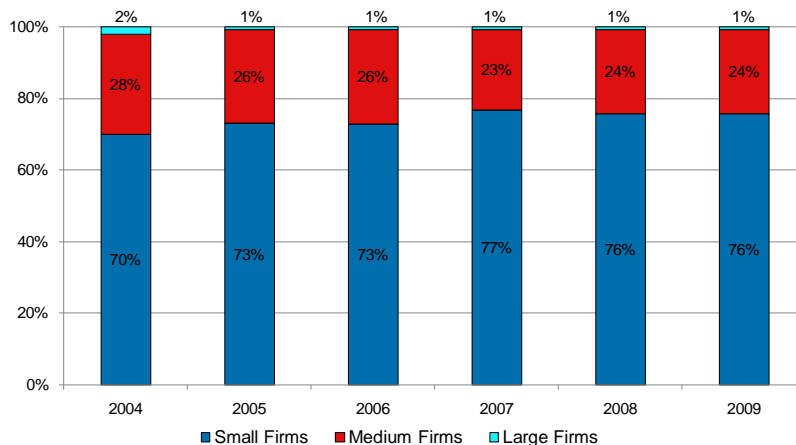


European Security Sector (companies, SMEs)



Source: ESD partner STI Database, 2009.

An in-depth analysis of the distribution, by number of contractors, of the DHS market to Small, Medium and Large firms for the period 2004–2009, made by the CSIS, stresses that more than 70 percent of DHS contractors are small firms.



Source: Federal Procurement Data System, CSIS analysis 2010.

Market Leaders

In the United States

All sources of information²⁰ converge on the fact that the big winners of the homeland security market, the top U.S. security companies, are mostly and generally all leading military contractors: Boeing, Lockheed Martin, General Dynamics, L-3 Com, Northrop Grumman, General Electric, Raytheon, Honeywell, Unisys, SAIC, to list the most prominent competitors.

DHS Top 20 firms, 2004–2009 (in constant 2009 dollars)

1	Integrated Coast Guard Systems	\$3,979,163,159
2	IBM	\$2,802,631,148
3	Unisys	\$2,285,665,607
4	Fluor Enterprises	\$2,019,273,571
5	Computer Sciences Corporation	\$1,721,588,994
6	Boeing	\$1,634,017,353
7	L3 Communications	\$1,479,312,139
8	General Dynamics	\$1,452,117,679
9	Accenture	\$1,414,790,101
10	Lockheed Martin	\$1,175,138,257
11	SAIC	\$974,475,308
12	Circle B Enterprises	\$974,220,637
13	Shaw Environmental	\$864,384,513
14	Northrop Grumman	\$784,353,608
15	Gulf Stream Coach	\$572,313,392
16	Morpho Detection	\$551,803,327
17	Cooperative Personnel Services	\$517,828,533
18	Bechtel	\$500,014,658
19	Nationwide Infrastructure Support Technical Assistance Consultants	\$486,384,667
20	CH2M Hill	\$465,347,424
	Total (2004-2009)	\$26,654,824,075

Source: Federal Procurement Data System, CSIS, 2010.

The homeland security contractors list includes mid-sized companies, and above all, major system integrators, which act as managers of large-scale homeland security programs:

- SBIInet program (Boeing)
- Bio Watch Gen-3 program (Northrop Grumman)
- U.S. Coast Guard Deepwater (Integrated Coast Guard Systems, a joint venture between Lockheed Martin and Northrop Grumman)
- FBI's Integrated Automated Fingerprint Identification System (Lockheed Martin)
- Integrated Wireless Network (IWN) program (General Dynamics)
- Transportation Security Administration Advanced Screening Technology programs (Unisys)
- Customs and Border Protection Agency Land Ports of Entry program (IBM)
- U.S.-VISIT Border Management program (Accenture)
- EAGLE IT Program (among the leading contractors are CACI, Booz Allen Hamilton, Lockheed Martin, SAIC, Northrop Grumman, General Dynamics, and BAE Systems)

Indeed, in five years, the top U.S. defense contractors have moved to consolidate their portfolio of products and services, and strengthened their market position by implementing the following strategic orientations:

- creation of “homeland security” new branch/division and/or subsidiaries

- strengthening the homeland security business by applying technologies and systems integration expertise developed in the defense market.
- acquisition of SMEs (small niche providers) with valuable technology, intellectual property and/or target market channels focused on intelligence and homeland security.

Major system integrators all have very similar and large portfolios with activities ranging from defense, intelligence and homeland security. Generally, they have built up strong positions through a number of acquisitions of smaller competitors and investments in homeland security, expanding their capabilities in information systems security/cyber-security, intelligence, critical infrastructure protection, and in a number of different specialty areas (i.e. detection).

Companies	Date / Firms acquired	Domains
Boeing	2008 / Digital Receiver Technology (DRT)	digital signal processing products
	2008 / Ravenwing	Cybersecurity solutions
	2008 / Kestrel Enterprises	Data management, development and systems integration, program management, training
	2009 / eXMeritus	Hardware and security software
	2010 / Argon	C4ISR and combat systems
Raytheon	2010 / Narus	Cybersecurity solutions
	2009 / BBN Technologies	IT, sensor systems, and cybersecurity
Lockheed Martin	2006 / SAVI Technology	RFID Equipment and solutions
	2007 / Management Systems Designers	IT and scientific solutions
	2008 / Eagle Group International	Logistics, IT, training and healthcare services
	2009 / Gyrocam Systems	Gyrostabilized optical surveillance systems
	2009 / Universal Systems & Technology	Interactive training and simulation, technical solutions
SAIC	2010 / CloudShield Technologies	Cybersecurity and management solutions
	2009 / Spectrum San Diego	Ultra-low-dose X-ray scanning systems
General Dynamics	2009 / Axsys Technologies	High-performance electro-optical and infrared (EO/IR) sensors and systems and multi-axis stabilized cameras
	2002 / Perkin Elmer	X-ray screening business
L-3 Com 	2006 / CyTerra Corporation	Advanced through-wall radar and explosive detection sensors for checkpoints
	2006 / SafeView	Non-invasive scanning systems
	2006 / TRL Electronics (UK)	Secure Radio and Satellite Communications for Defense and Homeland Security Applications (Electronic Counter Measures and cryptographic areas)
Northrop Grumman	2007 / Essex Corporation	Signal processing services and products, advanced optoelectronic imaging
	2007 / Xinetics	active optics such as deformable and hybrid mirrors, advanced wavefront control systems for real-time control of active optical systems
	2008 / 3001 International	Geospatial data production and analysis

Source: Authors.

European companies look overseas

The large European defense groups represent today's major competitors in the European security market. But, with a very fragmented and R&D-focused European market, these companies look, first and foremost, overseas for more profitable growth.

As shown by the UI's paper, *Challenges to Agenda-Setting Priorities: Toward Effective Public-Private Partnerships for Security in the EU and United States*, at EU level they have had an indubitable influence upon the shaping of the EU security-research agenda and various strategies and research projects. At the national level, the UK, French and German markets account for the largest share of

public spending, but fragmentation exists with regard to the many smaller programs, focused more on R&D than on procurement. Unsure of the European market demand and requirements, the industrial players are *de facto* and very active in pursuing business opportunities in the U.S. market, Middle East, North Africa and Asia.

Like their U.S. counterparts, European firms have acquired small and mid-sized companies in order to expand their portfolio of technologies and innovative forward-looking security solutions, opening new lines of business and entering new overseas markets. U.S. acquisitions include both defense companies doing homeland security work and stand-alone homeland security companies.²¹ In addition, European firms have developed a number of commercial and technology partnerships with U.S. providers.

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 the 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 businesses 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
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: Authors.

At present, European big players hold several key technological leaderships in the security market.

- EADS: PMR networks, Maritime security & coastal surveillance, integrated security systems

In 2003, the creation of the Defence & Security Division (today CASSIDIAN) underlined EADS' ambition to expand in the defense and security market. The acquisition in 2005 of Nokia's Professional Mobile Radio (PMR) activities has firmly established EADS as a global player in the secure telecommunication industry as well as defined it as the largest European PMR supplier. Furthermore, thanks to the acquisition of the French SME Sofrelog, EADS has consolidated its world market position in Vessel Traffic Services Systems and Coastal Surveillance Systems,

accounting for, as the world leader, more than 40 percent share of the market, ahead of Kongsberg (27 percent), and HITT (10 percent). The 650 M€ contract concluded between Romania and EADS in August 2004 represents the first important opportunity for EADS to showcase its capabilities in large-scale system integration in the border security domain. The project involves information and communication systems, equipment for checkpoints at airports and land borders, coastal surveillance systems and operation centers. The maritime component contributed to a win in July 2009 of the large Saudi Arabian national border surveillance program, which includes coverage of the Red Sea and part of the Arabian Gulf, beating competitors Raytheon and Thales. This award came after a number of contracts issued in the United Kingdom, Romania and Qatar and a subcontract for surveillance on the Saudi northern border. EADS is also pursuing homeland security opportunities in the United States. In order to sell its PMR solutions in the U.S. market and expand its industrial footprint. While solidifying its position in security systems and solutions, EADS also purchased PlantCML, a U.S. leading provider of emergency response solutions and services.

- **Thales: a dual-technology strategy**

Thales' security activities combine the group's former security and services divisions with the rail signaling and security systems businesses acquired from Alcatel-Lucent in January 2007. Following the operation, and in line with the company's dual-technology strategy, Thales adjusted its positioning and objectives for the civil security market, drawing on the group's mission, critical systems know-how and experience in the defense and aerospace markets. Thales' key technologies for the civil security market encompass secure information and communication systems (encryption), process supervision and control for critical infrastructure, sophisticated sensor systems (radars, infrared cameras, intrusion detection), biometric ID cards, electronic passports, command centers for the police and fire services, trusted e-government platforms, simulation and synthetic environments. In 2009, more than 20 percent of Thales' revenues came from its security systems, which totaled an approximate 2.9 B€ in 2009 (consolidated revenues 12.8 B€). The United Kingdom is the company's second largest country of operation after France and the leading European homeland security market. In this context, the acquisition in 2008 of the British company n-Cipher has further rounded out Thales' information security portfolio in addition to its information security services (internet and communications system security market).

- **SAFRAN Group: a world leadership in biometric and detection technologies**

Security activities reported 904 M€ in revenue in 2009 (9 percent of total revenue), divided in 3 major segments: secure identification (66 percent), smart cards (26 percent) and detection (8 percent). As part of the Defense Security branch,²² Sagem Sécurité is a world leader in biometric technologies for fingerprint, iris and face recognition and a major player in smart cards, identity management solutions, access management and transaction security. This business is positioned to become a major growth driver for Safran, and within a few years should generate 20 percent of the group's consolidated sales. Security business logged a 38 percent increase in sales and a 60 percent jump in earnings in the period 2005–2009. Since the acquisition of Motorola's biometrics business, Sagem Sécurité market share represents around 60 percent of the world AFIS market, ahead of Cogent and NEC. Moreover, with the purchase of 81 percent of the Homeland Protection division of General Electric, the group, already the world leader in biometrics, is now

number one worldwide in imaging systems that detect dangerous or illicit substances in luggage. Thanks to these two noteworthy acquisitions in the United States, Safran is building a real transatlantic biometrics and detection business.²³

- **Finmeccanica: expansion in the UK and U.S. homeland security markets**

The aerospace and defense Italian conglomerate, Finmeccanica, is positioned in both civilian and military safety-critical systems markets and delivers integrated solutions for non-military domains such as Critical National Infrastructure (CNI) protection, territory control and civil protection, maritime and border security and major event management and security. Within the field of Defense & Security Electronics, Finmeccanica operates through several subsidiaries, mainly based in Italy and in the United Kingdom (SELEX Galileo, SELEX Communications, SELEX Sistemi Integrati, Selex Services Managements, Elsas Datamat, and Agusta Westland). If Finmeccanica had consolidated its position in the UK security market, by launching a takeover bid for the British VEGA Consulting Services Ltd, the group has taken its U.S. footprint to a new level with the acquisition of the U.S. military contractor DRS Technologies for 4 B\$ in May of 2008. DRS has a prominent position in the U.S. security market (VTMS, port security, law enforcement, border control; subcontractor to Boeing on SBI-net). Thanks to the DRS portfolio, Finmeccanica is now considering possible bids on border control projects in the Middle East, North Africa and Central Asia).

- **BAE Systems: focus on information-based intelligence capabilities**

BAE Systems has established good positions in homeland security in both the UK and the U.S. security markets. Among the key European industrial players active in the U.S. security market, the group has established one of the most extensive market positions as the prime contractor or team member on a number of global contracts.²⁴ Alongside its established defense-related activities, BAE Systems has a growing position in national security with a focus on information-based intelligence capabilities (information technology, cyber-security, mission support and services), as well as seeks to capitalize on its leadership position in electronic warfare and infrared technologies. As a trusted provider of the U.S. DoD, BAE Systems has made a number of acquisitions related to defense, some of which are also related to homeland security. For instance, Armor Holdings, a U.S. maker of military and heavy vehicles (acquisition made in 2007) provides state and local police forces with mobility and protection systems (tactical vests, armor, helmets). BAE Systems are also engaged in extensive work in information technology for DHS. For instance, DHS has selected BAE Systems to develop a prototype for a system designed to protect commercial aircraft from heat-seeking, shoulder-fired missiles (JETEYE aircraft missile defense system). As a result of DHS grants, several municipalities have acquired their First InterComm first-responder interoperable communications system.

In the United Kingdom, BAE Systems has acquired Detica (2008), which is comprised of British civil IT contracts with the police, local government, banking, telecoms, transport, and health sectors. Furthermore, the group develops a number of partnerships with innovative UK SMEs in areas such as cyber-security, biometrics and intelligent surveillance systems (i.e. with the face-recognition British specialist Omniperception on developing a gait and facial behavior recognition to be integrated into street corner CCTVs).²⁵

Other European based mid-sized companies have gained stronger positions in the worldwide market, such as Konigsberg Maritime (tracking and tracing of goods for maritime transport submarket), or Smiths Detection in the air cargo security submarket (screening systems and equipment for x-ray screening and trace detection of explosives).²⁶

More generally, and as underlined by Ecorys Report, although Europeans hold technological leadership with regard to several products and services in the global security market, with the exception of the major players and a few mid-sized companies, the supply chain remains fragile.

U.S. industry, reluctant to pursue projects in Europe?

U.S. companies are already active in the international market, but their domestic market remains the most attractive and important. In Europe, the large number of competitors and the fragmentation of demand seem to have hindered competition from the United States. But U.S. defense groups like Raytheon, Northrop Grumman and L-3 Communications, which are well positioned in the British defense market, are counting on border security and IT projects to drive revenue growth overseas and to obtain entry into the civil security and surveillance market.

Raytheon is not only the most active company, but is the market leader due to its success in the UK market. In 2007, the group was selected as the prime contractor, by the UK Home Office, to develop and implement the nation’s e-Borders project, an advanced border control and security program. In December 2009, the Board of Directors of the European Organization for Security (EOS, a trade association) unanimously accepted Raytheon Systems Ltd as a new EOS Member, the U.K. affiliate of Raytheon Company. Northrop Grumman is a principal member of the BT team and was selected in December 2009 by the UK Technology Strategy Board to develop a cyber-test range for the research and testing of cyber security threats on large-scale networks. L-3 Communications also entered this market by acquiring TRL Electronics, a UK Leader in Secure Radio and Satellite Communications for Defense and Homeland Security Applications.

Conclusion/Recommendations

Despite the absence of a transatlantic political dialogue to identify common threats and common security missions, EU and U.S. official documents have revealed an impressive commonality of high level missions in the field of homeland security.

EU (ESRAB)	US (QHSR)
Border security	Securing and managing our borders
Protection against terrorism and organized crime	Preventing terrorism and enhancing security
Critical infrastructure protection	Safeguarding and securing our cyber space
Restoring security in case of crisis	Ensuring resilience to disasters
	Securing and administering our immigration law

Source: Authors.

Some differences exist in the approach toward key mission areas and their priorities, however, the capability and technology needs of both actors remain inherently similar.

Such similarity, thus, creates the necessary basis for transatlantic industrial cooperation within the security domain. Already special attention to certain industries is noticeable across the EU and the United States, particularly in biometrics, IT and secured communications. The European industry participation in the U.S. security market and the interest showed by some U.S. firms toward the EU confirms present-day transatlantic interaction and a more open market, when compared to the defense sector.

In order to foster cooperation, interoperability of solutions and common standards for next generation of security solutions is essential. Such a need is felt in the EU as interoperability is needed across the 27 member states as well as in the United States (across federal, state and local lines). The enlargement of transatlantic interoperability and standardization will also be crucial.

This dimension, which is transversal to all missions, has already been introduced at the transatlantic level in some security frameworks (i.e. FRONTEx, EDA). European high-level groups recognize the importance of this dimension recommending cooperation, especially with regards to standards and market access to third countries in the security FP projects. The launch of EU-U.S. R&D projects focused on the development of common technological building blocks could be the right starting point.

However, the economic slowdown on both sides of the Atlantic does not seem to offer the best window of opportunity for public investments, and industries seem to look to new emerging markets. The EC should support security procurement through European agencies in order to exploit R&D results financed with European resources.

In order to enhance the visibility of EU and U.S. security industries and SMEs as well as to assess the feasibility of industrial and technological cooperation in the security domain, the EU and the United States could co-organize an annual transatlantic security forum. Key institutions, stakeholders and end-users at the technical and operational level, rather than high political level, should participate and discuss the opportunities for partnership and contribute to information sharing, market trends analysis, channels for sales, key requirements, customer preferences and discuss the operating constraints and regulatory environment of the security market.



CHALLENGES TO AGENDA-SETTING PRIORITIES: TOWARD EFFECTIVE PUBLIC-PRIVATE PARTNERSHIPS FOR SECURITY IN THE EU AND UNITED STATES

Erik Brattberg, *Research Assistant, UI*, and Jan Joel Andersson, *Head of Security and Defence Programme and Senior Research Fellow, UI*

Introduction

This paper examines the relationship between governments and the evolving security industry in developing capacity to implement security strategies in the United States and in Europe,²⁷ respectively. We are interested in exploring if, and how, the security industry provides governments with the tools for carrying out strategies, and whether it does so in close cooperation with governments via institutionalized relationships. Our paper will explore that relationship, using the “traditional” defense industry relationship as an implicit comparison, to arrive at problem areas and issues for improvement. Our analysis is based on the premise that the relationship between government and industry is mutually dependent and supportive, rather than antagonistic or with industry as the only *demandeur* in the relations (as is the case in other policy sectors). Our main argument is that the industry-government relationship in the security domain is still evolving, hence sharply contrasting the defense industry, which has long-since evolved its capacity. The security sector, on the other hand, is still in the process of developing an efficient, effective and productive relationship with government so as to set the agenda. Our conclusion is that an effective and mutually supportive relationship between government and industry is crucial for the implementation of security strategies. As a result, this paper presents several recommendations for further strengthening cooperation between government and industry on both sides of the Atlantic.

This paper proceeds as follows: first we provide a brief overview of the traditional defense industry-government relationship in Europe and the United States. Then we account for the new security industry-government relationship on both sides of the Atlantic. Based on this discussion, we then draw some implicit conclusions about the changing nature of the industry-government relationship, point out some key similarities and differences between the EU and the United States, and some key challenges. Finally, we provide key recommendations for addressing these challenges.

The Traditional Defense Government-Industry Relationship

Europe

After a series of national and international mergers, beginning in the 1960s, the European defense industry has, as of 2010, reduced to only a handful of actors and countries. At the highest level, global companies such as BAE systems, EADS, Thales, and Finmeccanica are all among the top ten arms producers in the world. Rapid advance in technology development have made distinctions between aerospace, land armaments and naval systems less relevant. Today, BAE Systems produces the full range of armaments from artillery and fighter aircraft to nuclear attack submarines. Similarly, EADS produces military aircraft, electronic systems and missiles in several European countries. The exception to this trend of European and international concentration is the armored vehicle industry that largely remains fragmented across many programs and countries.

Behind this group of major arms producers, there are smaller, but still important European defense industry companies, such as the world's leading British engine maker Rolls Royce, major French naval producer DCNS, Swedish aerospace company SAAB and German armored vehicle specialist Rhinemetall. Moreover, there are several traditional defense industry companies in Europe owned by U.S. companies. Today, classic names such as Steyr-Daimler-Puch Spezialfahrzeug GmbH (STEYR-SSF) of Austria, MOWAG GmbH of Switzerland, and Santa Bárbara Sistemas of Spain are all part of General Dynamics European Land Systems (GDELS), a business unit of U.S. defense giant General Dynamics.²⁸

The traditional defense industry is organized into national defense industry associations. These organizations are in turn organized in the Aerospace and Defense Industries Association of Europe (ASD). Today, ASD members include 28 National Trade Associations in 20 countries across Europe, representing over 2000 aeronautics, space and defense companies. Together these companies employ a total of approximately 676,000 employees and a turnover of over 137 billion € in 2008.²⁹ The ASD is the result of a merger in 2004 of AECMA, EDIG and EUROSPACE to reflect the integrated nature of civilian and military technologies and between aerospace and defense. The simultaneous creation of the European Defense Agency (EDA) in 2004 meant that both the European defense industry and the EU, for the first time, had a unified contact point for discussion and exchange of views.

The EDA's mission is to support the EU member states and the Council in their efforts to improve European defense capabilities. The EDA's functions and tasks are to develop defense capabilities, promote Defense Research and Technology (R&T), promote armaments co-operation and to create a competitive European Defense Equipment Market and a strengthened European Defense, Technological and Industrial Base (EDTIB). By promoting coherence, these functions aim to improve Europe's defense performance. The argument is that a more integrated approach to capability development will contribute to better-defined future requirements in which collaborations - in armaments or R&D or the operational domain - can be built. More collaboration will not only provide opportunities for industrial restructuring but also promote larger demand and an expanding market.³⁰ The EDA is the central actor for EU discussions on the defense industry. The central role played by the EDA is underlined by the fact that the Agency's "shareholders" are not only the member states participating in the Agency but that the key stakeholders also include the Council and the

Commission as well as third parties such as OCCAR (Organisation Conjointe de Coopération en matière d'Armement), the LoI (Letter of Intent) group and NATO.³¹

United States

The traditional U.S. defense industry is the largest and most sophisticated in the world. Six of the seven largest defense companies and 16 of the world's 20 largest defense companies are American. Similar to the development in Europe, the U.S. defense industry has undergone a series of major mergers. Today, the traditional U.S. defense industry is dominated by a dozen companies led by Lockheed Martin, Boeing, Northrop Grumman, General Dynamics and Raytheon. Each of these companies has numerous production sites spread around the country and post arms sales ranging between \$20–\$30 billion per year.³² With nearly 3.5 million people employed in a defense-related industry, the traditional U.S. defense industry carries significant political clout at the local, state and federal level.

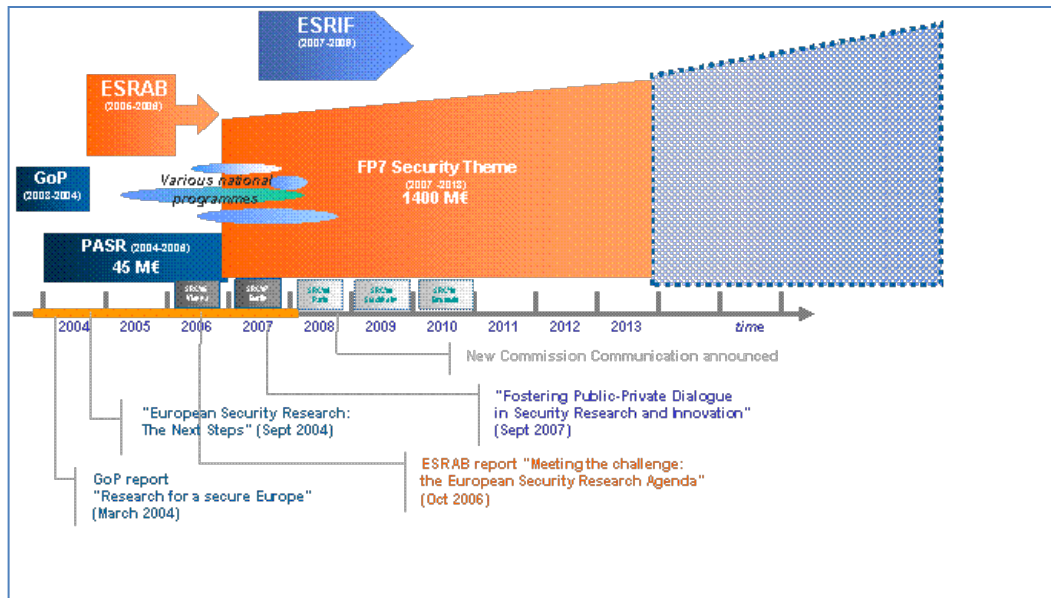
The relationship between the U.S. government, the U.S. military and the defense industry has long been very strong. For decades, a network of contracts and flows of money and resources between the defense industry, the Pentagon, the Congress and the Executive Branch have made relations between industry and government very close. The long tradition of government officials and retired military officers taking up positions in the private industry and the tendency of government to recruit procurement managers and policy specialists from industry, also lead to shared understandings and multiple access points to influence government policies. Such policies include approval for research, development, production, use, and support for military training, weapons, equipment, and facilities within the national defense and security policy.

The New Security Industry-Government Relationship

In this section we will discuss the changing security industry-government relationship in Europe and the United States. For both sides of the Atlantic, we will (i) focus on the expansion of the security agenda and (ii) describe the security industry.

The Widening of the European Security Agenda

While most security funding in the European Union remains available at the national level, the need to develop a European Security Research Program grew out of the awareness that Europe risked exclusion from the growing market of scientific research and technological innovation related to new security measures. To help remedy this situation, the EU started a process of consultation and coordination to fund security research and help the structuring of the market in the security sector. This process started with the *Group of Personalities* in 2004 and was followed by the *Preparatory Action for Security Research* (2004 to 2006), the *European Security Research Advisory Board* (ESRAB from 2005 to 2006), the *European Security Research and Innovation Forum* (ESRIF from 2007 to today) and the *FP7 Security Theme* (2007-2013), summarized in the figure below. The next section will begin by taking a closer look at the development of the EU security research program starting with PASR to the FP7 security theme.



Source: See http://ec.europa.eu/enterprise/policies/security/industrial-policy/research-agenda/index_en.htm.

Group of personalities in the field of security research (2002-2004)

In order to develop longer-term public-private cooperation on European security research, the European Commission, in 2003, set up the “Group of Personalities” (GoP), composed of high-level industrialists, Members of the European Parliament (MEPs), and representatives of international organizations and research institutes, whose purpose was to lend their expertise in establishing a strategy for a secure Europe and to spearhead the process of enhancing the European industrial potential in the field of security research.³³ The GoP presented to the Commission a report entitled “Research for a Secure Europe,” advocating the combination of national, intergovernmental and community research across the civil-military continuum and the development of a ESRP, with respect to civil liberties and ethical principles. Twelve recommendations were put forward and the guarantee that a minimum of €1 billion per year in funding would be allocated for research in the security field, in addition to existing funding. The GoP also recommended the establishment of a European Security Research Advisory Board “to draw strategic lines of action and to prepare the research agenda of a European Security Research Program as well as to advise on the principles and mechanism of its implementation. In September, 2004 the Commission published the communication “Security Research: The Next Steps” endorsing GoP’s recommendations.³⁴

Simultaneously, the Commission launched the Preparatory Action for Security Research (PASR), toward the end of the 6th Framework Program for research (FP6), aiming at harmonizing security research activities in Europe, coordinating existing capabilities and competences and preparing the groundwork for the introduction of the security theme in the next Framework Program. Between 2004 and 2005, three proposals led to the funding of 39 R&D projects totaling 45M€. The main

thematic areas of research included: crisis prevention and crisis management systems; space surveillance; critical infrastructure protection; and protection against terrorism.³⁵ PASR also served as the predecessor to the Commission's full security research program, the FP7 (see below).

European Security Research Advisory Board (ESRAB) (2005–2006)

The European Security Research Advisory Board (ESRAB) was established in April 2005 as an attempt to bring together, at European level, the market's demand and supply sides in order to jointly define commonly agreed upon strategic guidelines for European security research. It was tasked to ensure consultation and cooperation among all stakeholders in order to outline a comprehensive European security research agenda as well as to establish a network between end-users and stakeholders to identify technological capabilities. Additionally, it sought to provide advice on the strategic and operational aspects of the future program and on its implementation.³⁶ Consisting of some 50 high-level specialists and strategists, including public authorities (including MEPs and Commission's officers), think tanks and research institutes, research and technology suppliers and industry representatives, ESRAB's final report, entitled "Meeting the challenge: the European Security Research Agenda," was released in September of 2006. This report offers a strategic framework to structure the research content covering both technological and non-technological aspects, identifying and prioritizing only those areas which offer high potential to deliver European added-value. Among other things, the report recommends that European security research compliment national security research programs, and where these already exist, align themselves to EU programs.³⁷ The ESRAB report identifies three areas of cross cutting interest for security research: integration, connectivity and interoperability; capabilities and technologies; and demonstration programs (e.g. capability development, system development, and systems of systems demonstration).

European Security Research and Innovation Forum (ESRIF) (2007-2008)

In line with the final GoP report, the European Security Research and Innovation Forum (ESRIF) was established in September of 2007 to serve as an informal and voluntary group of experts representative of both the demand and the supply sides of the security sector and various societal organizations. To date, ESRIF has 64 formal members.³⁸ In addition, more than 600 individuals have registered as contributors to ESRIF's 11 working groups, providing a broad basis for the forum. ESRIF was established to develop a mid and long-term (up to 20 years) European Security Research and Innovation Agenda (ESRIA) linking security research with security policy making, through public-private dialogue by 2009.³⁹ Accomplishing this objective, ESRIF brought together industry, public and private end-users, research establishments, universities and non-governmental organizations from 32 countries. ESRIF's final report contained a set of key messages addressing the necessity of a future European security and relevant research, the need to reduce the fragmentation of the security market as well as the need to enhance the currently insufficient degree of interoperability and standardization.

FP7 "security theme"

To promote security research in Europe, the Commission has launched two, seven-year Framework Programs in the security domain, totaling €2.135 billion in funding over the 2007–2013 period. The

first is the FP7, which was launched by DG Research in 2007 and will last through 2013.⁴⁰ Under the FP7, the European Commission has made €1.4 billion specifically available for the security research theme (out of a total budget of €50 billion). This is the first time that DG Research has funded research in the security area, including “security of citizens,” “critical infrastructure,” “surveillance,” “border security,” and “crisis response.” This figure is somewhat misleading, however; security-related projects within other themes can also be identified, such as “information and communication technologies,” “transports,” and “space.” Additionally, under the FP7 framework is the Joint Research Centre (JRC), a research-based policy support organization to the Commission providing the scientific advice and technical know-how to support a wide range of EU policies touching five policy themes. The FP7 will provide the JRC with €1.8 billion for research across four priority areas. At least two of these themes—“security and freedom” and “Europe as a world partner”—relate to security.⁴¹ The second is the EU Framework Program on “Security and Safeguarding Liberties” with a budget of €745 million provided by the DG for Home Affairs.

The New Security Industry in Europe

This section will focus on the participation of industry in shaping the EU’s security research agenda. The GoP included 25 members, among them four members from Europe’s four largest aerospace and defense companies (EADS, BAE Systems, Thales, Finmeccanica) and four representatives from the ICT sector (Ericsson, Indra, Siemens and Diehl). In this context, Didier Bigo and Julien Jeandesboz conclude 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.”⁴² In ESRAB, out of a total of 50 personalities, 28 percent were industry representatives (bio, manufacturing and ICT), 36 percent from EU member states (ministries of Defense and Interior and police forces) and 28 percent from research institutes and academia. Since September 2007, EADS, Thales, Safran (Sagem), Finmeccanica, SAAB and Smiths Group are all members of the voluntary strategy group ESRIF, serving as rapporteurs of four Working Groups in charge of drafting building blocks for the security research agenda.

Beginning with the GoP, through to the PASR, to the ESRAB and ESRIF today, the biggest European defense companies have had an indubitable influence upon shaping the EU security-research agenda, strategy and research projects. Their inputs are noticeable in writing the three EU security research strategy reports. Furthermore, European defense companies have also benefited considerably from the EU security research programs. Of 39 security research projects (PASR 2004-2006) and 45 FP7 projects (first call), 21(54 percent) and 7 (15,5 percent), respectively, were led by European defense groups. Thales is the most active industrial player, participating in 23 projects, coordinating 8, followed by Finmeccanica, EADS, Safran/Sagem DS, BAE Systems, Diehl, SAAB, Dassault Aviation and Indra. Thales, EADS and Sagem DS are the most recurrent.

The industry has also sought to influence EU security policies through participation in the European Organization for Security (EOS), an association of European private-sector security actors founded in 2007. The organization’s primary goal is to support the development of a European security market by promoting innovation and implementation of European civil security capabilities. EOS recently produced a report entitled “Priorities for a Future European Security Framework,”

which contains a number of recommendations over a five-year period (2010–2014) on how to implement a structured European security framework.⁴³ These suggest:

- developing a comprehensive, coherent and sustainable EU model for security;
- strengthening the Public-Private Security Dialogue in support the development of security policies;
- creating, under the umbrella of an EU Security Program, relevant EU sectorial programs (such as Borders Control, Civil Protection, Protection of Resilience and Critical Infrastructures and Services, Security of Transport, Cyber Security);
- creating conditions for the development of a harmonized EU Security Market by establishing legal frameworks and societal/privacy aspects linked to security.

The creation of EOS was encouraged by the European Commission, which hopes to see the security industry become a more organized “counter-part” to help consolidate the European security market and considers EOS to be a viable alternative to the Aerospace and Defense Industries Associate of Europe (ASD).⁴⁴

With regard to ASD, its key priorities include future security research programs “that are fully geared to operational objectives, technology developments and to strategies for innovation implementation.” It also seeks to establish an appropriate and robust defense industry, proper market policies at EU level and a harmonized European Security Environment.⁴⁵ With regard to the latter priority, ASD notes that the current European security market is characterized by many purchasing authorities that coexist and act in limited coordination. Furthermore, ASD perceives the EU security market as “highly fragmented and unstructured.” ASD, therefore, seeks to increase competitiveness and reduce market fragmentation through the development of a comprehensive and sustainable European industrial security policy as well as a structured public-private dialogue between the demand and supply sides.⁴⁶

The Rise of Homeland Security in the United States

The 9/11, 2001 terrorist attacks highlighted the vulnerability of the United States to a “new” range of transnational threats and brought impetus for a homeland security overhaul. This process culminated with the establishment of the Department of Homeland Security (DHS) in late 2002. By consolidating many of the essential departments and agencies previously charged with providing for homeland security activities in the United States, DHS became responsible for identifying and developing plans for protecting critical infrastructure; conducting intelligence gathering and analysis; exercising the mechanisms to enhance emergency preparedness; coordinating and sharing information with other executive branch agencies, local and state actors and with non-federal entities.

But DHS has also come to play a key role in supporting homeland security research. For this task it has formed the Directorate of Science and Technology (S&T) to help organize scientific, engineering and technological resources for the various homeland security missions.⁴⁷ S&T partners include federal state and local agencies as well as laboratories, universities and the private sector. The Basic Research Focus Areas of the S&T Directorate were generated from six divisions of the Research Leads in the Directorate with input from the research community and vetted through the S&T

Directorate's Research Council. These focus areas represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs and help guide the direction of the S&T research portfolio to provide long-term science and technology advancements for the benefit of homeland security. These six focus areas are: Explosives Division Focus Areas (EXD), Chemical and Biological Division Focus Areas (CBD), Command, Control, and Interoperability Focus Areas (CID), Infrastructure and Geophysical Division Focus Areas (IGD), Human Factors Division Focus Areas (HFD), and Borders and Maritime Division Focus Areas (BMD).⁴⁸

The prioritized research needs initially focused on the area of counterterrorism. Currently, DHS spending on homeland security R&D is \$1.1 billion, a 9.2 percent increase from the 2008 fiscal year.⁴⁹ The largest sector of the DHS R&D portfolio is Domestic Nuclear Detection Office (DNDO). DNDO was removed from the S&T Directorate in 2006 and is now an independent entity devoted to radiological and nuclear counter-measures. The second biggest area is the chemical and biological countermeasures portfolio which is located within S&T. Furthermore, DHS research, excluding development funding, is heavily oriented around the life sciences and engineering. The research portfolio as a whole is currently expected to continue growing, as research becomes a larger part of DHS R&D and development funding declines.⁵⁰

Besides the Department of Homeland Security, several other federal agencies are involved in R&D efforts pertaining to the area of homeland security. Prior to the establishment of DHS, homeland security-related R&D was spread out across various federal agencies, but since its creation, much of this funding has been channeled specifically to DHS. However, some homeland security R&D funding remains with other federal agencies, including the Departments of Health and Human Services, Defense, Agriculture, and Energy and the Environmental Protection Agency.

The Homeland Security Industry in the United States

The reorientation of the U.S. security environment following the 9/11 attacks paved the way for an explosion of government spending in the homeland security area. According to HSToday, an industrial magazine, the homeland security industry “has grown at an extremely fast and disorganized pace.”⁵¹ In the early period following 9/11, the U.S. homeland security market tended to be dominated by smaller firms already specialized in homeland security technologies. But the growth and consolidation of the market soon attracted larger companies with extensive experience in government contracting to join the field, including traditional defense companies such as Halliburton, Lockheed Martin, Raytheon, and Northrop Grumman.⁵² According to Lockheed Martin's Senior Vice President, Art Johnson, larger companies have benefited because they have already established government contacts with the various agencies before they were merged into the DHS.

According to directory maintained by HSToday, the homeland security field now consists of some 300 companies,⁵³ while the *Washington Post* has listed almost 2,000 companies working on programs related to counterterrorism, homeland security and intelligence in the United States.⁵⁴ The initial focus of the homeland security market was airport security. The industry has since then expanded to include a wide range of different companies, including chemical, biological and radiological detection; border, rail, seaport; industrial and nuclear plant security; integrated technology and surveillance, etc. Even though most government contracts go to larger companies, smaller companies benefit as they serve as sub-contractors to these companies. During the FY 2005,

roughly a third of all government contracts went to smaller companies. Increasingly, however, U.S. government spending on homeland security is also going to so-called second-generation anti-terrorism products. Concurrently, homeland security spending has departed from the initial focus on terrorism and is exceedingly “all-hazards” oriented. In the aftermath of Hurricane Katrina a number of engineering and construction companies became major contractors to FEMA, which in FY 2006 accounted for roughly a third of the DHS procurement budget.

Unlike the traditional defense market in the United States, a significant challenge to security companies is customer fragmentation. Success in the homeland security market depends on the ability to sell to multiple customers of varying size: federal governments, state and local governments (counties and cities) and the private sector. While DHS plays a key role in homeland security, it is far from dominating the demand side of the market. The combined FY 2010 for state and local markets totaled \$16.5 billion, whereas the DHS homeland security market totaled \$13 billion. However, DHS still plays a major role in shaping the industry. The creation of DHS has contributed significantly to the growth in the number of homeland security providers (both in terms of products and services), new companies and new divisions of existing companies. Less than 1 percent of federal contracts in 2000, DHS outsourcing has quadrupled as a portion of federal contracting from 2003 to 2009.⁵⁵ Contrary to the confusion of its earliest days, DHS seems to have stabilized its policies and operations, with consistency programs and long term commitments of funding for acquisitions.⁵⁶ For instance, we can note a notable expansion of the involvement of DHS in long-term programs, particularly in electronic identification, cyber-security and critical infrastructure.

The growth of the homeland security market has attracted traditionally non-security oriented companies to enter the market and has encouraged the creation of many companies focused solely on this sector. According to Civitas Group, the dual-use nature of many of the homeland security sector’s applicable core technologies and its close alignment with the defense, intelligence, information technology and, in some cases, biotech markets, has also allowed established technology companies to diversify across a number of growing markets. It has also provided the opportunity for security-focused companies to diversify into adjacent sectors. This dynamic is contributing to the development of a market increasingly defined by a number of large companies at the top, a large and vibrant pool of small, innovative companies at the bottom, and a select few in the middle. Moreover, IT and software technology companies (e.g., Sun Microsystems, Oracle, IBM, HP Enterprise Company, HP, Cisco, MacAfee) that previously paid little attention to government contracts, now look for business opportunities in the homeland security market in the context of growing needs in IT Security expressed by the federal government/agencies and declining commercial spending.

The growing importance of services (from IT integration, engineering consulting, and management support to construction, guard services, and facility management), areas where DHS spends the most money, represents another trend, which has become more and more noticeable. This trend explains the growing involvement of service providers.⁵⁷ In five years, the top U.S. defense contractors have moved to consolidate their portfolio of products and services and strengthened their market position by implementing the following strategic orientations: creation of “homeland security” new branch/division and/or subsidiaries; strengthening the homeland security business by applying technologies and systems integration expertise developed in defense business; and acquisition of SMEs with valuable technology, intellectual property and/or target market channels focused on

intelligence and homeland security. Large defense companies retained their competitiveness on the homeland security market because they also had existing ties to various agencies that were wrapped into DHS when it was created. They anticipated a reduction in defense budgets and a shift in customer priorities, and then realigned their position to allow for growth in new and adjacent markets, while continuing to serve existing defense customers. Moreover, as noted by Civitas, the end-user demand for integrated solutions is a dominant characteristic of this market, a characteristic that tends to favor large systems integrators who can provide both the hardware and the necessary IT backbone for such systems.

Public-private relations in the U.S. security sector

In the United States, the security industrial base has not established separate formal mechanisms to interact with the public authorities in charge of developing homeland security requirements and acquisition policies. DHS acquisition policy is governed by the Federal Acquisition Regulation (FAR), which governs all government acquisition (the Department of Defense has the Defense Federal Acquisition Regulation Supplement - DFARS). No prominent industry associations exist that are dedicated solely to homeland security. There are formal committees under DHS that include industry members, but their interactions are controlled and must be conducted under the Federal Advisory Committee Act. Lobbying activities are closely regulated and lobbying by a specific company on a specific acquisition program cannot be undertaken with the responsible government entity while the acquisition is being considered.

However, defense companies, many of which also undertake work for DHS, use the existing national security trade associations and advocacy groups to also represent their interests in the homeland security domain. As a result, behavioral patterns and practices characterizing the defense sector seep into the security domain, despite the lack of a strong separate trade association or robust formal processes to influence the security agenda-setting as exist in Europe through ESRAB, ESRIF and so on.

What emerges from this analysis is a U.S. situation substantially different from the European one. In Europe, given the lack of a public authority dealing with security policies and procurement, companies commit themselves to joint efforts to institutionalize public-private partnerships in the security domain. In the United States, DHS centralizes the majority of federal decision-making and procurement policies and the FAR regulate all federal acquisitions. Companies, by themselves or through associations and lobbyists, attempt to influence government acquisition within a well-defined legal framework. Defense companies are better positioned to do so via the trade associations in place to represent them vis-a-vis the Department of Defense.

Conclusions

Whereas the Cold War environment was based on clear external threats from state actors which required traditional defense capabilities, the new security environment is characterized by new forms of both actor-based and structural threats, making security capacities harder to define. The changing threat environment and the different defense capabilities needed to handle new threats have paved the

way for “new” security industries in Europe and the United States. In both the EU and the United States, it is possible to contrast the emerging security industry-government relationships from the traditional defense-government relationships in two major ways.

First, the type of companies is different. Whereas the old defense industry was dominated by a handful of large companies with the capacity to produce large-scale weapons, the new security industry consists mostly of mostly smaller companies with niche specialties. It appears as though the traditional large defense companies have not been adequately prepared for the new security environment. Even though many larger companies are now entering the security market, a rapidly growing number of smaller companies with niche specialties in areas such as border security have already sprung up, particularly in the U.S. DHS seems to favor using existing civilian technology for homeland security application rather than developing new technology from scratch. In the EU, however, many smaller companies find the FP7 applications overly bureaucratic and the administrative burden too high.

Second, the type of government relationships is also different. Before, the large defense companies could enjoy “cozy” and heavily institutionalized relations with national governments, today this is much more difficult due to market fragmentation, on the one hand, and the lack of organization of the industry, on the other. At the same time, it appears that big traditional defense players have been able to leverage existing government contacts to some degree in both the EU and the United States. Of note is the fact that the EU has made specific efforts to cultivate and institutionalize relationships with the security industry and supranational governance in Europe, which is by definition a major contrast with the defense-government relationship of earlier years.

What then are the specific challenges pertaining to the new security industry developing in the EU and the United States and how are they best addressed? First, end-users are highly diverse. With several government buyers at both the national, regional and local level and with non-profit and private sector buyers, the market perceives a lack of predictability. The industry accordingly needs predictable funding and regular procurement requests as well as a predictable market for products. Furthermore, the industry needs clearer funding agendas and needs assessment by governments. Furthermore, public-private partnerships in the field of security research is of utmost importance in order to increase the security of infrastructures, to fight organized crime and terrorism, to help restore security in times of crisis and to improve surveillance and border control. Governments cannot pursue security for its citizens without being closely aligned with the security industry at both the policy formation and implementation stages. A characteristic of the security area is that much of the critical infrastructure remains in private hands. Industry actors must hence be involved in formulating requirements that prepare for future threats and aid in the countering of such threats. Finally, there is a need for greater integration of industry in agenda-setting. Here, the EU has arguably made more progress than the United States, incorporating industry in high-level working groups to assist the Commission in identifying industry expertise and capacity, etc. Conversely, there has been a lack of involvement within industry in defining the needs of the homeland security market in the United States—in clear contrast to involvement in the defense sector.



THE REGULATORY AND ACQUISITION ENVIRONMENT FOR SECURITY IN THE EU AND THE UNITED STATES

David Berteau, *Senior Adviser and Director, Defense-Industrial Initiatives Group, CSIS*; Guy Ben-Ari, *Fellow and Deputy Director, Defense-Industrial Initiatives Group, CSIS*; Priscilla Hermann, *Research Assistant, CSIS*; Sandra Mezzadri, *Associate Fellow, IAI*

This paper provides an assessment of the regulatory environments for security and homeland security in the United States and the EU through July 2010. This evaluation is an important element in the analysis of security strategies, as it defines the field of action for industry on both sides of the Atlantic and has a heavy impact on the development and fielding of security-related capabilities. The pieces of legislation discussed in this report are by no means comprehensive, yet allow for an understanding of current market conditions and provide the basis for comparative analysis.

Security Market Regulatory Environment in Europe

Introduction

The main features of the regulatory environment for the security market in the EU are complexity and fragmentation. There is nothing like a single regulatory framework for the security market, but a multitude of different rules and regulations with different purposes for different areas. The reasons for this are the characteristics of today's security environment, the specificities of security markets and the current state of European integration.

First, it is generally recognized that the main security threats today are not large-scale military conflicts, but regional crises, natural disasters and threats from non-governmental actors, in particular terrorism and organized crime. The latter often operates globally, in transnational networks, blurring the dividing line between internal and external security. Facing such threats, governments in the EU and around the world have redefined their security and defense concepts and started to develop a comprehensive approach, combining a broad variety of policies, instruments and actions. Consequently, the areas in which security relevant rules and regulations exist are as numerous as diverse.

Second, security markets are specific and highly regulated markets. In this respect, they have some similarities, but also important differences with defense markets. Whereas the demand-side in defense markets is exclusively public and centralized at the national level, the demand-side in security markets is public and decentralized (regional, national, local), but also private. This is the case in particular for operators of critical infrastructures. At the same time, the latter's demand for security (in particular against high-end security threats) is often driven by rules and regulations set by public authorities. In other words, public actors shape the security market as both customers and regulators, making the regulatory environment inevitably even more complex.

Third, in the EU, national and European laws co-exist. Although regulation of the security market occurs primarily at the member state level, the EU is actively promoting legislative harmonization and coordination. The Lisbon Treaty's renaming of the European Security and Defense Policy (ESDP) as the *Common Security and Defense Policy* is one such example. Security-related areas which fall under the direct competency of the Commission include, but are not limited to, research, transport, public procurement rules and standards. In addition to the legislative constraints caused by member state regulation, the Commission faces internal difficulties. The numerous Directorates General and Agencies simultaneously responsible for security activities contribute to the decentralized nature of this market sector and compound the level of bureaucratic complexity. Implications for the security market include poor product and service coordination and schedule delays.

Due to this complex regulatory environment, developing a comprehensive overview of the European security market is difficult. Assessing, in an exhaustive manner, legislation across all 27 member states and analyzing the implications for industry far exceed the size and scope of this report. Our objective is, therefore, to provide insight into the current regulatory framework of the EU focusing on three primary areas: the legislative environment for high-end security activities across the key mission areas, the Protect mission area and the recent developments in public procurement.

To begin, we will look at the EU's general policy and strategic framework for high-end security activities, regrouping the multitude of rules and regulations along four capability areas related to EU actions on counter-terrorism: prevent, protect, pursue and respond. Secondly, we will take a closer look at the Protect capability area which covers security sectors of major interest to industry, such as infrastructure security. These sectors are also the most regulated at EU level. We will also identify the challenges ahead and the limits of the current EU legislation.

Finally, we will analyze the new Defense Procurement Directive 2009/81/EC—which constitutes the only piece of legislation in the EU that applies to defense and security-related activities.

Main Features of the EU Security Regulations

EU legislative environment

EU legislation regulating the security market is quite recent. It is primarily “threat”-driven and seeks to respond to particular areas of weakness rather than provide long-term risk management and planning. It is also limited in scale and scope, with only a few binding legislative acts. The way and degree to which these EU legislative acts affect national law differs depending on the instrument used. Directives of the Council and the Parliament, for example, harmonize and coordinate national

legislation; regulations of the Council and the Parliament, by contrast, become directly part of national law and leave no room for interpretation. Different types of implementing acts do not set new law but modify and update existing EU-law.

EU-wide security initiatives

As there is no single security regulatory framework for the security market at the EU level, it is necessary to look at the main EU security policy and strategy documents to identify the future objectives for this sector. There are a number of key documents which set the framework for EU policies and actions and guide the launch of regulations in the security market, particularly in the “high-end” sector:

- the EU security Strategies: the 2003 Security Strategy⁵⁸ complemented in 2010 by the Internal Security Strategy⁵⁹
- the Counter-terrorism Strategy, with the latest update in 2010⁶⁰
- The Stockholm Program adopted in 2009 and the related Action Plan of April 2010.

These policy documents show that in the years following 2001 terrorism was indeed the main driver for measures in the field of security threats. The London and Madrid attacks helped to keep terrorism high on the political agenda as the principle security mission, which guided and shaped the others. An Action Plan to Combat Terrorism was adopted in 2001 and was complemented in December 2005 by a Counter-terrorism Strategy. The EU Security Strategy of 2003, which guides the EU’s Security and Defense Policy, was also strongly influenced by the terrorist attacks.

Over the last five years, however, we can observe a shift in security priorities at the EU level. Counterterrorism remains a major area of action; however, the Internal Security Strategy of 2010 and, more important, the Stockholm Program of December 2009 show that the EU’s Security framework has broadened considerably with a stronger emphasis on citizens’ direct interests, needs and perceptions. The Stockholm Program, subsequent to the Hague Program (2004–2009), is a comprehensive plan of EU justice and security policies for 2010–2014. The Commission has recently turned these political objectives into an action plan for 2010–2014 focusing on measures in the area of Justice, Fundamental Rights and Citizenship (such as improvement of data protection in the EU) and in Home Affairs (such as strengthening cooperation in civil protection as well as in disaster and border management).

More generally, security regulations and initiatives across the EU are systematically categorized across four capability areas: prevent and anticipate threats, protect citizens and infrastructures, pursue and investigate criminals, and respond by managing the consequences of a disaster.

The measures and initiatives initiated under the “Protect” pillar have the most effect on the security market as they require high value investments in infrastructure protection and border security and often produce new security standards.

Protection

The area “Protect” can be classified in 3 main priorities:

1. Protection of citizens: with measures such as securing EU passports through the introduction of biometrics;
2. Protection of borders (sea and land): with the establishment of the Visa Information System (VIS) , the second generation Schengen Information System (SIS II); and the development of risk analysis of the EU’s external border via the establishment of Frontex;
3. Protection of infrastructure (aviation, maritime and rail): with the implementation of agreed common standards on civil aviation, port and maritime security; the development of a European program for critical infrastructure protection; and the promotion of EU and Community level research activity.

The following section will address the regulatory frameworks for critical infrastructure protection. These mission areas are critical for European security and will, to a large degree, dictate the future regulatory environment for security across all 27 member states.

Legislation

- The terrorist attacks in Madrid and London highlighted the risk of terrorist attacks against European infrastructure. The EU responded in adopting a framework (EPCIP) for the protection of critical infrastructure that would develop a common level of protection in Europe. The objective was to make sure that each member state would provide adequate and equal levels of protection concerning their critical infrastructure and that the rules of competition within the internal market would not be distorted.
- More specifically, the Commission adopted in October 2004 a Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism."⁶¹ This Communication provides, in particular, a very broad definition of critical infrastructures covering a wide range of sectors: energy installations and networks, communications and information technology; finance (banking, securities and investment); health care; food; water (dams, storage, treatment and networks); transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems); production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials); government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).
- In 2006, the Commission adopted a policy package on EPCIP composed of a Communication (COM (2006)786 final) and a Directive (COM (2006) 787 final). The Communication deals with general policy in connection with EPCIP, whereas, the Directive focuses on the designation of critical infrastructure of a European dimension (European Critical Infrastructure or "ECI").
- In 2008, a Council Directive (2008/114/EC) was adopted on the identification and designation of ECI and the assessment to improve their protection in the field of energy and transport.

The conclusion to be drawn from this legislative framework is that member states and the owners/operators are ultimately responsible for protecting ECI. Identification of ECI is established via

a Commission developed procedure has developed a. However, the European Union has also adopted a number of legislative measures setting minimum standards for infrastructure protection in the framework of its different EU policies. This is notably the case in aviation and maritime transport.

Aviation Security

Security has been a matter of concern for civil aviation for several decades. However, in spite of its economic importance and cross-border dimension, aviation security has, up until more recently, been addressed on essentially a national level. Following the terrorist attacks of 9/11, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella. The EU adopted its first common regulations in the air transport security domain in the aftermath of the 9/11 attacks and international cooperation on security issues considerably increased.

Legislation

- The first common regulations adopted in 2002, following international standards on aviation security, provided the basis for harmonization of aviation security rules across the European Union with binding effect.⁶² In relatively short period of time, several acts of implementing legislation were added.⁶³ That regulatory framework has been fully completed and replaced by a new framework, in full effect since 29 April 2010, as laid down by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March, 2008 on common rules in the field of civil aviation security.
- The EU regulation (300/2008) lays down measures for the implementation and technical adaptation of common basic standards regarding aviation security to be incorporated into national civil aviation security programs. The regulation provides standards for airport planning requirements, aircraft security, staff training and most importantly screening. Member states and/or airports are given a list of screening and controlling methods and technologies for passengers, baggage, cargo and courier from which they must choose the necessary elements in order to perform their aviation security tasks in an effective and efficient manner (using a basic hand search, walk through metal detection equipment, conventional x-ray equipment, high definition x-ray and bio-sensory technologies such as sniffers, trace detectors and explosive detection dogs). The regulation also provides a set of guidelines for equipment used in support of aviation security. For instance it defines requirements (security, operation requirements) for metal detection equipment.⁶⁴ It also provides standards and testing procedures for x-ray equipment (performance requirements and operational requirements).⁶⁵
- Member states are free to set more stringent security measures in case of increased risk, provided they are relevant, non-discriminatory and proportional to the risk addressed.

Public Procurement

In August 2009, Directive 2009/81/EC on the procurement of defense and sensitive security supplies, works and services entered into force. Member states have two years to transpose this directive into their national legislation. Directive 2009/81/EC aims mainly at bringing the bulk of defense procurement into the internal market, thereby opening up national markets to EU-wide competition and establishing the basis for a European Defense Equipment Market.

The procurement rules laid down in Directive 2009/81/EC do not only apply to defense, but also to the security market. This directive is thus the only piece of EU legislation which covers the whole spectrum of military and non-military security, including contracts awarded by private operators of critical infrastructures in the water, energy and transport sectors. In the field of defense, its scope is (at least indirectly) defined by military lists. In the field of security, by contrast, its scope is defined in a very generic way: The directive applies to “sensitive procurements” and defines the latter as “equipment, works and services for security purposes, involving, requiring and/or containing classified information.” This very generic approach makes it possible to apply the directive across the entire spectrum of security areas. In this context, recital 11 specifies that “in the specific field of non-military security, this Directive should apply to procurements which have features similar to those of defense procurements and are equally sensitive. This can be the case in particular in areas where military and non-military forces cooperate to fulfill the same missions and/or where the purpose of the procurement is to protect the security of the Union and/or the Member States, on their own territory or beyond it, against serious threats from non-military and/or non-governmental actors. This may involve, for example, border protection, police activities and crisis management missions.”

To what degree the directive will open national security markets to EU-wide competition is hard to predict for various reasons. As clearly shown by the FRS paper, *The Security Market in the EU and the United States: Features and Trends*, there are hardly any figures on the size of these markets, let alone their openness. In other words: there is no reliable baseline for an impact assessment.⁶⁶ In addition, up until now, member states have exempted their sensitive security procurements via an exclusion clause of the General Public Procurement Directive 2004/18/EC, which states that this directive “shall not apply to public contracts when they are declared to be secret, when their performance must be accompanied by special security measures . . . or when the protection of the essential interests of that Member State so requires” (Article 14). The question for the future is twofold:

- How many contracts, which have been exempted up until now from directive 2004/18/EC, will be in the future awarded according to the rules of the new directive 2009/81/EC and,
- What is the financial value of these contracts in comparison to defense procurement, where are production volumes and orders normally much larger than in security?

The new directive contains a number of provisions specifically adapted to the special features of security procurement. For security customers, protection and privacy of classified information and reliability of suppliers are particularly important; the directive allows making such requirements in different forms (in particular, as selection criteria and/or contract execution conditions). These safeguards are expected to limit the cases where contracting authorities “have” to derogate in order to protect their essential security interests to only exceptional cases.

At the same time, however, the directive itself contains a number of exclusions which are particularly relevant for security. According to Article 13, the directive shall not apply to “contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security” (13a), nor to “contracts for the purpose of intelligence activities” (13b). The first exclusion is an almost literal repetition of Article 346 (1)(a) TFEU and therefore in principle redundant, since the directives applies by definition only subject to Article 346 (1)(a). The second exclusion is at the same time limited

(intelligence) and generic (activities). In this context, recital 27 specifies that “*some contracts are so sensitive that it would be inappropriate to apply this Directive, despite its specificity. That is the case for procurements provided by intelligence services, or procurements for all types of intelligence activities, including counter-intelligence activities, as defined by Member states. It is also the case for other particularly sensitive purchases which require an extremely high level of confidentiality, such as, for example, certain purchases intended for border protection or combating terrorism or organized crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces.*” This list of cases potentially covered by the exclusion indicates that Article 13 (a) and (b) are apparently tailor-made to security (rather than defense) concerns. The directive thus takes into account that non-military security procurements can often be even more sensitive than military procurements and accepts that in these cases transparent procurement procedures and transnational competition may not be appropriate.

In principle, the existence of common procurement rules in the security area should lead to greater market openness for European companies. However, due to numerous exceptions and the margin of maneuver, it is doubtful that the market will become considerably more transparent and open. The situation may be different for private operators of critical infrastructures who already face competition in their own markets and may, therefore, be ready to choose the economically most advantageous security solution, no matter whether it comes from a national or non-national supplier.

Conclusions

Currently, the European Union does not have a single regulatory framework for the security market as a whole, but each of its segments has a specific regulatory framework. To a certain degree, such fragmentation is normal and inevitable, since each sector has its own specificities, which must be taken into account in the rules and regulations governing the sector (see, for example, aviation versus maritime transport). The problem in Europe, however, is that fragmentation at sector level coincides with fragmentation at the national level. In some cases, EU legislation can overcome or at least alleviate this fragmentation, but definitely not all the time, and attempts to harmonize national rules at the EU-level still faces resistance from member states who are reluctant to delegate national sovereignty to Brussels.

At the same time, the European regulatory framework for security is characterized by important gaps. According to stakeholders, the most important loopholes concern:

- The lack of a proper liability protection system for both equipment suppliers and users, which creates considerable legal uncertainty in case of equipment- or system-failure.
- The absence of standards or differences between national and sector specific standards, which tends to reduce market transparency and efficiency.
- The lack of an EU security label based on agreed validation and certification procedures.
- The lack of an EU risk assessment methodology.
- The absence of an EU Security Industrial Policy.

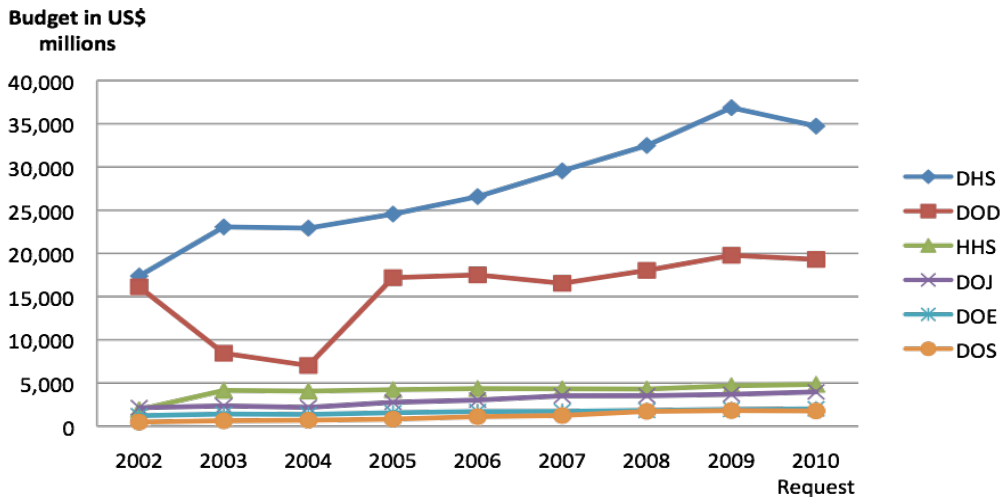
Such legislative gaps ultimately reduce market transparency, openness and legal clarity. Additionally, these gaps have the potential to discourage investment in technology development and innovation and create a non-competitive business environment, particularly for the security industry.

The Homeland Security Regulatory Environment in the United States

In the United States, homeland security activities are funded and undertaken by a number of federal agencies. The lead agency is the Department of Homeland Security (DHS) which was established on November 25, 2002 by combining the activities of 22 federal agencies and more than 2,000 Congressional appropriations accounts.⁶⁷ DHS today accounts for approximately 52 percent of the U.S. homeland security budget. The second largest contributor is the Department of Defense, which has accounted for roughly 29 percent of the federal homeland security budget during the period of 2002-2010.

below presents the breakdown of homeland security budget across various federal agencies for the past 9 years.

Federal Homeland Security Funding by Agency, 2002–2010



Source: Congressional Research Service (2010), Homeland Security Department: FY2010 Appropriations, p. 103.

Although regulation and funding occurs primarily at the national level, homeland security activities are also regulated and funded at the state and local levels. However, this study will focus on the activities undertaken by the Department of Homeland Security at the national level across four

primary mission areas: counterterrorism; infrastructure protection; border security; and preparedness, response and recovery.

DHS-Wide Developments Affecting the Industrial Base:

Legislation passed by Congress and acquisition guidelines and regulations prescribed by DHS are the two key elements that affect the homeland security industrial base.

Legislation

In recent years, DHS has not experienced much Department-wide legislative activity.⁶⁸ However, there are three notable developments addressed below:

The Support Anti-terrorism by Fostering Effective Technologies (SAEFTY) Act of 2002 is designed to provide critical incentives for the development and deployment of qualified anti-terrorism technologies by providing liability protections for manufacturers. Its primary objective is to minimize risk and encourage the commercialization of new technologies, services and software programs.⁶⁹

The Procedures for Handling Protected Critical Infrastructure Information is classified as a “final rule,” which came into effect on September 1, 2006. It provides a list of procedures that oversee the receipt, validation, handling and storage of critical infrastructure information (CII) voluntarily submitted to the Department and is applicable to all federal agencies, U.S. government contractors, and state and local entities with access to CII.⁷⁰

Recently signed into law is the Department of Homeland Security Appropriations Act of 2010, which provides a gross budget authority of \$51.9 billion in DHS funding for FY2010.⁷¹

Acquisition guidance

In efforts to enhance the acquisition and procurement processes, the Department has drafted and released several Department-wide acquisition guidance publications, notably:

The Homeland Security Acquisition Regulation (HSAR), which supplements and implements the Federal Acquisition Regulation (FAR) in the homeland security context and provides guidance for procedural uniformity for Department-wide acquisitions. It is applicable for all acquisition activities except for those within the Transportation Security Authority (TSA).

The Homeland Security Acquisition Manual (HSAM) is a supplementary document to both the FAR and the HSAR. Although non-regulatory, the HSAM also seeks to establish uniform DHS acquisition procedures for services and supplies.⁷²

The Major Systems Acquisition Manual (MSAM) reflects the Department’s efforts to provide guidance for the implementation of the DHS Acquisition Review Process. Designed as a tool for program managers, primary objectives include reducing the acquisition time cycle to productive time periods, using a systems engineering approach for major acquisition projects, estimating realistic total ownership costs and using flexible acquisition processes. It also seeks to align the Coast Guard major acquisition processes with Department policy and procedure.⁷³

The Acquisition and Program Management Division, established in 2007, is assisted by the Cost Analysis Division in the implementation of the Acquisition Directive 102-01. The directive establishes the framework and the tools for all acquisition procedures, regulations, and statutes and is also responsible for defining the Acquisition Life Cycles Framework (ALF), the Acquisition Review Process (ARP) and the Acquisition Review Board (ARB).

Governance and oversight

DHS accountability has faced scrutiny as current acquisition policies lack the management and oversight needed to curtail rising costs and schedule delays. As the GAO report concludes, although the Department continues to develop its acquisition oversight capabilities and has begun implementation of its interim acquisition management directive, there still exist great inefficiencies across the acquisition framework. Ultimately, the Acquisition Review Board (ARB), an entity charged with providing program decision memorandums with action items to improve performance, has reviewed only 24 of the major acquisition programs in FY2008-FY2009 and many of its proposed review action items have not been implemented in a systemic and timely manner.

Although there have been significant developments in this regard, rising budgetary expenditures and insufficient staffing levels continue to render a comprehensive review of acquisition programs difficult. In FY2009 acquisition spending increased by 66 percent and reached \$14.2 billion from \$8.5 billion in FY2004.⁷⁴ Although a tracking system has been installed to oversee the key information regarding all acquisitions by the acquisition oversight office, the lack of a department-wide requirements oversight body ultimately affects the Department's success in meeting both current and future critical mission needs.⁷⁵

Key Mission Areas

Counterterrorism

Dubbed the “founding purpose” of the Department, counterterrorism activities strive to prevent terrorist-driven violence on the United States by land, by sea and/or by air.

Legislation

- HSPD-4: National Strategy to Combat Weapons of Mass Destruction established in 2002 encourages the use of new technologies, strengthens intelligence collection and analysis and emphasizes the importance of strategic partnerships with alliances in order to combat and reduce the proliferation of WMD.⁷⁶
- HSPD-11: Comprehensive Terrorist-Related Screening Procedures created in 2004 builds upon HSPD 6 and clarifies the terrorist-related screening procedures used by DHS. It calls for coordinated procedures that “detect, identify, track, and interdict people, cargo, and other entities.”⁷⁷

Infrastructure Protection

Protecting the nation’s critical infrastructure and key resources (CIKR) is a core element of the DHS mission, and the Office of Infrastructure Protection (IP) is charged with this responsibility. Critical infrastructure is defined as “the physical or virtual assets, systems, and networks, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.”⁷⁸ Key resources are the “publicly or privately controlled resources essential to the minimal operations of the economy and government,” including agriculture and food, commercial facilities, energy, banking and finance, critical manufacturing, information technology, transportation systems and the defense industrial base.⁷⁹

Legislation

- The Critical Infrastructure Information (CII Act) Act of 2002 defines critical infrastructure information as the “information not customarily in the public domain and related to the security of critical infrastructure or protected systems.” This act seeks to increase infrastructure information sharing between the operators of CI and the government agencies charged with infrastructure protection activities.⁸⁰
- Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization and Protection was released in 2003 for the purpose of developing a framework that “identifies, prioritizes, and protects” the CIKR from terrorist attack. It defines the roles and responsibilities of the Secretary, Sector-Specific Agencies, state and local entities, other departments and agencies, as well as the private sector.⁸¹
- Homeland Security Cyber and Physical Infrastructure Protection Act, introduced in January of 2011, is still in the legislative process. If ratified, it will enhance domestic preparedness and collective response to terrorist activities by establishing an Office of Cyber-security and Communications, which will comprise a United States Computer Emergency Readiness Team and a Cyber-security Compliance Division, a division to be created by this act. Additionally, this act would call upon the Cyber-security Compliance Division to establish cyber-security requirements for civilian non-military and non-intelligence community federal systems.⁸²

Preparedness, Response and Recovery

Enhancing the nation’s preparedness, response and recovery in the event of a natural disaster, emergency, or terrorist attack is the third core DHS mission area and one that relies most upon collaboration with the state and local levels.

Legislation

- HSPD-8 National Preparedness of 2003 and the accompanying Annex 1 is a directive designed to enhance the current “preparedness” of the U.S. government’s ability to secure against and or directly respond to terrorist attacks, natural disasters and sudden emergencies. The fundamental principal of this directive defines the “all-hazards preparedness” goal which seeks to develop “readiness priorities” and couples the potential and or existing threats with the resources capable

of detecting, deterring, and recovering from any national emergencies. Annex 1 provides planning guidance in accordance with the Homeland Management System in the National Strategy for Homeland Security of 2007.⁸³

- The National Response Framework (NRF) of 2008, a Federal Emergency Management Agency (FEMA) initiative, replaces the previous National Response Plan. It provides the framework and guiding principles for the national response architecture and outlines the five principles of the response doctrine to better coordinate nation-wide initiatives.⁸⁴
- The FEMA Strategic Plan for 2008-2013 is comprised of 9 core competences and 2 strategies which will build upon existing federal, state, and local preparedness capabilities and incorporate new integrated, interoperable and coordinated response assistance activities.⁸⁵
- Disaster Recovery Improvement Act, introduced January of 2011 is still in the legislative process however, if passed seeks to amend the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Specifically, it aims to improve overall disaster relief by expediting the time needed and costs incurred of recovery projects.⁸⁶

Border Security

Securing the nation's borders involves protecting against the illegal smuggling of people and goods. Security measures must exist at all points of entry and prepare for, protect against, and mitigate all existing and potential threats by way of land, air and sea while fostering lawful immigration for visitors and residents alike. The four primary federal agencies within the Department responsible for border security activities are: the Customs and Border Protection (CBP), Bureau of Immigrations and Customs Enforcement (ICE), the United States Coast Guard (USCG), and the Transportation Security Administration (TSA).

Legislation

Border Security

- Established in 2003, the United States Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT) conducts verification procedures on non-U.S. citizens entering the United States. The U.S.-VISIT Final Rule, released in August 2004, expands to include aliens travelling with non-immigrant visas, individuals travelling under the Visa Waiver Program, and to lawful permanent residents at chosen land ports of entry.⁸⁷
- The Secure Fence Act of 2006 authorizes the funding for operational border security capabilities along U.S. land and maritime borders. Specifically, Section 102 requires the Department to construct, along an approximate 700-mile segment, security infrastructure along the Southwest border.⁸⁸
- The REAL ID Final Rule released in 2008, acting in accordance with the REAL ID Act of 2005, establishes minimal standards for state-issued driver's licenses and identification cards to standardize state procedures and regulations.⁸⁹
- The Emergency Border Security Supplemental Appropriations Act of 2010 allocates \$600 million for emergency funding for Southwest Border operations, \$394 million of which to the

Department of Homeland Security.⁹⁰ This bill is, however, offset by a \$100 million reduction in SBInet funding and \$552 million in revenue increases, resulting in a net impact of roughly \$52 million.⁹¹

- The Interim final rule regarding the implementation of the Electronic System for Travel Authorization (ESTA) Program released in August of 2010 amends the previous DHS regulation requiring travel fees by individuals from Visa Waiver Program countries. Specifically, it confirms that travellers with approved program authorization are exempt from paying ESTA fees if only updating an ESTA application. Travellers, however, with new passports must pay the fee.⁹²
- Border Security, Cooperation, and Act Now Drug War Prevention Act, introduced January of 2011, if ratified will authorize up to 500 additional U.S. Border Patrol, DEA and ATF agents along the Southwest border shared with Mexico. It will also increase the resources needed to protect the border from illegal immigration, drug trafficking and the smuggling of illegal goods by increasing the number of motor vehicles, radio communication systems and global positioning systems as well as by providing higher-quality body-armor.⁹³
- Border Enforcement Security Task Force, introduced in February of 2011, if passed will enhance border security by fostering greater collaboration between the federal, state and local governments and aid in the process of information sharing. Task forces will be established in designated areas facing cross-border violence.⁹⁴

Aviation and Transportation Security

- HSPD-11 Comprehensive Terrorist-Related Screening Procedures Directive, released in 2004, establishes wide-ranging screening procedures for cargo, people, and other entities suspected and or engaged in terrorist-related activities.
- NSPD-47/HSPD-16, released in 2006, further establish a strategic vision and comprehensive plan for increased border security at all airports and call for the establishment of a National Strategy for Aviation Security.
- Secure Airport Terminal Act of 2011, introduced in February of 2011, will, if ratified, increase the use of security cameras all airport screening facilities, at both areas of entry and exit. It also requires all camera's be used, maintained and tested in addition to other implemented technologies.⁹⁵

Port and Maritime Security

- The Maritime Port Security Transportation (MSTA) Act of 2002 works to prevent loss of life, transportation infrastructure disruption or destruction, economic instability and environmental damage. It provides a strategic framework regulating maritime commerce and the security of domestic sea ports.
- NSPD 41/HSPD13, released in 2004, provide policy guidelines for the U.S. maritime domain and call for the development of a National Strategy for Maritime Security. Released in 2005, the National Strategy for Maritime Security is designed to coordinate and implement all existing Department-level strategies and procedures and security programs at the State, local, and private sector.

- Security and Accountability for Every (SAFE) Port Act of 2006 amends the Maritime Port Security Transportation Act, establishes new port facility requirements, calls for the development and implementation of the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-PAT) and amends the Homeland Security Act of 2002 to establish the Office of Cargo Security Policy.⁹⁶
- The Coast Guard Authorization Act for FY2010 establishes, in section 401, a Chief Acquisition Officer to be selected by October 1, 2011. Additionally, in section 402, it appropriates funds for the establishment of an acquisition directorate designed to supply guidance and oversight for all USCG acquisition procedures and projects.⁹⁷

Conclusions

Focusing on homeland security activities at the national level, this section presented the key DHS-related legislation and acquisition guidance efforts affecting the U.S. homeland security market. Interestingly, recent regulatory efforts have focused on improving the oversight and management of ongoing and future R&D and procurement programs.

EU-U.S. Comparative Analysis

The final section of this paper presents a comparative analysis of the EU and U.S. regulatory environments for security and sheds light on the strengths and weaknesses of both.

Political Structure

Functioning largely under the purview of national jurisdiction, the EU security market is highly fragmented and complex. Market fragmentation is further exacerbated by the absence of a single Directorate General (DG) in the European Commission charged with centralizing EU security initiatives.

In the United States, the Department of Homeland Security is responsible for coordinating and leading homeland security missions and generating the capabilities to do so. Through its Directives and publication of acquisition manuals and guidance, the Department is able to foster a more centralized, transparent and competitive security market than its European counterpart.

Acquisition and Procurement Directives

In Europe, the Defense Procurement Directive is the first and only piece of legislation that pertains to the defense and non-military security sector at the institutional level and establishes the basis for a European Defense Equipment Market. Nevertheless, the EU does not have of a “European Standardization Handbook for Security Procurement” nor a corresponding “Code of Conduct,” for procurements not covered by the Defense Procurement Directive.⁹⁸

The Defense Procurement Directive and Code of Conduct are similar to the Department of Homeland Security’s HSAM, HSAR, and the FAR in that they establish the principles and procedures of DHS acquisition and procurement strategies at the federal level. However, unlike the United States,

the EU does not have an equivalent oversight body to facilitate the harmonization of acquisition practices.

Security Strategies and Acquisition Guidance

The European Security Strategy of 2003 and the Internal Security Strategy of 2010 are important EU achievements as they aid in the development of a clear and definable industrial policy or future roadmap for the security market. Specifically, the Internal Security Strategy re-establishes common threats and obstacles, defines a European Security Model and contributes value-added, concrete objectives in a manner similar to the DHS Quadrennial Homeland Security Review, which largely inspired its framework. The above-mentioned EU security strategies also strongly resemble the DHS Strategic Plan Fiscal Years 2008-2013 which describes the Department's strategy and quantifiable goals and objectives for 2013.⁹⁹

International Standards and Certifications

Currently, the EU lacks the legislation necessary to provide liability protection and product and service testing and evaluation of new capabilities before deployment. The United States, on the other hand, has developed the Office of Test, Evaluation and Standards and has enacted the SAFETY Act.

Regulatory Activity in Key Areas

Several areas have experienced significant legislative and regulatory activity in the United States and the EU.

Biometric and privacy protection

The United States has established a stronger regulatory framework for biometrics that has, in large part, guided the development of this capability in other countries. The U.S. Enhanced Border Security and Visa Entry Reform Act of 2002 not only mandates the use of biometric data in U.S. visas but equally requires that foreign consulates and embassies install biometrics in all travel documents for individuals traveling to the United States.¹⁰⁰

In compliance with U.S. regulation, EU Council Regulation (EC) 2252/2004 mandates the use of biometric identifiers in all passports and travel documents; however biometric finger scanning for non-EU citizens at ports of entry has not yet been established.

Legislation governing privacy protection for biometric identifiers in the EU is primarily regulated by member states who remain reluctant to store personal data in centralized databases, which has not yet been mandated by EU regulation. In the United States, privacy protection is regulated at the federal level through the Privacy Office.

Border security: aviation, maritime and port security

Developments such as the International Civil Aviation Organization (ICAO) and the European Civil Aviation Conference for aviation security and the International Ship and Port Facility Security Code (ISPS Code) for maritime security have been fundamental in bringing about global legislative harmonization. As this paper demonstrates, in the United States and EU, legislation in these fields is similar; however, U.S. standards and requirements are often more stringent than those in Europe.

This is due to the more centralized U.S. structure, where border security activities are overseen at the department level and implemented by numerous components (TSA, U.S. Coast Guard, and Customs and Border Protection). Additionally, the presence of U.S. certifications and standards as well as liability protection through the SAFETY Act, have fostered a more uniform security market. The EU, however, continues to suffer from national legislative fragmentation and a lack of equipment interoperability due to the absence of uniform standards. This has largely hindered the development of harmonized procedures in the aviation and maritime domains.

Preparedness, response, and infrastructure protection

The legislative environments for infrastructure protection are also similar between the EU and the United States as both seek to identify and define their respective critical infrastructures and key resources. The fundamental difference is that critical infrastructures in the United States operate across federal, state and local levels whereas, the European Critical Infrastructures (ECIs) function transnationally.

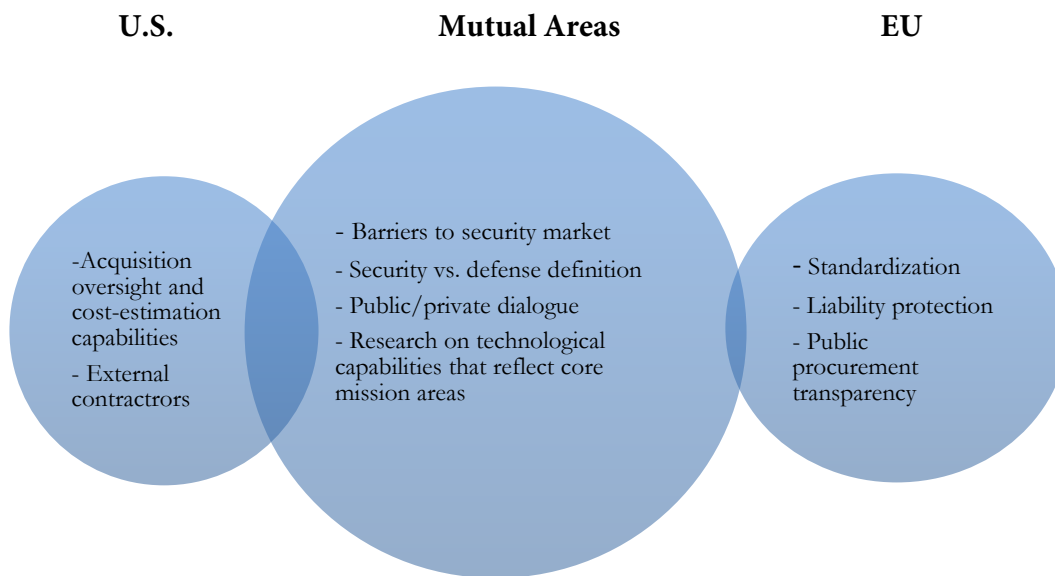
Ultimately, the EU lacks legislative force governing this domain and Council Directive 2008/114/EC is the only directive which addresses ECI protection, establishing the process by which member states must identify ECIs by January 12, 2011.¹⁰¹

Acts and initiatives related to infrastructure protection also frequently pertain to EU preparedness, response, resiliency and consequence management to terrorist attack.¹⁰² In the United States, however, greater distinction is made between these two security areas. Preparedness, Response, and Recovery (PRR) is considered a DHS priority and one that is strongly intertwined with all of the department's activities.

Recommendations

We propose a series of recommendations designed to strengthen the regulatory frameworks for, and the functioning of, the security markets in the United States and Europe. They are not all-encompassing, yet address the identified key legislative gaps and underdeveloped areas within the security market. Figure 6 provides an overview of the recommendations broken down by regional applicability.

Individual and Mutual Areas of Insufficient Security Market Development



Source: CSIS.

European Union

The most critical issue for the EU is the reduction of market fragmentation toward a single security market and the adoption of a more homogenous regulatory framework. This endeavor will require the harmonization of security strategies and policies across all 27 member states and constitutes the driving element for all EU-related recommendations. Additionally, instituting EU-wide security standards and requirements for security-related technologies will be fundamental for harmonizing and opening the EU security market as it will provide for a level of equipment interoperability that has not yet been achieved. The EU security market would also greatly benefit from the creation of an EU equivalent to the U.S. SAFETY Act, as liability protection would increase competition, foster innovation, and expand the number of products and services available. Greater transparency at the institutional level regarding public procurement practices and procedures could further strengthen the security market. Harmonizing European procurement guidance would lower market entry barriers for companies and streamline the acquisition process. Specifically, the creation of an EU Security Procurement Directive, covering the areas not governed by the Defense Procurement Directive, would help clarify the distinction between security and defense technologies and minimize the difficulties associated with dual-application technologies. The development of a European Handbook for Security Procurement would also standardize current security procurement practices and facilitate EU-wide expansion of the market sector in a uniform manner.¹⁰³

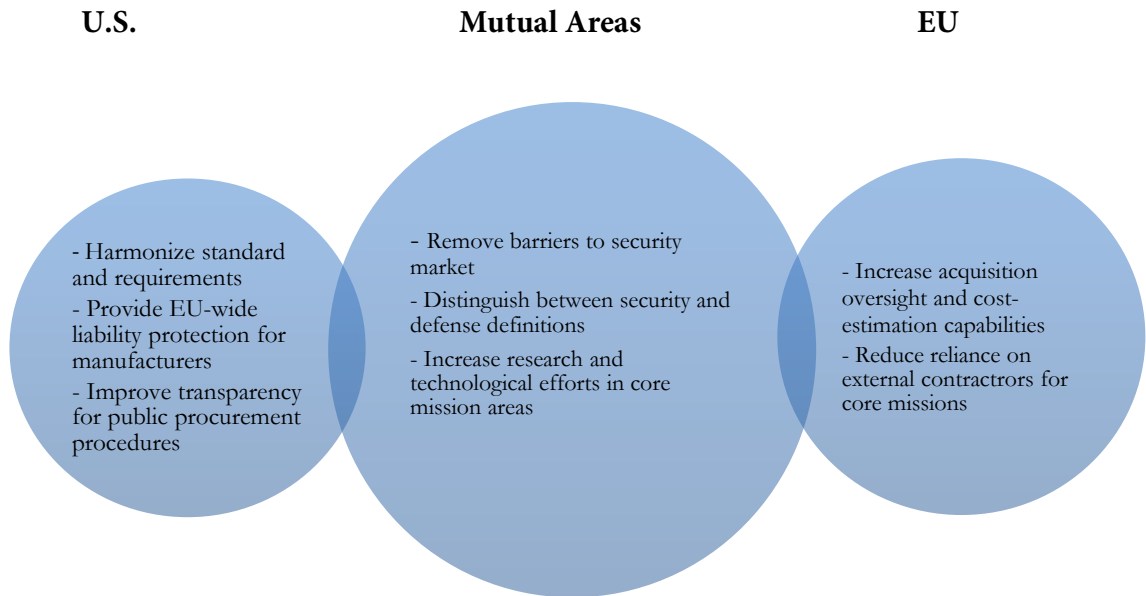
United States

As this report illustrates, the DHS's unrealistic cost-estimates and program evaluations have, in recent years, led to a significant increase in expenditure and undermined the development of new security

capabilities. Initiatives to enhance oversight and improve management are a good start but must be followed-up on.

Moreover, the department's reliance on outside contractors for undertaking core missions has also come under increased scrutiny, both internal and external. To address this issue, DHS is reducing the number of external contractors and increasing internal capabilities (an approximate 27 percent or nearly \$1 billion decrease in budgetary spending on professional service contracts by August 2010). Insourcing, however, will only prove to be more cost-efficient if DHS develops and maintains a framework that can effectively oversee and manage the activities and collaboration of a larger workforce. The recently drafted DHS Workforce Strategy for Fiscal Years 2011-2016, if properly implemented, will be instrumental in this process.¹⁰⁴

CSIS Recommendations for the Security Market



Source: CSIS.



TRANSATLANTIC INDUSTRIAL POLICIES IN THE SECURITY SECTOR

Valerio Briani, *Researcher, IAI*,
and Nicolò Sartori, *Junior Researcher, IAI*

Introduction

This paper assumes that after the end of the Cold War, and even more after the 9/11 terrorist attacks, the attention of Western governments, companies and societies has increasingly shifted from the defense to the security sector. The aim of this paper is not to verify such assumption but, rather, to investigate how this interest in security is translated concretely into EU and U.S. industrial policies and what consequences this shift may have on transatlantic industrial relations.

In order to reach this goal we

- assess the characteristics of the U.S. and European defense and security sectors, in terms of market dynamics and industrial structure. This will give us a starting point to understand the evolution of the security sector and judge whether the defense sector is being chosen as a model for development;
- identify which initiatives have been taken in order to influence developments within the security sector and investigate to what extent these initiative may have on the establishment of a security industrial policy in the EU and the United States;
- assess the potential impact of these policies on the future of the transatlantic relations, and suggest some ideas in order to foster what we do believe is the best evolution of the security industrial base, seen in the framework of transatlantic industrial relations;

The Defense and Security Sectors: Characteristics and Developments in the United States and in the EU.

In this paragraph we will briefly expose the main characters of the defense and security markets and industries, as they were at the end of the Cold War (and largely still are). In our view, the two sectors can be seen at the opposite end of an imaginary continuum in terms of market structure; a monopsonistic and almost monopolistic market with high entry barriers and high technological level

on one side (defense), and a fragmented, more low-tech and unregulated sector on the other side (security). Clarifying the main features of these two poles will give us a reference points to evaluate, in the following paragraph, if and how the post 9/11 security market is evolving and what role the EU and the U.S. governments are playing.

The Economics of Defense Industry

The defense industry has historically been a sector in which the highest national security interests overlap and intertwine with political and economic interests. On both sides of the Atlantic, the Defense Industrial Base (DIB) is largely considered both an economic and a strategic asset. According to generally accepted definitions, the DIB is composed of a public and private industrial complex with capabilities to perform research and development (R&D), design, produce, deliver and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Several academic studies have been carried out to investigate the economic functioning of the defense industrial sector, and its main characteristics can be summarized 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

Defense markets are imperfect. On the demand-side, governments maintain a relevant monopsony position as the sole buyer, at least in the most significant segments of the market. Small arms and, in the United States, some kind of armored vehicles are also available to private citizens or companies, but the size of these markets pale in comparison to that of governmental expenses. This allows states to maintain close control over the dynamics of their domestic defense markets.

Monopolies, duopolies or, at least, oligopolies characterize the structure of the supply-side, in which large integrated firms operate as exclusive prime contractors in a sector with high barriers of entry for newcomers. Production trends in the sector are basically affected by quantity and output. High R&D fixed costs are progressively rising in real terms, following the continuous technological evolution which characterizes the defense sector. Large-scale production allows economies of scale and learning, favoring decreasing unit costs.

Relevant technological spin-offs, the civilian/commercial application of a product or a technology originally developed for defense missions, affects the companies' industrial organization. In order to exploit the huge amount of technological spin-offs between the defense and civilian sectors, multi-product firms increasingly replace single-product specialists. This is the case, for instance, of the civil-military aerospace and defense firms, which rely upon massive civil profits to remain in the defense market.

All these elements result in highly concentrated industrial segments dominated by small numbers of large integrated firms. High fixed costs for research, high levels of technological know-how,

advantages deriving from economies of scale and learning as well as integrated organizational practices. All provide effective barriers of entry and exit as well as limit industrial competition and create markets dominated by a handful of well-established giant firms.

Defense is a strategic issue for the large majority of the world's countries, and for this reason political factors and security concerns dominate the sector's management and evolution. The role of the state remains paramount in shaping the nature of the defense market, particularly with regard to competition and international openness.

Like market dynamics, government choices also play a large role in shaping the defense market. Governments' planning powers, procurement spending and normative authority have relevant capacities to determine the size and the structure of their DIBs as well to control the evolution of the defense industrial sector. Tightly supervising the defense industry's activities; control by public authorities assures some strategic benefits:

- the independence and security of supply (re-supply) in equipment procurement;
- the development of specific equipment responding to national Armed Forces' requirements and needs;
- deeper information and control on products characteristics;
- bargaining powers when considering foreign acquisitions;
- surpluses for the balance of payments deriving from exports earning and imports savings;
- socioeconomic externalities such as
 - creation of high-wage jobs;
 - technology spin-offs and benefits.

During the Cold War period, governments, through ministries of defense, managed military products, setting needs and requirements; supported R&D for new weapon systems; negotiated contracts with suppliers; oversaw and evaluated program developments; set accounting and security restrictions on private companies. Defense business were kept under control in order to protect national security and keep the technological base ahead of that of potential enemies as well as to retain some national autonomy for the defense industrial base. In these circumstances, the defense industries were, in essence, a manifestation of national sovereignty, and despite some degrees of military and political integration deriving from the participation of NATO or the EU, Western governments jealously defended their political control over the defense industry's management.

Protected by national governments, the defense business evolved largely isolated from commercial pressures and dynamics while, in some European cases (France, Italy), the state directly assumed full control over the defense industry. Governments often sacrificed the economic and commercial efficiency of their defense businesses and provided subsidies to the defense industry in order to correct certain types of "market failure," supporting company's high costs of entry in new strategic markets, maintaining R&D levels required to guarantee desired industrial output and preserving positive externalities such as jobs, technologies and spin-offs. Conversely, issues of market

efficiency and value-for money were often put aside. The focus of defense industrial policies was mainly on obtaining the most advanced weaponry regardless of the costs.

With the end of the Cold War, new trends and drivers began to shape the industrial dynamics of the defense sector, and Western countries had to cope with new challenges and situations. These new elements, characterizing both the political and industrial environment, can be summarized as follows:

- decline in defense budgets and military expenditure;
- increased interoperability/communality requirements;
- privatization of services that once were provided by the military;
- technological evolution and growth of R&D costs;
- globalization and transnationalization of production and supply chains;
- openness of the research sector.

In order to deal with both budget reductions and increasing R&D costs driven by technological evolution, companies were required to ensure more commercial discipline and efficiency when procuring armaments. Therefore, as in both the United States and in Europe there was massive overcapacity, companies, backed by national governments, started responding to the new situation by restructuring and consolidating their assets.¹⁰⁵ Rapid, wide-ranging consolidation of the global defense industry in the past decade has left only five big defense and aerospace prime contractors in the United States and just four giant firms in Europe.¹⁰⁶ Together with some efforts toward restructuring and consolidating, the shrinking defense budgets increased the attraction of joint programs¹⁰⁷ and, therefore, the participation of overseas companies in the U.S. defense industrial base.¹⁰⁸ The collapse of the Soviet Union also meant that the countries previously included in the Soviet sphere of influence entered the marketplace. Companies started looking abroad for new potential customers in the attempt to globally spread their high fix costs, while taking advantage of economies of scale. The processes of globalization and transnationalization of markets and supply chains in part favored such developments, though in the defense sector political pressures and corporate reticence pushed for maintaining national control over a large part of the defense industrial assets.

At the end of the 1990s, many decision-makers and scholars started believing that these drivers would have fostered deeper industrial relations between Europe and the United States,¹⁰⁹ and that a competitive transatlantic defense market would have strengthened political relations within NATO as well as enhanced military interoperability, improved the quality of products and reduced the cost of equipment procurement.¹¹⁰ In reality, transatlantic defense business remains today largely fragmented, with market closures and protectionist behaviors, which often constrain competitive industrial practices. Industrial tie-ups such as mergers, acquisitions or teaming arrangements that would enhance cooperation between Americans and Europeans actors are, therefore, hindered by the enduring protectionist attitudes of many national military-industrial complexes. This is further aggravated by their reluctance to open their defense markets to transatlantic allies, as well as by Europe's chronic industrial fragmentation and national divisions. Finally, the desire to maintain

strategic independence through a national defense base has not faded away in the United States or in Europe.

In addition to political and regulatory limits, economic and commercial challenges also contribute to a delayed and effective opening of the two markets.¹¹¹ The existing technology gap between the United States and Europe is probably the most serious of these challenges. The global military economy has transformed over the last two decades, largely the result of technological developments that have reinforced the dominance of the United States over the transatlantic industrial sector. Differences in R&D resources and technological capabilities generate a lack of general balance between the two industrial systems, rendering attempts to promote market openness between the two sides of the Atlantic very difficult.

The Economics of Security Industry

During the Cold war, the security sector was much closer to any other market than to the defense sector. Moving from the analysis of the economic characteristics of the defense industry, we can assess that the security sector presents the following elements:¹¹²

- market structures extremely fragmented;
- short/mid-range product life cycles,
- mostly private R&D funding;
- low and mainly production costs;
- associated spin-offs.

The security market's structure presents a much more competitive environment when compared to the defense sector. On the demand-side, public authorities (not-exclusively military) remain the most important security customer, but it is questionable whether this assertion holds true (that is, whether public authorities represent more than half of the market). Security customers are highly diversified among both public institutions, central and local and private entities. These can be either large customers such as infrastructure operators (airport and port companies, rail operators, energy providers, telecommunications firms) or smaller, less demanding actors (companies, private citizens). Customer needs are, therefore, much more diverse and can be satisfied by a wide-range of products, from the more technologically intensive (for example access control technologies) to the most basic products (closed circuit televisions for domestic security).

Fragmentation of the demand, and, therefore, of customer needs, implies a very diverse range of suppliers. The supply-side is thus characterized by the coexistence of several firms, differing from one another in terms of dimension, organization, specialization and revenues. Some IT and defense giants operate in some segments of the sector (mainly systems of systems), along with many specialized security firms and SMEs with disparate specializations. Due to the heterogeneity and fragmentation of the demand, entry barriers on the supply-side are very limited to the low-end security sector, while higher-end segments require more technologically intensive R&D. In the systems of systems segment barriers to entry may be as high as in the defense sector; since very few firms possess the necessary systems integration capability this is, in fact the segment in which defense companies show the most

interest.¹¹³ Such fragmentation makes it harder for any actor on the demand-side to assume a leading position and exercise control over the industrial dynamics of the security sector through the sheer weight of its procurement.

Production trends in the sector are not heavily affected by quantity and output. R&D fixed costs may also be important in the security sector, especially in the higher segments, but their weight on company's industrial planning is sensibly lower. In the *systems of systems* segment, which is the more technologically intensive, R&D costs may also be lower than expected as these products are often the result of a successful integration of already existing products (or, products for which R&D has already been paid, often derived from defense research). Indeed, competition and low-tech requirements force firms to adapt and respond rapidly to the free market's short-term changes: emphasis is put on time and costs, rather than on performances and reliability.

Given these circumstances, government (both central and local) and private customers, do not have strong incentives, neither economic nor political, to maintain close supervision over the security industry's activities. Issues considered fundamental in the defense sector, such as the independence and security of supply, are less relevant when considering the security domain.

Therefore, the security industrial base is generally organized and operates according to economic factors rather than political and strategic ones. Although the security industry certainly has a strategic value, providing public authorities and private operators with equipment and technologies necessary to cope with some of the most demanding challenges for the new century, political concerns do not have a key role in shaping the sector's features. Multinational companies (in particular in the ICT sector with companies like IBM and Cisco) as well as some niche firms specialized in sectors such as biometrics, tracking, detection, sensors exploited such market fluidity to develop their businesses on the two shores of the Atlantic. For instance, a large number of Automatic Identification Systems (AIS) and Long-range identification and tracking (LRTI) producers, both American and European, operate competitively in the maritime security sector.¹¹⁴ Competitive dynamics dropped the company-level market shares, making it difficult to identify any dominant company really leading the market.¹¹⁵ Also in the detection segment, despite the fact that the majority of the firms are based in the United States, some European players operate and make huge profits in the transatlantic market.¹¹⁶ Smiths Detection, UK leading producer of various types of detection equipment is probably the most prominent example with 31 percent of the global market share.¹¹⁷

Security Industrial Policies in the EU and the United States

The evolution of the global security scenario, and in particular, the threats and challenges that we have to confront, is leading to an evolution of the market structures outlined in the previous paragraph. The security sector, in particular, is bound to undergo a deeper transformation, as its structure is, by far, less articulate and less institutionalized in comparison to the defense one. The evolution of the security market and of the security industrial base will be heavily influenced not only by external market forces, but by political choices of U.S. and EU governments in their double capacity as market regulators and potential procurement agents.

In this section we will try to outline the contour of such intervention by describing the EU and U.S. informal industrial security policies. “Informal” refers to the fact that neither the United States nor the EU currently have a formalized policy document which outlines objectives and tools to steer the direction of the security industrial output and structure. However, governments on both sides of the Atlantic sought after a large number of interventions, which are tantamount to an industrial policy, albeit a potentially incoherent one. In fact, the European Commission is starting to elaborate a formal security industrial policy, which makes the evaluation of the initiatives taken so far all the more urgent. Having identified the main trends in government’s intervention in the sector will allow us to question its impact on the transatlantic relationship.

The concept of “industrial policy” is multidimensional. Some authors stress the fact that an industrial policy refers to a specific industrial area, the development of which is believed to bring benefit to the economy as a whole.¹¹⁸ From this point of view, the development of a specific industrial sector is undertaken in order to maximize the economic health of a country, not merely to increase the productivity of firms operating in the sector. An increase in quality and quantity of industrial output is also a pursued objective, but it is a subsidiary one. The choice of the sector for an industrial policy should, therefore, fall only on the industrial sector which has a potential to produce a cascade effect on the economy. Others stress the role of an industrial policy in the transformation of the industrial structure in a desired direction (i.e. favoring the development of large companies, or maintaining a certain level of competition between producers). This conception is more apt to be applied in sectors which possess a significant strategic relevance for the state.¹¹⁹

It should be underlined that any concept of industrial policy implies some degree of skepticism in the functioning of free-market dynamics. If the “invisible hand” is considered sufficient to develop an industrial sector to its fullest potential, there should be no need for governmental intervention. It is tempting to assume that traditional U.S. and European views of free-market dynamics have influenced the way governance of the security sector is being addressed. Overall, we can assume that EU countries, given the influence of social-democratic and catholic political doctrines, are traditionally more open to the acceptance of governmental intervention in the economy; while the more traditionally liberal United States (in the economic sense of the word) has a stronger free-market leaning, and is, therefore, more suspicious of anything resembling governmental interference in the economy. Our analysis seem to suggest, in fact, that most U.S. initiatives in the security sector are merely geared toward obtaining better homeland security management, with very few regards to the development of the security industrial sector. EU initiatives, on the contrary, has been directed at influencing and shaping the market itself, as a prerequisite for enhanced societal security as well as for a cascade effect on the European economy.

The first, and main, U.S. initiative has been the forming of the Department of Homeland Security (DHS) in 2002. This was done in order to centralize and coordinate the various homeland security activities performed by some 22 federal agencies, thereby enhancing the governance of the homeland security activities. The Department of Homeland Security, being a procurement agency, doted itself on unified regulations for the procurement of products and services. From the market point of view, the creation of the DHS had a twofold effect. As highlighted by the CSIS-IAI paper, “The Regulatory and Acquisition Environment for Security in the EU and United States,” it acted as an aggregator of demand: the DHS now accounts for approximately 50 percent of the U.S. federal homeland security

budget. If we consider that the DoD accounts for another 27.5 percent of homeland security funds, we can say that the creation of DHS has led to a considerable reduction in the fragmentation of the U.S. public market. This, in turn, favored the entry of large defense companies into the security market, as these already possessed a long record of government-related procurement.

Another initiative which could have a significant impact on the U.S. security industrial base is the Export Control Reform Initiative.¹²⁰ Announced in August 2009, it aims to establish new criteria for determining what items need to be controlled, based on a three-tier construct and an interagency set of policies. However, the reform is still developing and it is too early to assess which kind of impact it could have.

European authorities, on the contrary, have been, from the outset, extremely interested in the potential benefits associated with the development of an industrial security sector. Between 2004 and 2010 EU authorities, institutions and various private and public stakeholders engaged in a very lively public debate on the security market in general and also on the possible development of a security industrial policy.

The first step was taken with the institution of the Group of Personalities (GoP) in 2004. The GoP, composed of a large number of prominent public and private security stakeholders, was tasked with developing a strategy to enhance European security research. The report produced by the GoP¹²¹ fell short of asking for a whole industrial policy in the field of security (which was not, after all, its goal) and focused quite strictly on European research needs, proposing the creation of an European Security Research Program and of a Research Advisory Board to prepare its agenda. However, the GoP report struck some chords, which would be accepted as the basis for the European discourse on security industrial policy: the need to overcome market fragmentation, the need for more coherent requirements and the need to fully exploit the synergies between security and defense technologies and goods.

The European Security Research Advisory Board (ESRAB) proposed by the GoP published its final report in 2006. The report, “Meeting the challenge: the European security agenda,” also contained hints regarding issues which were, according to the authors, beyond the original ESRAB mandate, but which were considered too vital to be overlooked. ESRAB proposed a Strategic Security Agenda, which would act as a framework for all activities directed at increasing European security, including research, policies, legislation and standardization as well as a European Security Board with the aim of advising on the content of a Strategic Security Agenda. This request amounts to a call for an advisory body for a security industrial policy.

The call was effectively answered with the establishment of the European Security Research and Innovation Forum (ESRIF), whose final report strongly argued for the formulation of an industrial policy able to overcome the perceived main weakness of the security market, fragmentation. It called for legislative and regulatory guidelines to level the field and encourage private companies to enter the sector. The ESRIF report also underlined the importance of a predictable level of demand as a prerequisite for the development of the security sector. Finally, the ESRIF report strongly highlighted the large number of commonalities between the security and defense sectors, and endorsed the exploitations of synergies between security and defense solutions.

The debate has not been lost on the European Commission, which proceeded to increase its work on the establishment of a security industrial policy. The EC responded to ESRIF suggestions with a Communication, which fully endorsed the need for an ambitious industrial policy in the security sector.¹²² This communication singled out two main objectives for an industrial policy: to overcome market fragmentation and to strengthen the industrial base. The first objective would require tackling issues such as the lack of a certification, validation and standardization, the lack of a harmonized European regulatory framework and lack of technical and organizational interoperability. Strengthening the industrial base would in turn require a mapping out of the current security industrial base, enhancing European innovation policy and synergies between security and defense policies as well as promoting the “security by design” concept.

The Directorate General for Enterprise and industry is, thus, currently working to develop a general definition of the sector and to understand the perimeter of industry by commissioning research projects, within the 7FP framework.¹²³ This will provide understanding as to what are the most innovative security sectors to be brought into the Lead Market Initiative as well as understanding on how to enhance synergies between security and defence R&D activities.

The Commission also recognized the security sector as one of the most important industrial areas to develop within the framework of a more comprehensive European industrial policy. The Commission’s Communication on an Integrated Industrial Policy for the Globalization era¹²⁴ singles out the security industry as one of the sectors which deserve specific initiatives, along with the space sector, transports and energy intensive industrial fields. In its Communication the EC recognizes the current limitations of the security market: its fragmentation (both from the demand and the supply-sides), the heterogeneity of national regulatory environments and the diversification of the different categories of security products. It also lays out the main areas, which will be the object of communitarian intervention: a fast track system for the approval of priority technologies, further progress on standardization and harmonization and more research on security technologies. The document also hints at the possibility of coordinated security procurement, probably between states. These ideas will be further developed in a Security Industry Initiative and through the setting up of a European Security and Dual-use Platform.

In September of 2010, the European Commissioner for Industry and Entrepreneurship Antonio Tajani expressed his intention to present a paper calling for an industrial policy for the security sector.¹²⁵ The paper, to be published by the second half of 2011, should focus on the areas of innovation, standardization and certification, pre-commercial procurement and dual-use synergies with defense R&D. This latest development should represent the final step of the elaboration phase of a European security industrial policy and signal the beginning of a new and more concrete phase.

What Future for the Transatlantic Security Sector?

The evolution of the security sector has been much different from that of the defense sector. During the whole Cold War period and beyond, defense has always been considered a strategic sector with regard to both national security and economy. This led to a tendency of protectionism and strict control from national authorities as a means to orient industrial output in the desired direction and

deny products and technologies to foreign states when deemed necessary. The end of the bipolar confrontation is forcing both governments and industry to recalibrate their relationship, by stressing, more forcefully, the issues of efficiency and competition. In the EU, this effort has also translated into a movement toward a common European defense market.

The security sector may be experiencing exactly the opposite development. During the Cold War, the security sector's political significance was closer to that of any other industrial sector; at the very least, security was not considered as much as a strategic field as defense. Consequently, its governance was mostly left to free market dynamics. The emergence of new threats during the 1990s, and even more after 9/11, forced governments to reevaluate the handling of the security market. Security systems instantly gained a strategic significance they never had even in the most dangerous times (for example, during the heights of international terrorism of the Palestinian Black September).

It is difficult to evaluate the consequence of such a shift in the handling of the security sector. The EU and the United States responded to this new challenge with quite different approaches. First of all, both aimed at tackling the fragmentation of the security market. This goal has been more easily attainable in the United States, for the obvious reason that the U.S. government already represents a single procurement agent, compared to the 27 national agencies in the EU. Therefore, all it took was the centralization of all procurement lines into the two departments of Homeland Security and Defense. On the European side, reducing fragmentation is bound to take a variety of different measures. The centralization of procurement would be the most effective but also the most politically delicate in a short-term perspective. A common measure both the EU and the United States are taking is to improve their respective regulatory environments, in order to provide a more even playing field for companies to compete. Another common endeavor, however, more effective in the EU than the United States, has been the attempt to establish better communication between demand and supply.

All these initiatives are steps in the right direction and should have positive effect on the functioning of the security market, as they tackle serious efficiency issues well-known by the business community. They also are shaping, or attempting to shape, the security market in a way similar to the defense sector; more centralized demand, close demand-supply relation, R&D costs incurred by the public sector and strict regulations. It would be very useful, therefore, to remind a couple of lessons learned from the development of the defense market. First of all, too much fragmentation is bound to limit the maturation of an industrial sector, but too much centralization could lead to inefficient monopolies in certain niche and specialized areas, with the consequent loss of competition. The efforts to reduce fragmentation should be carefully weighted in order to avoid excessive regulations and constraints. Also, a reasonably fragmented security market is an opportunity for small and medium enterprises, more suited to deal with small customers such as local police, etc. Secondly, a transatlantic dispute over security standards should be avoided at all costs. European stakeholders should take this into account, and engage their American counterparts in order to produce commonly accepted standards without prejudice to either industrial base. Third, the range of security issues the EU and the United States face is almost the same. All efforts should be made to link the EU and U.S. security markets, and all attempts to create excessively restrictive export control regulations should be avoided. In this regard, the current U.S. efforts to relax its export regulations should be sustained where possible. Furthermore, any initiative which could potentially bind the two markets together should be considered. The recent EU/U.S. agreement on cooperation in the field of security research

is a step in the right direction and could be expanded.¹²⁶ For example, the United States could be engaged as a partner in the EU security research programs, similar to the model of the partnership already established with Israel. However, the partnership should be based on the concept of reciprocity, as it would not be in the interest of the European Union to provide R&D funding for U.S. companies in the absence of any similar policy on the other-side of the Atlantic.

Notes

¹ Except if we consider the Galileo program (space based navigation system funded by the EC), or part of it, as a security system.

² ESRAB report: *Meeting the challenge, the European Security Research Agenda*.

³ Moreover, other resources within the 7FP are allocated to the JRC (1750M€ for non-nuclear research), but a relatively small and imprecise part is related to security. The EC allocated also about 745M€ for 7 years to the framework program “Security and safeguarding liberties.”

⁴FRONTEX Intellops and Blueprint project. EDA BIO-EDEP project, MIDCAS, SDR project. EUROPOL has established an operational agreement with the U.S. for exchange of personal data on specific kind of crimes.

⁵ COM(2009)691 final, p. 4.

⁶ Ecorys Research and Consulting, *Study on the Competitiveness of the EU security industry*, Within the Framework Contract for Sectoral Competitiveness Studies–ENTR/06/054, Final Report, Client: Directorate-General Enterprise & Industry, Brussels, 15 November 2009, p. 30.

⁷ Congressional Budget Office.

⁸ CIVITAS, *The Homeland Security Market essential dynamics and trends* (2006).

⁹ http://www.dhs.gov/files/grants/gc_1247254578009.shtm.

¹⁰ *Homeland Security, FY 2011 budget in brief*, p. 136.

¹¹ See *FY 2011 Budget in brief, Homeland Security department*. Details on the budget for each area and related technologies are available at the following internet page:

http://www.dhs.gov/ynews/releases/pr_1265049379725.shtm.

¹² CIVITAS report, op. cit.

¹³ Homeland defense is defined at the armed forces assets dedicated to the terror protection of the Homeland.

¹⁴ Interviews conducted by the authors.

¹⁵ CIVITAS Report, op.cit., and the “*Global Homeland Security 2009-2019*” report, published by the HSRC in June 2009.

¹⁶ Ecorys Report, op. cit.

¹⁷ *European Security Directory 2009*, ESD Partners, p.16.

¹⁸ Ecorys, op.cit., p.12.

¹⁹ *European Security Directory 2009*, op.cit., p. 36.

²⁰ Civitas Group, Homeland Security Research Corporation (HSRC), Jane’s Information Group, Security Industry Association (SIA), National Defense Industrial Association (NDIA) market reports and economic study.

²¹ “American market sparks European influx,” *HS Today*, 31 July 2008.

²² Since May 2005, and the merger between Snecma and Sagem, the new Safran group is organized in 3 branches of activities: Aerospace propulsion, Aircraft equipment, and Defence Security.

²³ In November 2009, Sagem Sécurité announced the launching of a new U.S.-based company called MorphoTrak, which will offer a host of biometric and identity solutions to the federal, state and commercial markets. The new company is a combination of its Sagem Morpho subsidiary and Printrak. Furthermore, in May 2010, the Safran group has decided to consolidate all security businesses within the group under a single name, “Morpho.”

²⁴ The group is a member of several U.S. teams selected by the federal administration, e.g. Lockheed Martin Team in charge of the FBI’s next generation identification system.

²⁵ “New facial, gait recognition software to be integrated in CCTVs,” *HS Newswire*, 25 February 2009.

- ²⁶ Ecorys Report.
- ²⁷ Of course most initiatives remain on the national level. For reasons of space constraints, however, we will not delve on national cases in this particular study but concentrate on the supranational EU level as such.
- ²⁸ <http://www.generaldynamics.com/> (Accessed 10 Nov. 2010).
- ²⁹ <http://www.asd-europe.org/site/index.php?id=2> (Accessed 10 nov. 2010)
- ³⁰ <http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122> (Accessed 22 Nov. 2010).
- ³¹ <http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122> (Accessed 22 Nov. 2010).
- ³² <http://www.sipri.org/research/armaments/production/Top100> (Accessed 6 Dec. 2010).
- ³³ See http://www.src09.se/upload/External%20Documents/gop_en.pdf, pp. 4-5 for complete list of the participants.
- ³⁴ COM(2004)590 final), *Security Research: The next Steps*, available online at: <http://cordis.europa.eu/documents/documentlibrary/69322111EN6.pdf>.
See also European Commission, IP/04/1090: *EU blueprint for Security Research programme*, 9 September 2004, available online at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/04/1090&format=HTML&aged=0&language=EN&guiLanguage=en>.
- ³⁵ Call for proposals 2004: ftp://ftp.cordis.europa.eu/pub/security/docs/sec_04_45_en.pdf; call for proposals 2005: ftp://ftp.cordis.europa.eu/pub/security/docs/pow_2005_en.pdf; call for proposals 2006: ftp://ftp.cordis.europa.eu/pub/security/docs/en_pow_13022006_final.pdf.
- ³⁶ *Meeting the Challenge: the European Security Research Agenda*. A report from the European Security Advisory Board. p.15. (http://www.src09.se/upload/External%20Documents/esrab_report_en.pdf).
- ³⁷ European Security Research Advisory Board, *Meeting the challenge: the European Security Research Agenda*, September 2006, available online at: http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf.
- ³⁸ For a complete list of these members, see www.esrif.eu/documents/members_22012009.xls
- ³⁹ <http://www.esrif.eu>.
- ⁴⁰ For more information see: European Commission, CORDIS – About Security Research website: http://cordis.europa.eu/fp7/security/about-security_en.html; European Commission, DG Enterprise and Industry – Security Research and Development website: http://ec.europa.eu/enterprise/policies/security/research/index_en.htm.
See also http://www.eurunion.org/eu/index.php?option=com_content&task=view&id=303&Itemid=58.
- ⁴¹ European Commission – Joint Research Center’s website: <http://ec.europa.eu/dgs/jrc/index.cfm?id=2350&lang=en>.
- ⁴² Didier Bigo, Julien Jeandesboz, *The EU and the European security industry questioning the ‘public-private dialogue*, INEX Policy Brief no. 5/February 2010.
- ⁴³ Report available online at <http://www.eos-eu.com/LinkClick.aspx?fileticket=7nRk3CbrwkM=&tabid=239>.
- ⁴⁴ Interview with security industry representative, Stockholm 2 June 2010.
- ⁴⁵ See ASD website: <http://www.asd-europe.org/site/index.php?id=4>.
- ⁴⁶ *ASD Key Priority 4: A Harmonised European Security Environment*, available online at: http://www.asd-europe.org/site/fileadmin/user_upload/ASD_KP_4-Security.pdf.
- ⁴⁷ Bullock, James, A. et al. (2006) *Introduction to Homeland Security*, Butterworth-Heinemann Homeland Security Series. p. 459.
- ⁴⁸ See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm.
- ⁴⁹ See <http://www.aaas.org/spp/rd/dhs09s.pdf>.
- ⁵⁰ See <http://www.aaas.org/spp/rd/09pch11.htm>.
- ⁵¹ *USA Today*, “Homeland Security generates multibillion dollar business,” 9 October 2006.
- ⁵² See http://www.cfr.org/publication/14827/homeland_security_technologies.html.
- ⁵³ Available online at http://www.hstoday.us/component/option,com_sobi2/catid,225/Itemid,325/
- ⁵⁴ See <http://projects.washingtonpost.com/top-secret-america/companies/>.
- ⁵⁵ “Synergy in Security: National Security Complex,” *Dollars and Sense* magazine, March/April 2010.
- ⁵⁶ “Investors favor homeland security firms,” *HS Today*, 22 October 2009.
- ⁵⁷ “Homeland Security Industry Shows Impressive Growth,” *Frost & Sullivan*, Feb. 4, 2010.
- ⁵⁸ Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*, Brussels, 2003. Available at <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

- ⁵⁹ “Towards a European Security model,” 23 Feb 2010, EU Council.
- ⁶⁰ “The EU Counter-Terrorism Policy: main achievements and future challenges,” Communication from the Commission, COM (2010) 386 final, 20.7.2010.
- ⁶¹ Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM (2004)702 final - Not published in the Official Journal].
- ⁶² Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (OJ L 355, 30.12.2002).
- ⁶³ The most important implementation acts are Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security (OJ L 89, 5.4.2003) replaced by Regulation (EC) No 820/2008, laying down measures for the implementation of the common basic standards on aviation security of 8.8.2008 (OJ L 221, 19.8.2008).
- ⁶⁴ Equipment shall be capable of detection small items of different metals, with a higher sensitivity for ferrous metals in all foreseeable conditions.
- ⁶⁵ Equipment shall provide for the necessary detection, measured in terms of resolution, penetration and discrimination, to ensure that prohibited articles are not carried on board aircraft.
- ⁶⁶ See DefSec report, pp. 183-186.
- ⁶⁷ See http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf (4/35).
- ⁶⁸ Key DOD acquisition related legislation in recent years includes the Weapons System Acquisition Reform (WSARA) Act of 2009 and the Implementing Management for Performance and Related Reforms to Obtain Value in Every (IMPROVE) Acquisition Act of 2010.
- ⁶⁹ See <https://www.safetyact.gov/jsp/homepages/displayHomeAbout.do>.
- ⁷⁰ See http://www.dhs.gov/files/laws/gc_1158333877680.shtm.
- ⁷¹ The FY 2011 Presidential budget is \$56.3 billion. <http://www.fas.org/sgp/crs/homsec/R40642.pdf>.
- ⁷² See http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsam.pdf.
- ⁷³ See <http://www.uscg.mil/acquisition/newsroom/pdf/msam.pdf> (10/468).
- ⁷⁴ See <http://homeland.house.gov/press/index.asp?ID=565&SubSection=2&Issue=0&DocumentType=0&PublishDate=0>.
- ⁷⁵ See <http://hsc-democrats.house.gov/SiteDocuments/d10588SP.pdf> (10/92).
- ⁷⁶ See <https://www.hsdl.org/?view&doc=2805&coll=limited>.
- ⁷⁷ See http://www.dhs.gov/xabout/laws/gc_1217614237097.shtm.
- ⁷⁸ See <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>: Section 1016(e) of the USA PATRIOT Act of 2001– (131/132).
- ⁷⁹ See http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf: Section 2(9) of the Homeland Security Act of 2002 (7/187).
- ⁸⁰ See http://www.dhs.gov/xlibrary/assets/CII_Act.pdf (7/11).
- ⁸¹ See http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#0.
- ⁸² See <http://www.opencongress.org/bill/112-h174/show>.
- ⁸³ See <http://www.fas.org/irp/offdocs/nspd/hspd-8.html>.
- ⁸⁴ See http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf (4/4).
- ⁸⁵ *FEMA Strategic Plan Fiscal Years 2008-2013*. FEMA P-422, Jan. 2008 (pdf) (11/64).
- ⁸⁶ See <http://www.govtrack.us/congress/billtext.xpd?bill=h112-57>.
- ⁸⁷ See http://www.dhs.gov/files/laws/gc_1229618480915.shtm.
- ⁸⁸ See <http://npl.ly.gov.tw/pdf/5480.pdf>.
- ⁸⁹ See http://www.dhs.gov/files/laws/gc_1172765386179.shtm.
- ⁹⁰ Office of the Press Secretary. Statement by the President on the Passage of the Southwest Border Security Bill. August 12, 2010.
- ⁹¹ The SBI net, as of January 2011, has since been cancelled ; <http://www.gop.gov/bill/111/2/hr6080>.
- ⁹² See http://www.cb.gov/xp/cgov/newsroom/news_releases/national/08062010_2.xml.
- ⁹³ See <http://www.govtrack.us/congress/bill.xpd?bill=h112-77>.
- ⁹⁴ See <http://www.govtrack.us/congress/bill.xpd?bill=h112-770>.
- ⁹⁵ See <http://www.govtrack.us/congress/bill.xpd?bill=s112-318>.
- ⁹⁶ See <http://www.govtrack.us/congress/billtext.xpd?bill=h109-4954>.

- ⁹⁷ Congressional Research Service, *Summary—H.R.3619: Coast Guard Authorization Act of 2010*, <http://www.govtrack.us/congress/bill.xpd?bill=h111-3619&tab=summary>.
- ⁹⁸ See http://ec.europa.eu/enterprise/newsroom/cf/document.cfm?action=display&doc_id=5579 (30/318).
- ⁹⁹ See http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.
- ¹⁰⁰ Originally requiring 2-print finger scans, as of 2008 DHS has mandated that all ports of entry be equipped with 10-print finger scanning for international visitors.
- ¹⁰¹ See http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm
- ¹⁰² Examples include COM (2009)0149, COM (2004)698, and COM (2004)701.
- ¹⁰³ http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf (30/318).
- ¹⁰⁴ See http://www.dhs.gov/ynews/testimony/testimony_1286227672682.shtm.
- ¹⁰⁵ The U.S. 50 largest defence suppliers of the early 1980s have become 2000s top five contractors, creating a sort of oligopolistic market. In Europe, most firms continued to look inwards, and consolidation mainly took the form of large national defence champions acquiring small domestic firms. At the same time, the merger of DaimlerChrysler Aerospace AG (DASA) of Germany, Aérospatiale-Matra of France, and Construcciones Aeronáuticas SA (CASA) of Spain, gave life to EADS, the very first European company in the sector.
- ¹⁰⁶ In the U.S., Boeing; Lockheed Martin; Northrop Grumman; General Dynamics; Raytheon. In the EU, BAE Systems, EADS; Finmeccanica; Thales.
- ¹⁰⁷ The Joint Strike Fighter program represents a transatlantic case in point in this sense. Eurofighter, as well, can be considered a representative European consortium.
- ¹⁰⁸ Rolls-Royce acquisition of Allison and GEC-Marconi take over on Tracor.
- ¹⁰⁹ K. Hayward, *The Globalization of the Defence Business*, in G. Adams (et al.), *Europe's Defence Industry: a Transatlantic Future?*, CER, 1999.
- ¹¹⁰ A. James, *The Prospects for a Transatlantic Defence Industry*, in Burkard Schmitt (Eds), *Between Cooperation and Competition: The Transatlantic Defence Market*, EUISS Chaillot Paper 44, 2001.
- ¹¹¹ K. Hartley, *Defence Economics and the Industrial Base*, Centre for Defence Economics, University of York.
- ¹¹² Of course, the Security Industrial Base (SIB) includes also dedicated divisions or subsidiaries of large defense firms (i.e. Finmeccanica's Selex Sistemi Integrati, Selex Galileo and Eltag Datamat; BAE's Detica; Boeing's Tapestry Solutions; Lockheed Martin's Homeland Security Division).
- ¹¹³ For a more precise picture, see *The security market in the EU and the U.S.*, by H. Masson and L. Marta.
- ¹¹⁴ Leading transatlantic vessel-traffic equipment manufacturers are: Northrop Grumman Space & Mission Systems Corp, USA; Kongsberg Maritime – Group Kongsberg, Norway; Jotron, Norway; Sam electronics, Germany; Thrane & Thrane, Denmark; CNS Systems, Sweden; Maris, Norway; Samsung, USA; Transas, Ireland; Comar Systems, UK; Bluetraker, Slovenia; Marinetrack, UK; Bureau Veritas, France; Satamatics, UK.
- ¹¹⁵ Ecorys, 2009.
- ¹¹⁶ Leading detection equipment companies are: Smiths Detection, UK; L3 Security & Detection Systems, U.S.; Rapiscan Systems, U.S.; AS&E, U.S.; Bruker Daltonics, U.S.; Environics OY, Finland; ICx Technologies, Rae System U.S.
- ¹¹⁷ Smiths Group Official Webpage, available at http://www.smiths.com/smiths_detection.aspx.
- ¹¹⁸ See for example H. Pack, K. Saggi, *The case for industrial policy: a critical survey*, January 16, 2006, http://siteresources.worldbank.org/INTRANETTRADE/Resources/Internal-Training/HowardPack_KamalSaggiPaper.pdf.
- ¹¹⁹ Jacques Gansler, *U.S. Defence Industrial Policy*, in "Security Challenges," vol. 3, n.2, June 2007.
- ¹²⁰ See Us government website at <http://www.export.gov/ecr/index.asp>.
- ¹²¹ *Research for a secure Europe*, http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf.
- ¹²² EC COM 2009(691), http://ec.europa.eu/enterprise/policies/security/files/mami/comm_pdf_com_2009_0691_f_communication_en.pdf.
- ¹²³ See the ECORYS-led *Study on the competitiveness of the EU security industry*, November 2009, http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf; or IAI-led *Study on the industrial implication of the blurring lines between security and defence*.
- ¹²⁴ European Commission, *An Integrated Industrial Policy for the Globalisation Era; Putting Competitiveness and Sustainability at Centre Stage*, COM(2010)614.

¹²⁵ See DG ENTR website, http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4593&lang=en&tpa=0&displayType=news&ref=newsbytheme%2Ecfm%3Flang%3Den%26displayType%3Dnews%26fosubtype%3D%26tpa%3D0%26period%3Dlatest%26month%3D%26page%3D10.

¹²⁶ See the EC website at <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/616&format=HTML&aged=0&language=EN&guiLanguage=en>.