Sempere, Carlos Martí

Working Paper

A Survey of the European Security Market

Economics of Security Working Paper, No. 43

Provided in Cooperation with:
German Institute for Economic Research (DIW Berlin)

Suggested Citation: Sempere, Carlos Martí (2011) : A Survey of the European Security Market, Economics of Security Working Paper, No. 43, Deutsches Institut für Wirtschaftsforschung (DIW), Berlin

This Version is available at:
https://hdl.handle.net/10419/119367

Economics of Security Working Paper Series

economics-of-security.eu

Carlos Martí Sempere

A survey of the European security market

February 2011

Economics of Security Working Paper 43.

This publication is an output of EUSECON, a research project supported by the European Commission's Seventh Framework Programme.

European Security Economics
EUSECON
www.economics-of-security.eu

Economics of Security is an initiative managed by DIW Berlin

Economics of Security Working Paper Series

Correct citation: Marti, Carlos (2011). “A survey of the European security market”. Economics of Security Working Paper 43, Berlin: Economics of Security.

First published in 2011

ISSN: 1868-0488

For further information, please contact:

Economics of Security, c/o Department of International Economics, German Institute for Economic Research (DIW Berlin), Mohrenstr. 58, 10117 Berlin, Germany.

Tel: +49 (0)30 89 789-277

Email: eusecon@diw.de

Website: www.economics-of-security.eu

Economics of Security is an initiative managed by DIW Berlin

WORKING PAPER 43

A survey of the European security market (version 0.5)

Carlos Martí Sempere

Ingeniería de Sistemas para la Defensa (Isdefe),
Beatriz de Bobadilla, 3 Madrid-28040, Spain

WORKING PAPER 43

Foreword

This document synthesizes the results of the research made on the European security market. It deals with questions of interest regarding the provision of security goods and services for protecting society from terrorism and organised crime. It explores issues such as market revenues, demand and supply, industrial capabilities, technology, research and development, innovation, business strategies, competition as well as market structure, agents' conduct and economic performance.

The research has been based upon desk analysis of open source information related to the security market. Economic theory and critical analysis has been applied to understand the gathered information, derive knowledge, point out key issues and assess trends and drivers that will likely shape the sector's future.

The study is the outcome of the working package number 5 included in the research project *A new Agenda for European Security Economics* (EUSECON). This project with code number 218195 has been financed by the European Commission within the 7th European Research Framework Programme. The task has been performed by the company ISDEFE according to the scope and work plan described in the EUSECON proposal.

The author wishes to express his appreciation to all the individuals that have provided input and valuable comments to this study, including anonymous referees. Any flaws or omissions contained in this document are solely the responsibility of the author.

WORKING PAPER 43

Index

List of Tables

List of figures

List of boxes

I. INTRODUCTION

Security is a fundamental *good* without which societies can hardly prosper and enjoy freedom[1]. Investment in security affords relevant benefits by means of the prevention and reduction of damage to life and property and a better resilience to quickly recover from a security incident. This investment also diminishes the likelihood that the incident spills over into other areas and ends up disrupting key functions in a society strongly interdependent. An adequate investment in this area enhances the citizens' confidence and the general welfare of society. Yet, benefits reaped from security are somewhat intangible and not easy to measure, because the cost savings from prevented (and avoided) security breaches cannot be directly observed since such breaches never occurred.

Security can be improved through the provision of specialised services, such as cash and valuables transport, as well as material means, such as large intelligence databases or personal protective equipment. These goods and services can contribute to reduce the vulnerability of society to terrorism and organised crime and mitigate the consequences of an attack. The collection of economic agents that produce these goods and services is what is known as the security industry.

The most appropriate measure of success in this economic sector is the ability to find and offer affordable solutions to security issues that improve the citizens' feeling of confidence. Whilst security enhancing measures always entail a sort of societal burden, returns are also provided through the creation of jobs, industrial capabilities, shareholders' profits and innovations applicable in other economic sectors. In short, this type of spending has a positive effect on the overall industrial and technological base of society, contributing to economic wealth in the long run.

The security industry has a long history, but the terrorist attacks during the first decade of this century, technological advances and a society more sensible to security issues have stimulated the growth of this market. This environment has also awakened the interest of having a better knowledge of this economic sector. However, studies regarding this industry do not abound and information concerning economic data, market conditions, industrial capabilities, structure of the industry, conduct of agents, and performance is often scarce or absent. Hence, some action to reduce this knowledge gap seems to be desirable.

OBJECTIVE OF THE SURVEY

The present survey aims at increasing the knowledge available on this market. It has been the result of two years research based on the collection of available information, its analysis, evaluation and fusion in order to raise understanding and develop knowledge. The study has taken a comprehensive approach addressing the different customers and suppliers and other agents as well as the main security goods and services provided. The research has been financed by the European Commission within the 7th European

[1] Article 3 of the Universal Declaration of Human Rights says: '*Everyone has the right to life, liberty and security of person*'.

Research Framework Programme under the research project *A new Agenda for European Security Economics* EUSECON (reference number 218195).

SCOPE OF THE SURVEY

Before starting the analysis, it seems worthwhile to set the scope and the boundaries of the survey in order to determine which undertakings should be included or excluded from the research. For such a purpose, a definition of the sector would be helpful.

Definition of the sector

Research carried out on the available literature to find a common accepted definition of the security sector has been unsuccessful. Only a short definition of security economics Brück *et al.* (2009: 8) has been encountered. It states:

'Security economics is understood as those activities affected by, preventing, dealing with and mitigating insecurity including terrorism, in the economy'.

This definition has been used to further develop a pragmatic, objective and somewhat comprehensive definition of the industry.

The security industry is understood as the industry that supplies the products and services specifically used by the human being to prepare, prevent, protect, respond, reduce, palliate and deal with the threats and consequences that undesired events have on our society. These consequences may be summarised in terms of damage to people's life, health, property or other assets, including information.

The first part of the definition identifies the goods and services required in activities aimed at diminishing risk, and in case it materialises, mitigate its consequences. No explicit distinction is made on the beneficiaries, since it may be the citizen, a social group, or even society as a whole. The main effects of security incidents are briefly summarised making an explicit reference to information since it may be a potential target of cybercrime.

The most important but also problematic part of the definition is the term '*undesired events*'. These events can be distinguished by uncertainty, and their ability to create fear or insecurity on human beings with regard to welfare loss. Whilst this feeling is to some extent subjective and may be caused by many events, some events are feared more than others. Interviews may aid to highlight these different perceptions as can be seen in figure 1.

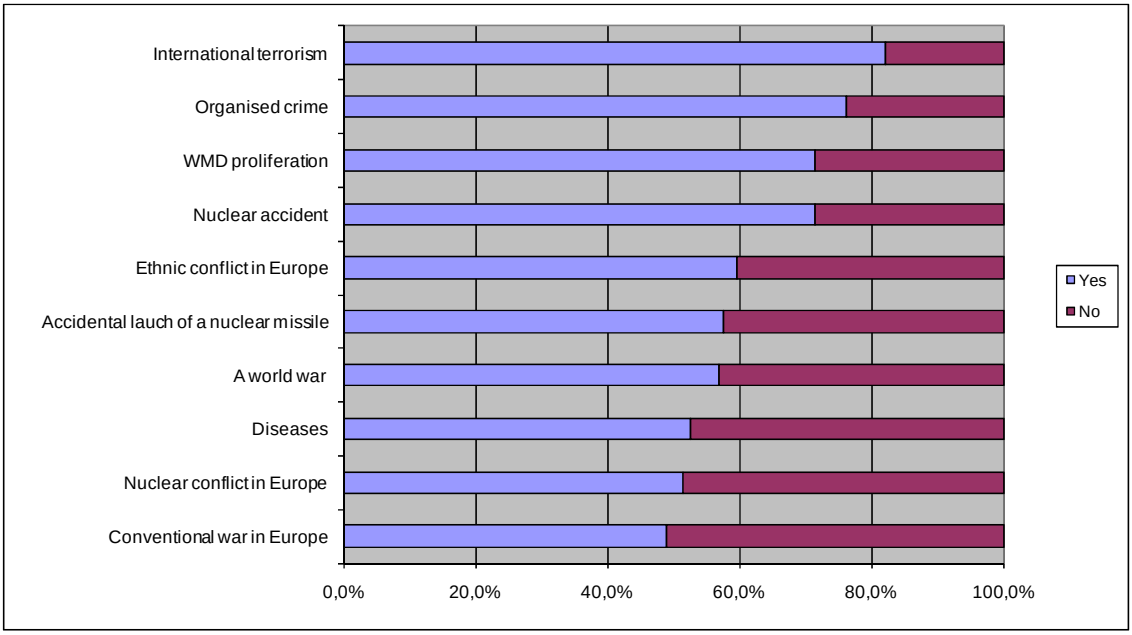

Figure 1. What do European Union citizens fear?
Source: Eurobarometre, Sondage no. 58.1 Oct./Nov. 2002.

Based on the above figure, five main sources of insecurity can be identified: armed conflicts, terrorism, organised crime, diseases/pandemics, and natural or man-made disasters. As can be seen, the two most relevant sources are terrorism and organised crime. The industry related to these two sources is largely common since most products and services apply to both needs. Commonalities are also shared with the defence industry, but differences also exist in terms of customers, products, and technologies.

This survey will focus on the industry that addresses threats associated with terrorism and organized crime. The reason behind this approach is on the one hand that it faces the most relevant sources of insecurity, and on the other hand that it is an industry with its own idiosyncrasy that has not been surveyed with the same depth as the defence industry (see for example Gansler 1980, Markusen 1999 or Hartley 2007). This does not mean, evidently, that the analysis of the industries which confront other kind of insecurities may not also deserve economic studies akin to the present one.

Terrorism can be defined as the premeditated use or threat to use violence by individuals or subnational groups in order to obtain a political or social objective through the intimidation of a large audience beyond that of the immediate victims. Incidents that have no specific political or social objective shall be deemed as criminal rather than terrorist acts (Enders and Sandler, 2006:3).

Terrorist actions are commonly aimed at casualty-rich and newsworthy targets as for example official sites like embassies or military installations, critical infrastructures, symbols and historical attractions like prominent monuments and iconic buildings, high ranking public officers like diplomats or judges, and crowded spots like public places, entertainment complexes, shopping malls or transit stations.

The term organized crime usually refers to large-scale and complex criminal activities carried out by tightly or loosely organized associations and aimed at the establishment, supply and exploitation of illegal markets at the expense of society. Such operations are

generally carried out with a ruthless disregard of the law, and often involve offences against the person, including threats, intimidation and physical violence (United Nations, 1990:5)

Unlawful activities of organised crime include smuggling; fraud and theft; drug trafficking; counterfeiting of documents, currency and commodities; financial crimes; illegal immigration and human beings trafficking, kidnapping and extortion. Since terrorism cannot openly collect taxes, often it turns to criminal actions for funding their activities like the ones mentioned before (Europol, 2009: 6). Such common behaviour enforces the argument to analyse jointly both sources of insecurity. Terrorism or crime can be considered transnational when they involve more than one country through a variety of possible connections such as perpetrators or victims.

What seems to mark out organised criminal activity from ordinary crime is the high level of entrepreneurial skill that is applied to its operations that often includes the suppression of rival gangs (Schelling, 1971). Nonetheless, a clear-cut distinction between organised and ordinary crime is often not easy to trace.

Box 1. Definition of terrorism and organised crime[2]

Main products and services

There is a plethora of policies and instruments to eradicate terrorism and organized crime. Some try to abate them addressing their root causes[3] –being they economic, political or social– offering opportunities and incentives to these organizations and their members to change preferences and abandon illegal activities. For example, communications strategies are used for challenging the ideologies (battle of ideas) that extremists believe justify the use of violence. Since state failure, disintegration and internal conflicts in foreign countries could raise threats to European security, diplomacy combined with the adequate incentives and sanctions (e.g. against terrorist harbouring states) is another key instrument to reduce the threat of terrorism and organised crime[4].

Yet these (soft) policies to forestall threats before they become critical are only effective in the long term and may not be able to defeat all sources of terrorism and organised crime. Therefore more direct measures may be required, which demand capabilities (NRC, 2002:27) that can be grouped in the following ones.

- *Intelligence and surveillance* is an essential capability since these organisations operate in a concealed way. They involve technologies to: (a) gather information of members, assets and behaviours; (b) monitor sites and areas; (c) detect concealed weapons and operations' plans, and (d) to maintain the profiles, databases and systems to exploit such information once collected.

[2] The EU provides a definition of a terrorist act in the '*Guidelines for a common approach to the fight against terrorism*' dated 26 of March 2003, partially declassified on 14 of February 2008. See also a wide discussion of both terms in Engerer (2008).

[3] For a comprehensive analysis of root causes of terrorism see Davis and Cragin (2009).

[4] See COM(2003) 313 final on European programmes to fight poverty and inequality, to support democratisation and respect of human rights and to improve governance throughout the world.

- *Prevention* is aimed at disrupting their operational and logistic chain cutting off their access to money, weapons, knowledge, technologies, infrastructures[5], and other resources; preventing the recruit of new members, foiling their attack plans (e.g. jamming radio-detonators), or hindering their movement by means of checkpoints in transport networks[6].

- *Protection / denial* is needed should detection and prevention fail. It means hardening the target so that destruction or disruption becomes more difficult such as reinforced building structure, blast-resistant containers, redundant systems and so on. It may include precautionary measures such as the deployment of manned guarding.

- *Interdiction* or *crisis management* seeks to detect and forestall an imminent attack by identifying and neutralizing perpetrators, and preventing them from bringing their violent operation to fruition such as the deactivation of an improvised explosive device (IED).

- *Response and recovery* also called *consequence management* means containing and limiting the damage level and the number of casualties in the aftermath of an attack by organizing emergency responses, public health measures and restoring critical functions increasing in such way resilience[7].

- *Attribution* refers to the ability to identify the perpetrators of an action carried out and it is essential to select the adequate response. It includes forensic science and other investigative and identification techniques to analyse terrorist and criminal means, track and apprehend suspects, and support the arrest and prosecution of individuals responsible of the illegal action.

In addition, we shall consider another area that we will name *preparedness* than involves all the planning, organising and training processes needed to meet said capabilities.

These capabilities are mainly focused on raising the cost and reducing the benefits of terrorism and organised crime actions[8]. They support active measures to abate the source of threat, aimed at stifling the operational capabilities of terrorist and crime organisations, as well as protective or defensive measures aimed at strengthening potential targets, thereby increasing the difficulty in striking them with success (Enders and Sandler, 2006:85). As will be illustrated, the security industry mainly concentrates on providing goods and services for the second type of measures.

---

[5] This may be composed of training camps, communication networks, safe houses or havens (even for financial assets).

[6] The detection and disruption of the flow of persons and illegal goods within terrorism and organised crime networks may help to unveil and neutralise these groups. Port, airports, and stations are excellent places to spot, in particular when they are collocated at borders, since these organisations are increasingly becoming trans-national (Europol, 2008, 2009).

[7] Resilience can be defined as the system's ability to recover after failure. It is measured by the time until a backup system starts functioning, the time until the full capacity is restored and sustainable, and the time to clear all backlogs.

[8] Large penalties and fines for those committing such actions is a fundamental way to raise such cost (Becker, 1968).

This survey uses a broad definition of the term industry considering all the agents involved in the value chain of security goods and services. It encompass industrial activities related to research, design, development, production, assembly, test, evaluation, supply, maintenance, upgrading, logistic support, human services and project management. The provision of these goods entails a large supply chain of subsystems and components, some of them proceeding from other economic sectors. That means, on the one hand, that a relevant part of the product value is generated outside what is considered here the security sector, and on the other hand that many suppliers to this industry operate also in other economic sectors.

Organisations in charge of security require a large set of products and services for sustaining their dairy operations as for example clothing, food, fuel, office equipment, computers, furniture, and motor cars; or services like catering, cleaning, construction, consultancy, legal advice, telecommunications, training and transport. This survey will not focus on these widely demanded goods and services, which do not show relevant differences when they are bought by security organisations, but in those which exhibit specific features for underpinning security operations, although this distinction, in practice, may easily blur.

Fuzzy boundaries

Even narrowing the scope of this industry, the difficulty to set clear boundaries still remains and is a source of controversy. This is the case of the industry related to the restoration and recovery of the situation to pre-event levels. This task involves long term activities that do not differ essentially from routine activities of maintenance, repair, reconstruction or upgrade. Hence, a criterion is needed to set the scope, being a reasonable principle to consider only the industry related to the emergency activities performed in the aftermath of a security incident.

Similar troubles appear when a distinction of products and services related to organised and ordinary crime is attempted. Since operating methods and countermeasures are alike –organised crime being perhaps more sophisticated and larger– a real distinction cannot be settled and so it seems reasonable to consider the industry that faces both types of illegal activities as unique.

Often suppliers are specialised divisions of firms, whose business is not only focused on security, being frequently this market not the main source of revenues. In such cases, these companies shall be considered part of the security market as long as they manufacture products and services used to cope with terrorism and organised crime. Companies that only provide some subsystems and components that cannot operate autonomously should be in principle considered outside this sector. Yet, in certain cases attention should be paid when said companies provide key specific components with few applications in other markets.

Diseases and pandemics are other major life risks that are confronted with the support of the health industry. This industry is related to terrorism and organised crime since it provides essential support to avoid and restore any damage on health and life. Products and services provided by this industry do not markedly differ from those aimed at protecting the population against injuries, illnesses or pandemics caused by hazard. This

industry[9] should be considered outside this sector. Notwithstanding the analysis of its capabilities to defeat attacks against public health, such as a chemical or biological one, is of interest from a security point of view.

The industry related to natural disasters –such as floods, storms, droughts, earthquakes, forest fires– or man-made disasters –such as technological or industrial accidents–, usually known as the safety industry, addresses the goods and services to respond to hazards that cause damage without purposeful action. Whilst many goods and services for mitigating damages are also shared with those used in the case of a terrorist or criminal action, the preventive means are of a very different nature as for example weather forecasting systems, forest fire detection systems, real-time water-level measurement in rivers and watersheds to pre-warn of flooding, safe design to avoid human operator mistakes and so on).

The EU vision[10] and the Department of Homeland Security (Bush, 2002)[11] take an all-hazard approach when security issues are at stake. This suggests that the analysis of the sector in order to be comprehensive should address all kind of threats and risks. However, the differences in technologies, products and services –and therefore industrial capabilities– and the variety of customers –in addition to law enforcement, health, civil protection and environmental protection agencies shall be considered– raise doubts about the convenience and appropriateness of such a broad approach. The study will consequently focus on a narrower field, yet the reader will be warned when products and services neatly address both areas.

The difficulty in distinguishing between internal security, mainly related to the fight against terrorism and organised crime, and external security, mainly related to defence activities, poses additional challenges in qualifying suppliers to both industrial sectors. In effect, these groups may be powerful enough to raise small armies, and their attacks can take a form similar to that of insurgency and guerrilla using weapons such as mortars, RPG guns, MANPADS (Man Portable Air Defence System) or even CBRNE (Chemical, Biological, Radiological, Nuclear and Explosive) devices. Additionally, terrorists could also act as proxy of certain states or may have foreign training camps and logistics bases. Countering such organisations may require joint actions of law enforcement units and armed forces[12] such as air or space surveillance, hostage recovery, maritime counter-terrorism, fight against piracy and smuggling in high seas, bomb disposal, renegade aircraft interception, and special operations for the persecution

---

9 A detailed analysis of this economic sector can be found in A.J. Curley Editor (2000). Handbook of Health Economics.

10 See COM (2006) 786, Directive 2008/114/EC or the definition of security established in January 2005 by the European Committee for Standardisation on Protection and Security of the Citizen (CEN BT/WG 161). The definition states: '*Security is the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made)*'. Dr. Alois J. Sieber (Institute for the Protection and Security of the Citizen - IPSC) presentation on *Standards for Security and Protection of the Citizen* in the Security Research Conference, Ankara, April 2008.

11 The Department of Justice and the FBI play also a relevant role.

12 The role of armed forces to combat terrorism may be considered exceptional in Europe. Land Army has been used by the British government to combat terrorism in Northern Ireland. France, faced with a continuing terrorist bombing campaign, deployed 37,000 military personnel and police to security functions, including 5,000 soldiers to patrol train stations, bus terminals, and airports in the terrorist bombing of the St. Michel train in Paris on July 25, 1995 (Jenkings, 1996).

of terrorists up to their havens in host countries. Moreover, high risk conditions (Olympic Games, World Cups) and internal security incidents with far reaching consequences generally demand the (spare) capabilities of armed forces when civilian capabilities become insufficient. Having said that, a rational criterion would recommend analysing the industry that does not supply what is traditionally considered military equipment.

Insurance companies play a relevant role in the security field, since they allow the transfer of the residual risk which cannot be mitigated with other types of security investment. These companies facilitate the purchasing of insurance against potential damages, providing financial support for incident recovery. Based on the estimated risk and consequences of undesired events, they set the payable amount (premium) for covering the economic losses of these events. They provide deductions to homeowners, businesses and other organisations when they have made investments in cost-effective loss-mitigation measures. Hence, insurance companies may have a considerable influence in setting security standards and as a consequence in the demand of security products and services[13]. However, since these companies are not true solution providers in reducing or eliminating threats, they would be considered out of the scope of this survey.

Closely related industries and markets

The capability of some security products and services to indistinctly face defence, natural and man-made disasters, safety and other social needs as well as the similarity of development and production methods explain that security firms usually operate concurrently in these markets, because they provide advantages in terms of a more diversified customer base, synergies and economies of large production. This is the case of the following industries.

- The defence industry because it shares common needs in areas such as surveillance, communications and management systems, operational vehicles, or small arms to neutralise terrorist and criminals when they oppose resistance to law forces.

- Building monitoring and management industry because it usually integrates in their solution fire protection, access control, or intrusion detection in addition to heating, air conditioning and other building controls.

- Industrial automation and control industry since it shares related technologies based on sensors, communication devices and control systems.

- Scientific instrumentation industry, such as X-ray, computer tomography, radiological detection devices and so forth, because these instruments facilitate some inspection processes.

- The ICT industry because it provides hardware, software and communications for many security solutions.

[13] According to Wharton (2005:155) the European insurance companies still play in this area a low role.

SURVEY APPROACH

The survey has been based mainly on available information related to the security sector. The list of references at the end of the study reflects the main data sources used. A considerable part of the survey has been devoted to collect and analyse such information. The sparse and fragmentary nature of said information has made the appraisal of this economic sector more complex. Few complete studies on this market have been found, confirming the initial hypothesis of an area where knowledge gaps exist.

Market studies performed by consultancy companies such as Frost & Sullivan, Inc., Gartner, Inc., International Data Corporation (IDC) or Ecorys have been quite useful, having in mind that open reports offering some numbers about the security sector are few. Information of the security market in Central and Eastern Europe is very scarce. Probably this is due to a less developed market *vis à vis* Western Europe. The EU Competition merger reports of security companies have been also a source of accurate insights on some market segments. During the study the author was able to assist to the Security Essen fair held between the 5th and the 8th of October 2010, where he had the opportunity to dialogue with some industrial representatives.

The survey follows a descriptive approach complemented with the analysis of main patterns and features identified. The traditional Structure – Conduct – Performance method has guided this analytical process. Classical literature on industrial organisation such as Scherer (1980), Tirole (1988) and Martin (1993, 1994) have provided theoretical insights to discover and understand fundamental patterns of this industry. Some studies coming from the defence market (Hartley, 2007: chapter 33) have been also a good information source since large and complex security systems suppliers, in particular in the high-end government market, show similar patterns. The use of analogy and educated assessments has been made when information available was poor.

The multiple dimensions of security make suppliers in this economic sector numerous and diverse. An exhaustive analysis of all industries involved would be, in addition to unfeasible, meaningless. It has been thought that it would have more sense to focus the survey in the more important and developed markets where the industry has been able to work out cost-effective solutions to security needs which generate considerable revenues such as video-surveillance, access control, intrusion detection, security services, transport- or ICT-security. Yet an effort has been made to mention and briefly describe the whole market especially for those products and services related to relevant threats, although their economic size could be considered small. The survey highlights also emerging markets with good growth prospects where products are in the development stage and only available as prototypes or pilot projects.

Concrete examples have been provided about products and services and industry suppliers to better explain some market features. Their names are given only as examples of industrial capabilities and do not represent any positive or negative recommendation about them.

DOCUMENT DESCRIPTION

This report has been organised in nine chapters. An introduction, facts about the security industry, basic market conditions, main market segments, the role of government, market structure, market conduct, market performance, summary and conclusions. A list of acronyms and references used across the study closes the document.

The introduction describes the goals of this survey and provides a definition of this economic sector in order to fix the scope of the research. This definition helps to identify the suppliers and the main products and services provided in this market. Boundaries with other markets and industries closely related with this economic sector are also discussed. Finally, a short explanation of the methodology used for doing the study is made.

The next chapter provides some quantitative information about this economic sector. It includes information about EU and Member States expenditures including R&D outlays, industrial revenues across market segments, country distribution, employment, market trends, imports and exports and markets in other world regions. The main problems related to the collection and accuracy of quantitative information are highlighted. Time series, when available, have been presented and commented. A short description of the Member States industry and table showing the main European security firms is also given.

The chapter of basic market conditions describes those exogenous factors from the demand and the supply side with relevant influence on the market. Key aspects of the demand include main customers, demand drivers and restraints, geographic markets, price elasticity and substitutes, growth rate and cyclicality, and marketing and purchasing methods. The relevant question of a European security market, where national boundaries set barriers to the single market, is analysed in detail. The supply side describes key aspects such as the supply chain, technology, research and development, product and services features, and the role of standards.

The next chapter provides a detailed analysis of the main market segments. It highlights the different classes of products and services supplied in this market, emphasizing the specific conditions of demand and supply associated to them. For each of these classes, the main features, technologies, providers, supply chain, customers, regulatory conditions and market trends are described. Whereas the study concentrates on the European industry, a close look is made also to the world industry due to the international character of the market. Products and services have been grouped around the following areas: preparedness, intelligence and surveillance, protection, interdiction, response and recovery, and forensics.

The following chapter analyses the government role from four basic points of views. The first is the role of government as entrepreneur. The second is the role as supporter of the industry and as improver of its dynamic performance. The third is as a large purchaser of security solutions, and the fourth is as enacter of specific regulations with a relevant impact on the demand and quality of security goods and services. Main EU initiatives and regulations in this area also presented.

The key topics that lay down the market structure are analysed in the next chapter. It addresses questions like the main market agents, product differentiation, entry

conditions, cost structure, industrial concentration, and the role of imports. Entry conditions analyses questions like economies of scale, absolute cost advantages, sunken costs and R&D. The concentration analysis considers horizontal and vertical integration within the supply chain as well as conglomerates and joint ventures. This analysis is a previous step to study market conduct and assess market performance.

The market conduct chapter analyses the behaviour of industry to achieve its goals focusing on those aspect that might have a negative impact on market performance. It analyses questions related to pricing such as competition, collusion, exclusionary practices and vertical restraints. The strategies related to the product such as research, development and innovation; marketing and advertising; bundling or contract implementation practices are examined. Conduct regarding mergers and takeovers with influence on market structure is also assessed. A list of more important mergers in the sector is also presented.

The market performance chapter analyses questions related to industrial performance. It analyses the three main aspects of market performance, namely allocative efficiency, productive efficiency, and dynamic efficiency or rate of technological progress. The analysis discusses in detail the impact of the industry structure and its conduct on such performance. The role of incentives in dynamic efficiency is discussed in more detail, since this is an essential question in this market. Government intervention to encourage such efficiency is also discussed. The life cycle of technology is presented as a method to assess the evolution of this industry and the problems it faces to achieve best performance. Some economic indicators are used to better assess the performance of this industry.

The last chapter sums up the main findings of the survey. It describes the main market features, and it envisages future market trends such as areas of future growth, the role of the defence industry in this market, and the permanent need of research and development. It also infers some conclusions. In particular, it assesses the different vision of security to each side of the Atlantic and its large impact on the industry as well as the complexity of the efficient allocation of resources to security. Some areas where there is a chance for improving market performance based on some policies are pointed out as could be the case of a more consolidated EU market, profiting for advances in other market sectors. Finally, a way ahead concerning future research on this economic area is suggested.

II. FACTS OF THE SECURITY INDUSTRY

The terrorist attacks to the Twin Towers in New York and the Pentagon in Washington (2001), that was ensued by the Madrid (2004) and London (2005) bombings, raised concerns of many nations about their security. These attacks have resulted in the creation of the U.S. Department of Homeland Security (DHS) with an important budget to address security issues that was mimicked with expenditure increases of EU institutions as well as Member States. Such expenditures have stimulated the demand of security goods and services, and the growth of this market.

The European security market is second only to the North American market. Yet, getting numbers about the size of this market in terms of revenues or employment is not easy. The statistical classifications used by governments to record economic activity do not help to measure this activity. NACE version 2 reserves some codes for security related services[14], but the supply of many security good and services are included in broad category codes, where those addressing security cannot be easily demerged[15]. Therefore, the utility of official sources of information for estimating the size of this economic sector is limited.

Estimates of industrial output and employment may be obtained collecting data from industry, but here problems also arise. First, the identification of all the firms operating in the market is required, including first and second tier suppliers of key security equipment. Identifying the suppliers is certainly complex having in mind that the number of companies operating in the market is rather large. Furthermore, since companies operate simultaneously in many markets and countries, information about security revenues and exports are not always disclosed. Even if data were available, it is normally considered confidential for commercial reasons and is not delivered to researchers on this topic. Moreover, some market figures obtained by consultancy companies are often derived from estimates based upon interviews whose reliability is unknown and whose audience may not cover the complete sector. This explains that computed values from distinct sources frequently show large differences. All these reasons invite to value the figures obtained through this way with caution.

GOVERNMENT EXPENDITURES

[14] They are: code 80.10 for *private security activities*, 80.20 for *security systems services activities* and 80.30 for *investigation activities*. Code 84.24 is used for *Public Order and Safety* and code 84.25 is used for *Fire Services*.

[15] This includes code 25.72 *Manufacture of locks and hinges*; code 25.99 *Manufacture of other fabricated metal products n.e.c.* that includes safes, strongboxes and armoured doors; code 26.30 *Manufacture of communication equipment* that includes CCTV cameras and fixed and mobile communication systems for security; code 26.51 *Manufacture of instruments and appliances for measuring, testing and navigation* that includes equipment for surveillance and inspection; code 32.99 *Other Manufacturing n.e.c.* that includes safety gloves and headgear; code 33.20 *Installation of industrial machinery and equipment* that includes the installation of security equipment; code 43.21 *electrical installations* that includes burglar alarm systems; code 47.59 *Retail sale of furniture, lightning equipment and other household equipment* that includes electrical alarm systems; code 70.20 *Technical Testing and Analysis* that includes operation of police laboratories, and code 74.90 *Other professional, scientific and technical activities n.e.c.* that includes security consulting.

Since the State is one of the main investors in security relevant information can be obtained from budgetary information. Some Eurostat figures can be obtained of these expenditures as can be seen in table 1.

	2001	2002	2003	2004	2005	2006	2007
Austria	779,1	839,3	837,2	922,3	912,6	922,8	945,1
Belgium	715,6	834,0	873,1	760,5	794,5	804,6	821,8
Denmark	531,6	549,1	581,6	625,6	674,8	698,3	744,6
Finland	650,0	603,0	633,0	613,0	637,0	635,0	672,0
France	4.362,0	4.973,0	5.447,0	5.775,0	5.956,0	5.952,0	6.178,0
Germany	9.520,0	10.060,0	9.860,0	10.520,0	10.640,0	11.350,0	12.100,0
Greece	189,0	195,0	222,0	263,0	267,0	288,0	406,0
Ireland	510,4	579,5	598,7	635,9	696,0	872,2	1.023,5
Italy	3.868,0	5.088,0	5.371,0	5.239,0	5.451,0	5.403,0	5.710,0
Luxembourg	49,7	61,5	79,1	84,6	89,9	85,8	80,1
Netherlands	2.657,0	3.169,0	3.336,0	3.490,0	3.507,0	3.951,0	4.281,0
Portugal	384,5	348,3	412,4	390,9	432,4	429,4	449,4
Spain	2.529,0	2.922,0	3.119,0	3.591,0	3.794,0	4.063,0	4.702,0
Sweden	1.212,5	1.356,6	1.348,0	1.281,0	1.364,8	1.510,5	1.552,7
United Kingdom	15.393,9	17.230,5	17.032,1	19.635,8	20.786,7	21.121,3	21.997,8
EU-15	**43.352,3**	**48.808,8**	**49.750,2**	**53.827,6**	**56.003,7**	**58.086,9**	**61.664,0**
Bulgaria	136,5	46,5	168,3	176,1	184,6	161,4	286,0
Cyprus	29,0	33,4	36,0	35,7	34,4	39,2	44,1
Czech Republic	365,4	500,1	480,2	525,8	527,3	626,6	674,4
Estonia	62,9	75,4	79,3	66,6	88,1	106,7	131,0
Hungary	277,0	410,9	346,0	349,9	361,2	349,4	361,8
Latvia	45,6	43,5	44,8	54,3	112,9	172,3	221,8
Lithuania	49,0	60,3	68,4	79,8	89,3	112,9	145,9
Malta	14,5	13,5	15,2	13,9	13,1	12,6	12,4
Poland	0,0	845,4	983,0	1.064,7	1.428,6	1.653,8	1.960,0
Romania	0,0	279,3	389,6	382,5	670,8	686,6	469,4
Slovakia	256,1	250,1	186,5	269,1	280,7	346,0	368,3
Slovenia	114,4	119,5	126,9	132,9	126,3	150,0	179,6
EU-12	**1.350,4**	**2.677,9**	**2.924,2**	**3.151,3**	**3.917,3**	**4.417,5**	**4.854,7**
EU-27	**44.702,7**	**51.486,7**	**52.674,4**	**56.978,9**	**59.921,0**	**62.504,4**	**66.518,7**
Growth rate		15,2%	2,3%	8,2%	5,2%	4,3%	6,4%

Table 1. Government expenditures in Public order and safety (2001-2007)
Source: Eurostat (series: General Government expenditure function, Classification of the functions of government: 3 Public Order and safety, National accounts indicators: P2 Intermediate consumption + P5 gross capital formation). Values in million €.

Table 1 records public order and safety expenditures for European countries. This value corresponds to 0.5% of GDP of the EU-25 for 2007; 0.4 for intermediate consumption and only 0.1 for gross capital formation. It includes expenditures in police services, fire protection, law courts, and prisons. This value is 25% smaller than the defence sector. From the table, it can be seen that the United Kingdom, Germany, France and Italy are the four main consumers.

The table shows a moderate growth rate similar to defence expenditures, with a peak between 2001 and 2002 that might be explained by the 9/11 attacks which raised the social perception of insecurity. However, the attacks in Madrid (2004) and London (2005) did not reflect a leap in government expenditures. This may be due to the fact

that the increase in security expenditures was reflected in the budget of transport organisations that is not reflected in these values. For example, the Madrid Metro Authority awarded €132.5 million 2005 to improve its security system[16].

	Intermediate consumption	Gross capital formation	Total	R&D million €
Austria	0.3	0.1	0.4	29.9
Belgium	0.2	0.1	0.3	
Bulgaria	0.4	0.4	0.8	
Cyprus	0.2	0.2	0.4	0.0
Czech Republic	0.4	0.1	0.5	1.5
Denmark	0.3	0.1	0.4	
Estonia	0.5	0.7	1.2	0.0
European Union (27 countries)	0.4	0.1	0.5	
Finland	0.4	0.0	0.4	4.0
France	0.2	0.1	0.3	
Germany	0.4	0.1	0.5	300.0
Greece	0.2	0.0	0.2	0.0
Hungary	0.2	0.1	0.3	0.0
Ireland	0.5	0.1	0.6	0.0
Italy	0.3	0.1	0.4	0.0
Latvia	0.6	0.0	0.6	0.0
Lithuania	0.3	0.2	0.5	0.6
Luxembourg	0.1	0.1	0.2	0.1
Malta	0.2	0.1	0.3	0.0
Netherlands	0.6	0.2	0.8	
Norway	0.3	0.0	0.3	0.4
Poland	0.4	0.2	0.6	7.1
Portugal	0.2	0.0	0.2	28.0
Romania	0.2	0.1	0.3	
Slovakia	0.5	0.2	0.7	
Slovenia	0.3	0.1	0.4	
Spain	0.3	0.1	0.4	0.0
Sweden	0.4	0.1	0.5	
United Kingdom	1.0	0.2	1.2	72.8

Table 2. Government expenditures in Public order and safety
Source: Eurostat *gov_a_exp* (COFOG)

Table 2 shows for 2008 government expenditures as a percentage of GDP. As can be seen from the table, values significantly differ between Member States. This suggests differences in national perceptions of insecurity and in the preferred mix of consumables, services and long term investments aimed at achieving security.

The values shown could only be considered as an estimate of the overall demand size for three reasons. First, it contains information related with the supply of common products and services that are not specific for security purposes such as fuel. While gross capital formation reflects purchases of security equipment, yet the value is merged with expenditures, such as real state investments, that are not part of the security market. Second, it does not reflect relevant security expenditures of other State organisations such as environmental protection agencies, civil protection, or transport

[16] http://www.belt.es/noticias/2005/marzo/30/metro.htm as 24/03/2010.

security. Third, it does not consider expenses of private agents such as companies and individuals. According to Ecorys (2009:31) report this value ranges between 67,74% and 69,77% of government expenditures.

EU expenditures

The European Union is a relevant investor in security. This is because many security activities have a true European dimension and are led and supported by the EU Commission. Several Directorate Generals and European agencies purchase goods and services related to security. DG Enterprise and Industry manages €1,400 million for security research during the period 2007–2013 (see below). DG Justice, Freedom and Security[17] allocates funds during the same period to programmes related to '*security and safeguarding of liberties'* including critical infrastructures protection[18] as can be seen in table 3.

	2007	2008	2009	2010	2011	2012	2013	Total
Prevention and fight against crime	58,0	67,0	91,0	107,0	133,0	142,0	147,0	**745**
Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks	12,7	15,2	17,7	20,3	23,0	23,4	25,1	**137,4**

Table 3. DG JLS expenditures related to security and safeguarding of liberties in million €. Source: DG JLS web page (10/01/2010)

The *Civil Protection Financial Instrument* is another source of funds. It has a reference amount of €189.8 million for the same period. The EU Health Programme 2008-2013 supports actions on preparedness and response to CBRN threats to public health. These funds finance the different EU Rapid Alert Systems in the event of pandemics or biological contamination. With a financial envelope of €2,062 million for the period 2007-2013, the *Instrument for Stability* includes assistance for the development of effective control of illicit trafficking in CBRN material or agents. The EU Phare programme has financed during the period 2000 - 2006 some projects related to border protection in Central and Eastern Europe states. For the period 2007-2013 the Community will finance €1,820 million through the EU External Border Fund of the Solidarity and Management of Migration Flows Programme[19]. Other DGs involved in security projects are Energy, Mobility and Transport, Maritime Affairs and Fisheries, Information Society and Media, Environmental Protection, and Joint Research Centre with its Institute for Protection and Security of the Citizen.

European agencies involved in security issues are Europol (€80 million budget in 2010), Eurojust (€30.6 million budget in 2010), the European Border Agency – FRONTEX (€83 million budget in 2009), the European Network and Information Security Agency - ENISA (€7.9 million budget in 2010), and the European Defence Agency – EDA (€31 million budget in 2010) also involved in security projects as for example Software defined Radio and Maritime Security. It is planned a new Agency that will be operational in 2012 that will manage the Schengen Information System (SIS II), Visa

[17] This Directorate has been split in two since July 1, 2010: DG Justice and DG Home Affairs.

[18] The European Programme on Critical Infrastructures Protection (EPCIP) was launched the 12th of December 2006. COM(2006) 786 final.

[19] COM (2006) 733 final.

Information System (VIS), EURODAC and other large-scale IT systems in the area of freedom, security and justice.

R&D expenditures

Eurostat *gov_a_exp* database have been accessed to identify government outlays in security research, an important figure in this economic sector. The result is shown in Table 2. As can be seen not all nations provide data. With the exception of Germany and the United Kingdom, outlays are relatively small. The amount spent by the EU in security research is also a relevant value. Within the Preparatory Action on Security Research from the period 2004-2006 it was €45 million distributed between 39 projects. The expected amount that will be invested in the 7th European Framework Research Programme is €1,400 million from the period 2007-2013, which represents 2.75% of the total research budget. As can be seen from the different calls, this activity is heavily skewed towards applied research, development and demonstration projects.

INDUSTRY REVENUES

Since market size is hard to measure from the demand side, we turn now to see if some data can be obtained for the supply side. For this purpose, we will use market studies performed by some specialised consultancy companies due to the lack of other data sources. Such information, however, as we have mentioned, is also subject to problems. The methodology used to estimate the numbers and a measure of its accuracy is not unveiled. Having in mind that information has been obtained based on interviews there is a chance of some bias due to estimates based on simplified reasoning or on commercially sensitive data. Furthermore, since documents are prepared for a target audience (e.g. investors) the risk of some bias slippage in the final figures cannot be fully discarded.

Physical security market

Data for the physical security market has been obtained from Frost & Sullivan (2008d). It rates the European security market in 2007 of access control, video surveillance, intrusion detection and fire detection around €14.5 billion. The market was valued considering product related services (supply, installation, maintenance) and value added services (alarm monitoring, remote system management)[20]. The United Kingdom, Germany, Iberia and France represented the four largest markets in 2007, with a contribution over 65% of the overall market. Growth rate was estimated around 6.9% for the period 2007-2013.

The distribution of the revenues between customers can be seen in the following table[21].

	%	Billion €
Residential[22]	17.6	2.55
Commercial	35.5	5.15

[20] This market was valued by Frost & Sullivan (2004:1-10) in €4.66 billion in 2002. Yet the value only accounts for the development and manufacturing of security equipment. It does not include revenues of distributors, security solution providers, retailers, system integrators and related business entities.

[21] Frost & Sullivan (2004:6-58) estimated that private enterprises spent in 2002 $7.5 billion on security equipment.

[22] Frost & Sullivan (2006) valued this market for 2005 with a lower value: €1.6 billion.

Industrial	14.6	2.12
Government	16.9	2.45
Banking and finance	8.4	1.22
Transport	7.1	1.03

Table 4. Distribution of the market between sectors

The distribution of the revenues between products and services can be seen in the following table:

	%	**Billion €**
Hardware / software	31.9	4.63
Installation	29.7	4.31
After sale / maintenance	20.1	2.91
Value added services	18.3	2.65

Table 5. Market distribution between products and services

The distribution of the market between the kinds of application can be seen in the following table:

	%	**Billion €**	**Hardware Billion €**
Video surveillance[23]	19.6	2.84	0.91
Access control	14.0	2.03	0.65
Intrusion detection	22.8	3.31	1.05
Fire detection	43.5	6.31	2.01

Table 6. Market distribution between the different applications

The distribution between geographic regions is[24]:

	%	**Billion €**
United Kingdom	17.12	2.48
Germany	17.00	2.47
Spain / Portugal	16.20	2.35
France	14.70	2.13
Italy	8.70	1.26
Eastern Europe	9.70	1.41
Scandinavia	7.20	1.04
Benelux	6.20	0.90
Alpine (Austria, Switzerland)	2.90	0.42

Table 7. Distribution between geographic areas.

These numbers only reflect the physical security market, but do not account the market segment of doors, mechanical locks and fences. To get numbers related to other security market segments we have analysed the Ecorys (2009) report whose figures can be seen in the next table.

Technologies	**EU (low estimate)**	**EU (high estimate)**
Screening and scanning	3.5	4.5
Tracking and tracing	3.0	4.0
CBRNE	1.0	2.0

[23] The value of the hardware equipment was estimated by Frost & Sullivan (2007) in $1.42 billion.

[24] However, Frost & Sullivan (2005) rated total sales of security equipment in Germany in the range of €1 billion in 2001, and UK value in the range of €2.4 billion. Such differences raise concerns about data accuracy.

Biometrics	1.0	1.5
IT & Secure Communication	6.0	7.0
Physical security protection	10.0	15.0
Protective clothing	1.5	2.5
Total	**26.0**	**36.5**

Table 8. Ecorys estimation of market revenues in billion € (2008).

As can be seen the value for physical security is of the same order of magnitude that the one provided by Frost & Sullivan. Yet IDC (2009) provides a higher number for the ICT market (see below). These values are decomposed in the following areas.

Sector	EU (low estimate)	EU (high estimate)	Global market
Aviation security	1.5	2.5	5.2
Maritime security	1.5	2.5	6.7
Border security	4.5	5.5	9.9
Critical infrastructures	2.5	3.5	12.6
Counter-intelligence	4.5	5.0	19.4
Physical security*	10.0	15.0	39.2
Protective clothing	1.5	2.5	10.0
Total	**26.0**	**36.5**	**103.1**
* It includes CCTV, access control equipment, intrusion and detection systems, etc. Public expenditures estimated between €15.5 to €21.5 billion.			

Table 9. Ecorys estimation of market revenues in billion € (2008).

Manned guarding services

Market value of manned guarding services has been collected from Frost & Sullivan report (2008b). Total size of the market is €24.5 billion. CoEES (2009) also provides some numbers that are slightly different, but of the same order of magnitude. The Eurostat *sbs_na_1a_se_r2*) table, however, provides a higher value €34.5 billion. A detailed table per member state is provided in chapter III.

Network and information security

IDC (2009) estimated the value of the EU Network and Information Security (NIS) market in 2007 in €10.7 billion of which 4.8 corresponds to software products, 4.7 to services and only 1.13 to hardware. More details of this market are provided in chapter III.

Summing up numbers

Aggregating these numbers, the revenues of the security market in Europe could be in the range of €59 billion[25]. This number does not include market revenues of areas closely related to security like the RFID market, or the electronic payment market. The value represents the 0,48% of the total GDP of the European Union in 2007, a value that can be considered low when compared with other economical sectors as for example. €1,115 billion in transport in the EU in 2005 according to Eurostat (2009) or €670 billion of the ICT market according to EITO (2007).

[25] Senger (2006) provides a rough estimate of the European market for the year 2004 around €100 billion including the computer security and the equipment and services market.

EMPLOYMENT

Private security services are the main source of employment in the security market. Frost & Sullivan estimates this figure in 1,240,000 employees for 2007. Eurostat table *sbs_na_1a_se_r2* provides a quite close estimate 1,112,903 for 2008. Measuring the remaining labour force is not easy. For the equipment market, the survey has found only a very outdated value in Frost & Sullivan (2004) that estimated this number in 54,500. Subtracting revenues of security services from total revenues and comparing it with revenues and employees of the defence industry, a linear estimation could be made where working people would give a value in the range of 300,000. Nonetheless, this estimates lacks of any empirical ground.

EXPORTS / IMPORTS

Reliable information about export and import has not been feasible. Very obsolete data was found in Frost & Sullivan (2004) about export of security equipment regarding CCTV, intrusion detection systems, and access control systems. It amounted to €1.31 billion in 2002 of which 0.19 corresponds to export outside the EU and the remaining amount to intra-community sales. The value represents only the 0.04 percent share of the total European Union exports in 2002. Imports represented €1.79 billion of which 0.58 corresponded to imports outside the EU sharing probably the USA the lion share. As can be seen, the trade balance was negative for the whole European Union in that year. These values, however are rather old, and only reflect part of the security market.

From the different reports analysed Russia, South America (especially Brazil), Middle East (Arabia Saudi[26], UAE), India and Far East (China[27], Singapore) are the main importing countries. Middle East and Asia seem to be markets with a growing demand, a consequence of the shift of fundamental terrorism to these regions due to large support populations and lower security controls than USA and Europe (Enders and Sandler, 2006:201). The private demand of security in South America could be influenced by a higher perception of insecurity due to high crime rates, large differences in wealth, and the weakness of state law enforcement organisations. These threats combined with low domestic industrial capabilities offer business opportunities to the European industry. Main exporting firms are large EU companies like the ones mentioned at the end of this chapter. The competitive edge of the industry is mainly based on non-price factors.

MARKET SIZE TREND

Prospects of market evolution are not easy to forecast. As has been shown public and private expenditures have overall a positive trend slightly higher than inflation. Yet, these values do not collect private investment. Unfortunately, the information is too aggregated to identify growth variations in the different market segments. Furthermore, time-series information of past growth is a feeble indicator of market trends.

[26] For example, Saudi Arabia awarded a contract to EADS Defence and Security as prime contractor for a full national border surveillance programme valued in €1.6 billion (Defence News, 1 July 2009).

[27] China is a complex market with price controls, high tariffs rates, restrictions on investment from abroad and absence of stringent property rights. This creates an adverse business environment for foreign companies. According to Ecorys (2009:26), China has used reverse engineering to develop products and enter the security market.

Information can be attained from market studies. These studies make interviews to stakeholders to know their expectations in sales and purchasing plans. Such values may be aggregated to get a better estimate of market trends. For example, Frost & Sullivan (2005) estimated a compounded annual growth rate above 10% in 2005 a value too high compared with the ones recorded in table 1. A more recent report of Frost & Sullivan (2008d) for physical security reduces this value to 6.9% till 2013. Having in mind that these reports are mainly focused at investment organisations some biases may exist in the information provided. Yet, the majority of reports consulted (Frost & Sullivan, Gartner, Ecorys and IDC) show beyond question a positive trend, at least until 2008. This could point out a trend in Europe to invest in security above general growth.

The recent economic downturn that began in 2008 will negatively impact on the market. Yet little information is available for assessment. A downturn implies the decline in the construction sector, closures of banks and commerce and so on, that will shrink the demand. It also means tighter budgets that will stifle large investments in new equipment and the life enlargement of deployed systems and a delay in their renovation. While continued technological improvements and sustained security concerns (e.g. the loss of jobs of a downturn may increase burglaries leading end users to install alarms for basic level of protection) may insulate the market to some extent to this fall in demand, it probably will not be immune.

THE WORLD SECURITY MARKET

USA expenditures

A look at USA spending in security is necessary being its market the largest in the world and its industry the leader. The main difference that can be observed is the large federal budget, in addition to States and cities expenditures, whose yearly value can be seen in the next table. This quantity has no comparison with EU Commission expenditures that are more modest. Budget includes expenditures in natural and man-made disasters and the fight against terrorism rather than organised crime. The peak that is observed in 2006 was mainly due to the Katrina hurricane. Customs and Border protection, Coast Guard, Emergency Management Agency, Transport Security and Immigration and Customs enforcement are the beneficiaries of nearly the 79 % of the budget. However, these numbers reflect total budget, not the amount spent in purchases to industry as we have shown previously for EU member states.

2001	2002	2003	2004	2005	2006	2007	2008	2009
15.0	17.6	32.0	26.6	38.7	69.1	39.2	40.6	49.2

Table 10. Homeland Security Budget in billion $.
Source: ***The budget for fiscal year 2010, historical tables. Outlays by Agency***

The U.S. DHS (2009:17) reserves 2% of the budget to Science and Technology. That means that nearly $1 billion is allocated to research and development. This amount could be in practice larger having in mind that some supplies often involve a certain amount of development. Nearly one half of the budget goes to CBRN countermeasures (James, 2004:33). Yet, the majority of federal homeland security R&D remains outside the DHS (*ibid.*: 34). The Department of Justice also invests relevant quantities in R&D as the National Institute of Justice (NIJ) which invest $0.233 billion according to the 2007 annual report.

The value of USA private expenditures is not accurately known. O'Hanlon *et al.* (2003:xii) estimated total expenditures about $100 billion of which $35 is federal share, which means that Federal States, cities and private organisations spent around $65 billion. Civitas Group (2006) estimated this value at around 43.3% of government expenditures. Hobijn (2002) and Hobijn and Sager (2007) estimated private spending for the USA based upon protective services labour cost and electronic security capital cost in a higher value at 83.43%.

The market in other world regions

Some values of the security market in other world regions can be seen in the following table.

Country	Revenues in billion €
EU	26.0
USA	42.0
China	13.5
Japan	3.8
Israel	2.7
Russia[28]	1.1
Rest of the world	13.9
Total	**103.0**

Table 11. Security market size in world regions. Source: Ecorys (2009)

Other values have been found during the research. Civitas estimated world revenues for the year 2006 in the range of $55 billion, where USA share was only $31 billion. This amount is considerable smaller that the quantity estimated by Ecorys. EPOSS (2009) report estimate the safety and security equipment world market around €25 billion, of which 5 billion relates to electronic devices. The market has an expected growth rate of 7%. The report states that the European market is more than one third of world market in this domain (approximately €10 billion). Again, such large differences invite to be wary about the accuracy of these quantitative estimates.

MEMBER STATES INDUSTRY

Security companies in Europe show notably differences in size. There are a few number large companies with a European, and often international, dimension capable to provide products and services across countries. They are followed by medium size companies able to operate at national level ensued by a large number of small companies that often are only able to operate at regional or local level. Smaller companies mainly focus in providing security goods and services to the lowest market segment, i.e. residential and private companies market. These companies mainly distribute, install or integrate small to medium scale security systems, or provide manned guarding services.

The largest companies have a good market share in some sectors, but Frost & Sullivan (2004:3-1) reports that companies holding a share higher than 20% are unusual. Hence the concentration pattern is of oligopolies where a few companies jointly have the largest market share. In its report, Frost & Sullivan estimates that there were more than

[28] The U.S. Commercial Service report written by Elizaveta Ninyaeva (31/01/2008) estimates total size in $6.8 billion of which $1.7 was equipment.

150 security systems manufacturers who have presence in Europe (100 in physical security and 50 in RFID). It also estimated that the number of distributors and installers was very high, in the range of 2,500, most of them of very small size.

Differences in the industry between member states can also be appreciated. It is more developed, as could be expected, in the most industrialised member states where a rich network of companies provides a solid ground for organising the supply chain. More relevant countries are United Kingdom, France and Germany followed by Italy, Sweden and Spain. Italy has a large number of small security companies (*ibid.*: 8-17). Other countries, in particular Eastern Europe, have a smaller security industry with few domestic production capabilities. For this reason, they have to recur to imports for getting some products.

European champions

In the following table, it can be seen the main suppliers of security products and services across the European Union, being some of them true world leaders which operate in the international market. As can be seen, many suppliers belong to large and diversified holding groups. Revenues and employees working in the security market have been given. However, such information is not always available. In such a case, total holding values have been provided. These companies are often prime-contractors in the provision of large security solutions, due to their system integration capability. They hold a relevant share in the market segments where they operate.

Company	Main activity	Country of origin	Rev.	Empl.
Assa Abloy AB[b]	Access control systems, doors and locks. Companies belonging to the group include HID Global, Securitron and Keso.	Sweden	€3,177	32,723
Axis Comm. AB[b]	IP-Cameras.	Sweden	€180	663
Bosch Security Systems[a]	Consultancy, design, deployment, maintenance and monitoring, CCTV, sensors, alarms, system integration	Germany	€1,349	11,610
Cassidian (old EADS Defence and Security)[a]	Nationwide Security, Critical infrastructures security, major events security, ICT security	Europe	€5,400	28,000
CISCO[b]	Communications security, networked CCTV	USA	€28,446	66,129
G4S[b]	Solution design capabilities in security systems. Manned guarding services.	United Kingdom	€6,372	561,876
GE Security	Wide security product portfolio	USA	$1,800	3,150
Giesecke and Devrient	Banknote production and processing, smartcard-based solutions, software and services for electronic payment, Security documents and identification systems	GE	$1,700	10,000
Gemalto NV[b]	Identity and security cards	Netherlands	€1,659	10,000
Gunnebo AB[a]	Bank Security & Cash Handling, Secure Storage, Entrance Control and Services	Sweden	€640	6,000
Honeywell[b]	Intrusion, video surveillance, access control, integrated solutions.	USA	€26,300	128,000
IBM Global Technologies services[b]	Business continuity and resilience services, system integration, computer security services.	USA	74,555	398,455

Ingersoll-Rand[b]	Electronic and biometric access control systems.	USA	€9,527	60,000
L-3 Communications Security and Detection Systems	X-Ray screening systems and Metal Detectors.	USA	$345	608
Niscayah[a] (old Securitas Systems)	Consultancy, design, deployment, maintenance and monitoring.	Sweden	MSEK 7,600	5,600
Panasonic[b]	CCTV systems	Japan	€71,977	305,828
Prosegur[a]	Security Services	Spain	€2,100	100,000
SAGEM Morpho (ex Sagem Securité)[a]	Identification, detection and biometrics	France	€904	5,600
Securitas Group[a]	Manned guarding services.	Sweden	MSEK 62,667	260,000
Siemens Building Technologies[a]	Building automation, fire safety and security.	Germany	€7,007	42,575
Smiths Detection	Explosives, chemical and biological detectors; weapons and contraband detection.	USA / UK	€2,300	639
Sony[b]	CCTV systems	Japan	€69,486	180,500
Thales Security Solutions[c]	Security solutions for supervision and control of critical infrastructures, Id documents, computer security.	France	€2,977	19,827
Tyco Fire and Security / ADT[d]	Video-surveillance, RFID, electronic access control, intrusion detection, electronic article surveillance.	USA	$7,200	61,000
United Technologies Fire and Security[a]	CCTV, access control, intruder, systems, fire detection and extinction. Brands: Chubb, Kidde, Onity, Lenel.	USA	$6,500	43,000
a: company web page at 12/01/2010. b: the 2009 EU industrial R&D investment Scoreboard. c: Annual report 2009 page 132 d: Data provided through direct contact with the company.				

Table 12. Main companies in the security sector. Revenues in millions

RESUME AND CONCLUSIONS

This chapter has presented some relevant numbers and information about the security industry. No authoritative source or institution has been found which provides expenditures on security, as this term is understood in this survey. We have used different approaches to obtain the best estimate of this market. First, we have analysed government expenditures and second we have tried to estimate some economic values based upon information supplied by the proper industry. Based on available information total expenditures in security would be in the range of €59 billion of which nearly one half would correspond to security services.

While some insight has been achieved, it can be said that, unfortunately, numbers obtained should be seen as broad indicators or rough estimations of economic activity rather than exact measures; especially having in mind that revenue information has been collected based on interviews and unknown methodology. Therefore, numbers shall be used and valued cautiously.

Overall, data collected is too patchy to provide a stable ground onto which advanced economic analysis of the sector could be performed in order to better characterise and

assess the market. Availability of data and quantitative information remains an outstanding issue that certainly will require further research. Solving practical problems to get accurate and reliable information about the market will demand, nonetheless, a non-negligible effort whose costs would certainly need some kind of sponsoring.

III. BASIC MARKET CONDITIONS

Basic market conditions can be seen as exogenous characteristics or features with a substantial influence on the structure, conduct and performance of an economic sector. A meaningful understanding of these conditions is a first step to improve the knowledge about the security industry.

Hence, the aim of the current chapter is to examine in detail these conditions from both the demand and the supply side. From the demand size we analyse with some detail the main customers, demand drivers and restraints, geographic markets, price elasticity and substitutes, growth rate and cyclicality, and marketing and purchasing methods. The important question of a single European security market and the barriers for its consolidation is addressed in detail. From the supply side key aspects such as the supply chain, technology, research and development, product and services features, and the role of standards is described.

DEMAND SIDE

Main types of customers

Unlike defence, the achievement of security often calls for some kind of collaboration between public and private agents. Whereas private companies and individuals are able to protect themselves to some extent applying different measures; they still need the support of public bodies to effectively fight against terrorism and organised crime. Police forces and the judicial system are essential instruments to enforce law and prosecute members of these groups, whereas civil protection agencies are crucial to provide emergency services and a first response in case of a security incident with wide and severe consequences on society.

Governmental organisations and agencies are the main customer in the security market, ensued by large organisations, usually in charge of critical infrastructures[29]. Companies are the third major buyer of security. Individuals is the smallest market segment in revenues, although the largest in number of customers.

Government / Public sector

The government, being the principal and ultimate security provider to society, requires relevant capabilities in surveillance, intelligence, prevention, protection, interdiction, response and recovery, and attribution to combat terrorism and organised crime. Such relevant role makes the government the purchasing leader of security goods and services in terms of volume, innovation, projects scale and prominence. Governments are sophisticated buyers that usually demand high-end products and services, with a large industrial impact, to demonstrate effective security solutions.

[29] The European Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection defines a critical infrastructure as: *An asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*

These capabilities are distributed across different public organisations and agencies like police forces, forensics and crime investigation units, customs and border protection, prison management, emergency or civilian protection. These organisations and agencies have different responsibilities and operational scope (European, national, regional or local level). Most of them have their own budget and have autonomy to decide on what products and services buy. This means that acquisition in the public sector is not centralized and thereby the different needs and purchasing capabilities of these agencies do display a less common and coherent purchasing pattern.

Private companies

Private companies and organisations are the second major consumer of security. The protection of their business becomes an integral part of their strategy in order to avoid the economic losses that a security incident may create. Security investment is the result of business continuity and security plans that address measures to defeat potential threats and vulnerabilities. Many corporations have a security department and a Security Officer in charge of managing security issues.

Operators and managers of critical infrastructures[30] largely invest in security because the disruption of services they provide can potentially have, in addition to internal losses, far-reaching and long-lasting consequences due to the dependency that society and other infrastructures have on them. Infrastructures deemed critical are transportation (road, rail, air, inland, ocean and shore sea shipping and ports), health, energy (electricity, oil, gas), water, information and communication, finance, food, chemical (e.g. refineries). The production of dangerous goods, the defence industry and agriculture may also share to some extent this critical nature.

Transportation is a paradigmatic example of critical infrastructure since it handles the movement of large volumes of people, goods and services. It is international in scope and intertwined in economic and social activities. For instance, a few seaports handle a major share of the goods moved in international trade, and commuter and rapid rail transit systems are the circulatory systems of urban environments, critical to the functioning of towns and cities (NRC, 2002:211).

Being transport a major target of terrorism, organisations and companies involved in this activity are large security investors. The most developed area is air transportation where the identity of the traveller and the inspection of his belongings inspection are routinely performed. These controls are complemented with surveillance of main areas of the airport, protection of the perimeter protection against intrusion, and access control for the working personnel. Rail and road transport also benefit from security measures, however the open nature of these systems and the large mass movement they often support limit certain kind of controls since, being too strict, they will cause intolerable delays (above 15-30 minutes).

[30] These infrastructures are indistinctly owned by state agencies, private companies and often managed through some form of public / private partnership.

Banks and financial institutions invest largely in security to protect the high value assets they custody against theft. Retail stores also invest in security for the same reason[31]. Private organisations with a large number of users and customers like shopping malls, cruise ships, resorts, amusement parks, or sport arenas are also large investors to avoid any security incident.

Individual and residential market

Individuals buy security to protect themselves and their main assets, fundamentally against ordinary crime and theft. Since household is the main asset and the place where people live, this market is many times known as residential market. According to Frost & Sullivan (2006) estimates there were 163.7 households in the EU in 2005 of which 5.5% were equipped with some kind of security equipment. This low value suggests that security does not hold a high priority in the individual's life and that current measures – based mainly on fences, doors and locks– do satisfy security needs of the majority of citizens, been seen more advanced measures as a kind of luxury expenditure.

Demand drivers and restraints

The sense of security is a fundamental desire of the human being. This is the ultimate reason of the demand of goods and services, since they are able to reduce or remove the chance of suffering damage on what one values most such as life and property.

A naïve approach would suggest that security expenditures are closely correlated with the statistics of terrorism and organised crime. Yet, statistical information of the EU and government expenditures and crime does not show *prima facie* a good correlation as can be seen in the next figure. Furthermore, the sparser nature of terrorist actions still correlates worse. This simple explanation, consequently, must be discarded and other factors with deeper influence in the demand should be searched for.

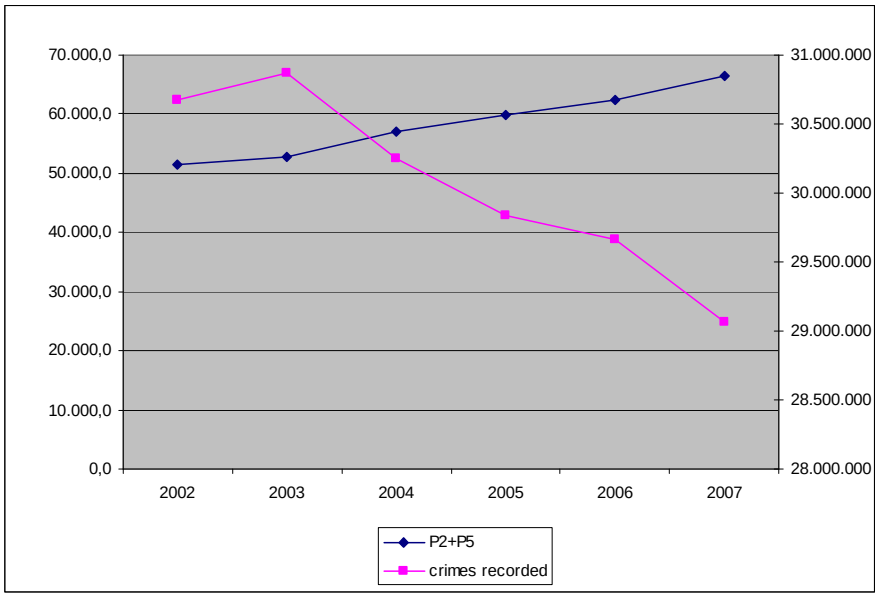

Figure 2. Security expenditures and number of crime in the EU.

[31] Frost & Sullivan (2004:6-56) estimated around 4.14 million retail stores in the EU (Eurostat number for 2007 was only 2.81 million, however information of relevant countries like France or Italy was not available).

Source: Eurostat.

From an economic viewpoint, the decision to implement security and preparedness measures should be driven by whether the benefits of added investment outweigh the costs of doing so. Additional resources should be allocated until the marginal benefits (i.e. reductions in expected losses of an attack) no longer exceed the marginal costs of improving security measures. Putting this rather simple principle into practice, however, is not straightforward, making it hard to estimate optimal levels of protective measures, or ordering them by priority. This is owed to the complexity of measuring the cost of terrorism and organised crime in quantitative, accurate and objective terms, and the benefits of security and preparedness measures in reducing such cost. Benefits and costs depend on many variables, whose real value and influence is unknown and traditional cost-benefit analysis is rendered nearly impossible (Jackson *et al.*, 2007b:38). Here, we analyse in detail these foreseen difficulties grouped around the following areas.

a) Risk perception, loss expectations and risk aversion,

b) Investment required to gain a feeling of confidence or peace of mind,

c) User acceptance.

Risk perception, loss expectations and risk aversion

Risk perception, loss expectations and risk aversion lay down the expected utility of a security investment. The frequency and the type of incidents occurred in the past, and the damage on possible targets may serve to assess risk and the undesired consequences. These values can be combined to measure the likelihood-weighted losses of a potential security incident and compare it with the cost of implementing a security measure. Finally risk aversion will determine the customer willingness to overinvest (underinvest) in security being he or she adverse (prone) to risk.

This quantitative measure is however troublesome. On the one hand risk assessment requires information regarding the likeliness of such events as for example predilection of terrorism on a certain target. This assessment is not feasible when statistical information about terrorism and organised crime behaviour is unavailable or it is not disclosed by intelligence and law enforcement agencies for security reasons[32]. Nevertheless, in a context where group behaviour changes according to past experience and evolving circumstances, historical data might be misleading for assessing risk.

The difficulties to assess risk scientifically –and its reduction due to a new solution– are highlighted in OECD (2003b:15). Models, such as game theory, may be used to palliate

[32] Private organisations may be also reluctant to share with the government their proprietary knowledge about their vulnerabilities and preparedness level, as well as to report security breaches for fear of negative market reaction. This is because they may be exposed to firm liability, drop in share value, and loss of customer trust and competitiveness. Chalk (2008:7) for example reports that one half of piracy attacks are unreported due to the losses associated to the incident reporting. Data breach notification acts exist in some USA states regarding the loss of personal data. The European Union has develop a proposal of Directive on this issue (see the common position 16497/1/08 adopted by the Council on 16 February 2009). The directive relies on '*naming and shaming*' to encourage firms to improve protection of personal data. This levels up the playing field and prevents the competent being penalised for taking protection seriously (Anderson *et al.*, 2007:26).

some weaknesses, in particular when the empirical frequency distribution for very uncommon events cannot be identified and the real performance of the new countermeasure is unknown. A large variety of disciplines and areas of expertise needs to be combined to develop valid threat scenarios and to understand causal relations and the phenomenon under analysis in order to unfold a workable model. Anyhow, models have to simplify reality assuming linear relationships or standardised behavioural patterns of human beings and are not immune to a certain degree of subjectivity. These limitations may make these models inappropriate to explain, reproduce or predict with accuracy and reliability real world conditions and complex phenomena.

The evaluation of potential damages is hard to estimates. It needs to assess the likelihood that the terrorist or criminal action succeeds as well as the likelihood that the damage propagates (second order effects) due to interdependencies of the target with other assets[33]. Cross-effects of different security measures to reduce risk and damages are also hard to ascertain. Moreover, the quantification of losses such as property and assets, restoration costs, or loss of revenues may be relatively easy; but non-monetary values such as business reputation, personal suffering, items losses of purely personal value (e.g. the symbolic value of a national monument), or family stability are harder to evaluate. Finally, long-term effects of protracted events, such as changes in consumption and investment spending on different sectors (e.g. tourism) due to risk aversion, are often neglected due to their computational complexity.

The cost of new measures raises also problems. The total cost of ownership needs to consider (research and) development as well as system operation and maintenance costs. These values will have some degree of uncertainty until implemented. Cost shall include not only the financial and material costs but also other more intangible such as any reduction in privacy and civil liberties, inconvenience, or time spent by the public due to security measures.

Risk assessment and its reduction due to a new investment is made therefore within an environment of bounded rationality (Simon, 1978) based on cognitive biases due to unavailable or wrong information about perceived levels of threat, imperfect information on the effectiveness of security measures, inability to make complex calculations under uncertainty demanded by strict *rational choice*, simplified models subject to scientific controversy, where interest and attitudes of those involved in the decision –such as elected official, experts, the public and firms– may differ, and where psychological factors such as culture, age, character may play a significant role. In such environment there is no objective measure of risk and different views of risk, involving different technical considerations, may be pertinent and legitimate. In such a case, maximizing the expected utility or net pay off is extremely complex for policy makers for two reasons. First, because data collection and utility computation is costly, and second because there may exist more than one and often competitive objectives, whose indifference curves to make trade-offs, are hard to determine. This may be particularly true in decisions for safeguarding against low probability events characterised by large losses, as many security events are, where probability and losses based on statistical analysis will have a low degree of confidence.

[33] For example, many benefits of ICT systems applied to security derive mainly from the capability to speed up response. Developing models on how faster response can reduce eventual costs is a substantial challenging task.

A decision process driven by bounded rationality is based on heuristics, whereby only a tiny part of the space of potential solutions is analysed –since alternatives have to be searched for at a cost–, and simplified reasoning, whereby rules of thumb and rough estimations are used to rank solutions. Such process will settle for solutions that appear to be *good enough* whether or not truly the best. Bounded rationality may give room to decisions where intuition, emotion (fear and moral panics), pre-established beliefs, constituencies concerns, the behaviour of other actors, or debatable slanted reports may play their role. This explains, for example, that after a terrorist attack overinvestment is quite frequent due to a higher risk perception, in particular when the means of attack are novel or the location is unprecedented, while just the opposite occurs after a large period without incidents. This pitfall is caused by the use of the '*availability*' heuristics whereby a very recent event is taken as a signal that similar events are likely to happen soon, a method that leads to systematic and serious biases on probability estimates (Tversky and Kahneman, 1973).

Risk aversion may accentuate the desire to invest in security well above the expected loss. This may influence, for example, Public Authorities that may feel the need to retain the confidence of their constituencies, especially in election years, investing in rather visible security measures even if they are not too effective[34]. In the same vein, many executives likely prefer to invest rather than exposing themselves to the risk of being sued for negligence should be the firm target of an attack.

Behaviour influence in risk perception

The behaviour of terrorism and organised crime influences the kind of threat and so the demand of security solutions. This behaviour varies between groups due to differences in goals, strategies and capabilities. For example, Islamic terrorism is more prone to cause indiscriminate mass casualties (Europol, 2009). This behaviour changes over time according to changes in the political and economic climate and the capabilities of these groups based on their human and financial capital.

A fundamental advantage of these groups is the small risk they confront due to the freedom with which they can select the time, place and method of their attacks; the small quantity of resources and the economic cost that their actions demand, the openness and accessibility of many high pay-off targets, and the easiness to conceal their planned actions. This behaviour, perceived from the outside as unpredictable, makes the achievement of a wide protection very difficult, since safeguarding each potential target is unaffordable.

The decision of a terrorist group to attack is influenced by many factors. Davis (2009) enumerates the following ones as the more important:

- The perceived benefits, which also include the increase of popular support such as attacks provoking government repression[35]. The acceptability of perceived

[34] As Schelling (1963) shows, in a game-theoretic framework, an efficient strategy may be to demonstrate power toward perpetrators, because expectations about the behaviour of the opponent may be more relevant than the worthiness of the implemented measures.

[35] Historically when groups have committed (or have been perceived as committing) particularly atrocious attacks, there have been backslashes in sympathy and presumably in material support as well.

risks to achieve operational success such as weakness of defences, group capability, and group effectiveness versus counterterrorism measures.
- The acceptability of resources required such as money, technology, people, or time.
- Enough situational awareness achieved through intelligence[36], surveillance and reconnaissance, as well as technical knowledge and communications capabilities.

Attacks are chosen from a combination of target attractiveness, feasibility, effectiveness and cost, and therefore, they are hardly random, though due to asymmetric information they are perceived so. For example, suicide tactics are used primarily against well protected targets whose probability of success using a conventional method is low and that of apprehension is high. Such evidence of rationality means that we can expect terrorists to be clever and to make good operational choices that exploit target weaknesses. More positively, however, it means that with good intelligence and analysis, we can expect to understand their calculations and how to affect them with the adequate incentives.

As a conclusion, it can be said that since terrorists are sensible to operational cost-benefits considerations. Hence, this information should be used to assess the risk of potential attacks and to devise countermeasures that increase their costs and bind their benefits.

Box 2. Factors influencing terrorist decisions and behaviour

The limited availability of resources of these groups and the constraints imposed by law enforcement and other well-funded security measures, in particular the need to go undetected, place anyhow significant burden on these groups and abridge their operational capability. This explains that they apply a very conservative or very practical strategy, grounded on widely diffused, well proven and inexpensive technologies in comparison with those that States can afford[37]. Offensive capabilities are often limited to a small range of tactics and technologies, mainly based on arson (e.g. Molotov cocktails), bombings (based on rudimentary home-made explosives that can be readily assembled using ingredients that may be found elsewhere) and firearms. Yet, the sheer destruction these groups cause using such means and tactics creates a media sensation that is highly effective in transmitting their message to the public. Bigger risks are only accepted for high pay off targets where sophisticated equipment is indispensable to succeed. This also explains that in spite of the growing interest of terrorism in advanced weapons including CBRN, gathering the resources and means to acquire (or manufacture), deploy and use these weapons with success is outside the capacity of the majority of these groups[38].

[36] Personnel with privileged access to critical infrastructures, particularly control systems, may serve as terrorist surrogates by providing information on vulnerabilities, operating characteristics, and protective measures.

[37] Yet available technologies are used quite effectively. For example, the internet, satellite phones, and other advances in communication permit the coordination of operations and the execution of attacks at widely dispersed places. This facilitates their activities and according to Enders and Sandler (2006:41) has helped to increase the transnational number of terrorist incidents. Europol (2009) reports that several organisations run their own websites on servers located outside the EU –whose owners and webmasters cannot be identified easily– to recruit new members, promote radicalization and raise funds.

[38] Although accurate surface-to-air missiles are widely available and have been in some terrorists' arsenals for years, they have not been used against commercial aircraft outside conflict zones.

One of the main problems in evaluating the utility of security measures against terrorism and organised crime is that these organisations do not passively react to them. On the contrary, they try to undermine those using different methods. For example, they may shift their attacks to more vulnerable targets; change their tactics and operating methods; use available technology in quite innovative ways, or use new technologies to overcome current protective measures such as for example the use of non-metallic guns, non-nitrogen-based explosives or flammable liquid explosives to disable current controls. In the same vein, illegal border traffic in the south of Europe has proved flexible, innovative and capable of learning, despite substantial efforts at control.

The potential efforts of terrorism and organised crime to degrade the effectiveness of defensive systems mean that they must be addressed in planning to ensure that efforts to protect society are effective. Expending resources for systems that can be easily neutralized in a sense *does the terrorist' work for them* by diverting those resources away from better use (Jackson *et al.,* 2007:132). However, some systems can continue to pose problems for these organizations even after they know how to evade or neutralize them. Those problems are a price the group must continue to pay over time-in the effort needed to counter the technology, the increased planning burden it creates, new or different weapons that must be procured, or resources that must be expended to protect the group from its effects (Jackson *et al.*, 2007:132).

If the utility of the security solution significantly falls, as a consequence of the new behaviour, to the point of becoming obsolete, it will trigger a new cycle of measures and the demand of new equipment in a recurrent process that resembles an arms race. The contest of measures and countermeasures between the State and these groups may press the research and development of new security equipment with higher performance and rise expenditures and product prices, however not always with a clear outcome in terms of increased security. R&D will contribute to unit cost escalation, whose steepness will depend on the innovation capability of terrorism and organised crime that probably is lower than defence arm races due to their resource constraints and other reasons commented in Box 3.

The capability of terrorist groups to use technology to leverage the magnitude of their attack is also a relevant question when deciding the resources that societies should commit to curb their activities. Jackson (2001) analyses this problem and has found many restraints on terrorist groups to use adequately technology to achieve their goals. He has also found an overestimate of the actual threat posed by the terrorist adoption of some weapons due to their complexity. He cites for example the unfulfilled prediction made in the 1980s and 90s that the use of grenade launchers would greatly increase. The ability to adapt a technology for unique *local* requirements seems to demand a much deeper understanding than that required to just use the technique or product. One example he gives is the fabrication of homemade mortars by the PIRA. Although

Terrorist, so far as we know, have not attacked agriculture and have not attempted to seize or sabotage nuclear reactors (Jenkins, 2006). To date, most terrorist groups have used the internet to facilitate their own operations rather than to disrupt the operations of a target audience (Enders and Sandler, 2006: 257). The White House (2003:viii) National Strategy to Secure Cyberspace recognises that *the required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date*. Chalk (2008:19) also explains the low level of maritime terrorism due to its technological complexity. Yet, strategically, these groups will be interested in declaring more capabilities than available with the aim to raise the threat level and fear.

straightforward in principle, the mortars constructed by the group experts had generally proven inaccurate and caused many operational accidents.

While bomb-making manuals are readily available on the internet, those same characteristics mean that the knowledge delivered has likely not been *validated* and could simply be wrong. Additional tacit knowledge has to be gained through experimentation than can be dangerous and expensive such as deaths caused by homemade explosives. Moreover, the pressure of law enforcement may prevent the adoption of a new technology or deprive the time necessary to adopt it.

Group leadership and structure may also have a negative influence on technology acquisition. If discussion of problems and solutions is viewed as dissent or criticism to the leader for choosing the technology, no such questioning will occur and the group will lose the chance to optimize its use. And if a movement chooses to organise itself using a *cell* or *leaderless-resistance* model –where small independent groups operate in varying degrees of ignorance about the plans and intentions of other group members– technology adoption by the entire movement will be essentially impossible (as may be the case of Al Qaeda in relation to CBRN weapons).

The availability of financial and human resources may hinder the capabilities of these groups to profit from certain technologies. Because of the illicit nature of their activities, extremist groups cannot take advantage of the labour mobility which exists among commercial firms. In the absence of confounding factors, the larger an organisation, the more likely its members are to posses the appropriate explicit and tacit knowledge base to efficiently absorb new technology and the more likely it is that the organisation can afford to devote some of its members to technology acquisition activities.

Finally, the short live of most terrorist groups partially explains why most operations use relatively simple technologies and '*non-innovative*' tactics.

Box 3. Terrorism capabilities, technology and innovation

Embedded and dual use security solutions

Security solutions, rather than defence equipment tend to have more than one use. They are many times integrated in the design of wider solutions which incorporate specific features to underpin security measures. The inherent difficult of measuring objectively the utility of security solutions to counter rare events explains that some investment are more palatable for decision makers when they are meshed in solutions aimed at achieving wider and more peremptory goals. This multipurpose nature helps to justify the investment.

Investment required to gain a feeling of confidence

The utility of a security solution depends on the vulnerability reduction in terms of a less likely event and fewer consequences. Utility should be measured in terms of net value, i.e. after discounting the cost of the investment to trade off between performance and cost. In theory, the selection process shall choose the solution whose net value is higher. However, the availability of financial resources often limits the set of available choices. That means that, keeping other things equal, stakeholders with bigger

economic resources will tend to invest more in security provided they are more effective. And, in macroeconomic terms, it means that nations with a large GDP will be more prone to invest in security.

User acceptance and ethical issues

The utility also depends on the acceptance of security solutions which may downshift their demand, slowing down or reversing the deployment of these solutions. When the security solution is perceived as a degradation of the quality of life, as for example the time spent in airport controls, an adverse social, political or psychological response may be triggered. This negative response may unfold when the disutility surpasses utility as may be the case when disutility is clearly observable, whereas the potential damages of a security shortfall are harder to envisage. Disutility may be also perceived very high when fundamental rights[39] such as privacy or the search of social cohesion may be jeopardised by some solutions, especially when they are not subject in sufficient ways to political and judicial scrutiny.

Several security solutions raise concerns about their potential impact on privacy expectations of citizens. Apprehensions, in general, are based on fear of misuse or abuse –i.e. that these solutions are used for purposes other than that for which they were intended– and whether the loss of privacy is really required to attain the security goal. For example, there is a fear that governments use the new and powerful surveillance and facial biometric technologies to track people[40]. Employees may fear that management will be tempted to monitor their performance using CCTV cameras or access control systems. Also at issue is whether people will be arbitrarily monitored based on their race or ethnic origin or whether security staff may be tempted to indulge in video voyeurism by, for example, focusing on young, attractive females. A similar case is related to systems used to detect weapons hidden under clothes that show the image of a person nearly naked when millimetre waves or backscatter X-ray scanners are used, something found too intrusive and invasive by many citizens[41].

Concerns also appear when some technologies may reveal health information. This is the case of biometric retinal scans that can identify changes in the retina due to vascular dysfunctions caused by diseases such as AIDS, diabetes or high blood pressure. There are also concerns that, in the future, facial recognition may be used to detect expressions and thus emotional conditions. The lack of friendliness of some security systems may also induce a negative response. For example, retina scanning requires close proximity with the reading device. People may resist biometric devices because of hygiene issues

[39] See the EU charter of Fundamental Rights and the European Convention on Human Rights.

[40] In January 2001 a face recognition system was installed in the Superbowl in Tampa (Florida) in an attempt to identify 'wanted' individuals entering the stadium. (NTSC, 2006:73).

[41] Some prototypes of these systems have been tested in airports in the USA and Europe. The department for Transport and BAA trialled this kind of system on the Heathrow express train line and Paddington railway station in London in early 2006. According to GAO-10-484-T report, TSA plans to deploy 1,800 systems by 2014. To protect passenger privacy and ensure anonymity, strict private safeguards are built into the scanning procedure. The officer who assists the passenger does not see the image that the equipment produces, and the officer who views the image is remotely located in a secure resolution room and does not see the passenger. Blurring is also added to protect privacy and images are deleted from the system after the person is cleared. On the European view on this issued, see the European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection.

such as Japanese citizens[42]. And other people may find fingerprint scanning distasteful due to its criminal connotations.

The European data protection Directive 95/46/EC sets out strict principles that have to be observed in the design and operation of security systems that manage personal information. This is the case of systems that store biometric information, video images, or e-mail[43] since this information is considered personal data. Principles to observe are transparency, legitimate purpose, and proportionality. This implies fair data collection (e.g. right to be informed), minimised data collection, storage and processing; and adequate measures to assure confidentiality and security of processing in order to avoid data leakage[44].

The demand of widely accepted or regulated security solutions

When security measures are widely acknowledged by society as tacit social norms or regulations acceptable for the level of risk, then the demand of security goods and services related to these measures becomes more subject to the overall trend of society evolution. This is the case of transport where a more mobile and interconnected society is raising the number of passengers (see figure below) and merchandise across the world increasing the opportunities of clandestine immigration[45], commerce, theft and the free movement of terrorists and criminals. The creation or the expansion of airports, seaports, mass transport hubs and border checkpoints to support this growing traffic demand security goods and services to verify legitimate travel and trade, and avoid merchandise loss.

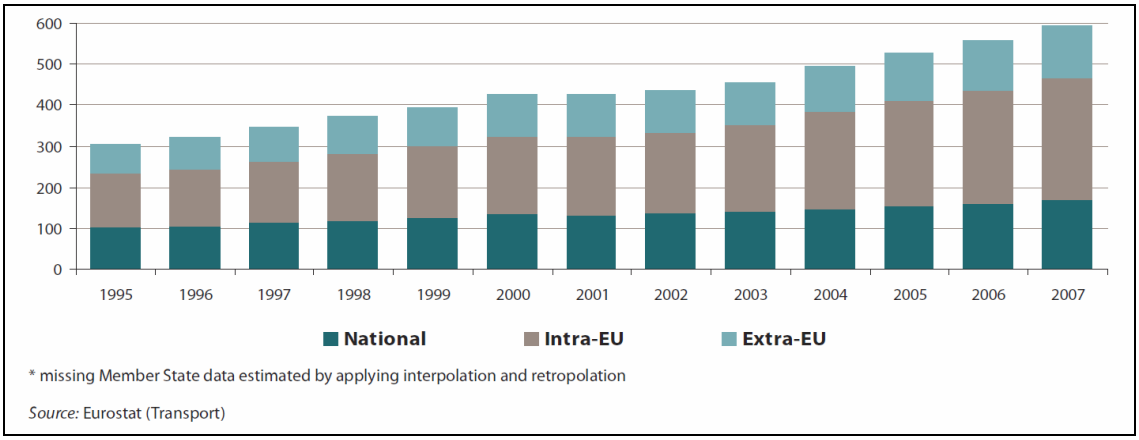

Figure 3. Air passenger in Europe

In the same way, the demand is correlated with the growth of certain businesses such as bank offices, retail stores, office buildings, enterprises or manufacturing units where the goods and services related to security and safety are considered an inseparable part of the business. The rate of renewal of certain assets like cars, personal computers, or

[42] More details can be found in GAO (2002) report.

[43] E-mail is correspondence and is covered by the right to confidentiality of communication laid down in the European Convention of Human Rights.

[44] The article 29 of the Directive sets up a Data Protection Working Party as an independent advisory body on data protection and privacy. Its mission is laid down in article 30.

[45] This is a consequence of population ageing of most advanced European countries that is creating shortages of specific skills combined with the growing population of developing countries and the expectations to earn wages in excess of those in their country of origin. This scenario will probably persist throughout the next decades.

households better explains the demand increase of car antitheft systems, software security packages, and home alarm systems. The growing momentum of e-commerce, e-banking services and other on-line services due to the development of the internet and the information society is also pushing expenditures in computer security to shatter the rising threat of cybercrime attracted by the sensitivity and value of exchanged information.

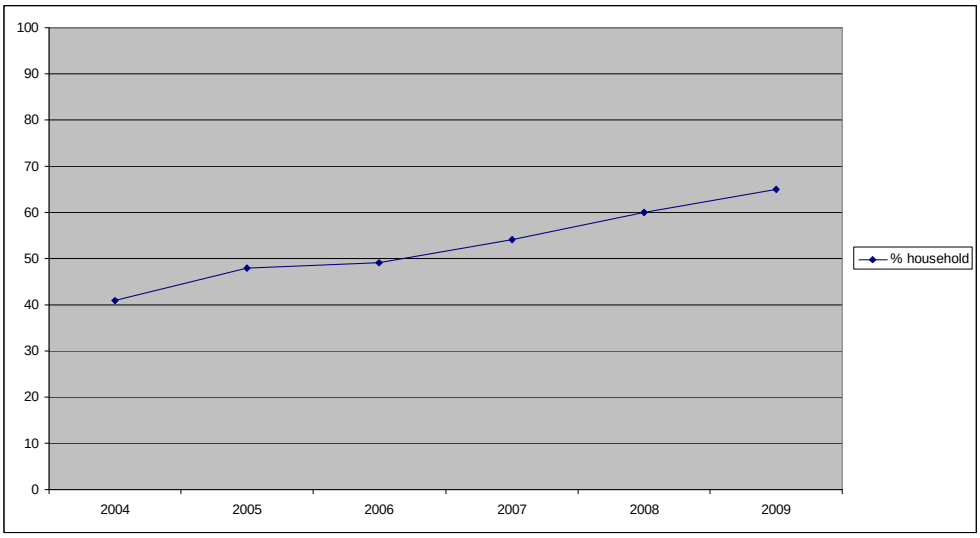

Figure 4. Number of European households with connection to the internet.

Security and other societal needs

Investment in security is driven by its perceived utility in comparison with other personal or societal needs. That means that in periods with low rate of security incidents, perceived as a less risky environment, or periods where income decreases, preferences may turn to other welfare competing needs considered more important such as healthcare or education.

The trade-off between security and efficiency

Security investment is associated with an efficiency loss since it is often seen as a misallocation of resources which has to be financed as an overhead internal cost. Security investment are often seen as unproductive since it, like pollution abatement and environmental protection, generates an intangible output (often hardly discernible from null effect) that is not considered part of private or public accounts.

Security measures are also perceived as a source of disutility since they are expensive to apply and usually diminish performance, create inconveniences and cut out customer satisfaction. This is because security entails monitoring and enforcing services such as inspections and controls. The paradigm is transport security where solutions reduce passengers or cargo throughput due to inspection delays. Other example could be the preservation of large dataset of e-mails or phone calls for investigative purposes as required by the EU data retention Directive 2006/24/EC[46].

[46] This directive obliges operators to keep data relating to mobile phone, fixed telephone, internet access, email and telephony regarding a communication's *termination* data (source and destination) and its date, time and duration –but not its content– for at least six months but not longer than two years.

Security investments, whereas reducing fragility and local disruptions that could lead to widespread and catastrophic failures, work also against productive efficiency in terms of lean production systems, resource concentration to increase economies of size, '*just enough, just in time*' deliveries to shrink inventories, and infrastructures coupling to leverage benefits from scale and interconnectedness[47]. This is because security requires robustness (system ability to tolerate failures) and resilience that is achievable through different means such as system hardening; redundant assets[48] and compartmentation (geographic backup sites, back-up lines or routes) and spare capabilities like spare parts and emergency teams able to provide enough resources to quickly respond and avoid any supply congestion in case of an emergency or security incident[49]. Consequently, security will stifle the competitive advantage of the industry and impact on their profit due to higher cost per unit sold or loss of customer base when such measures are perceived more as a burden than a benefit. As security measures raise operation and transaction costs, they usually have an adverse impact on trade and economy[50]. Their efficiency and opportunity may be questioned when security incidents are extremely unusual, using the social norm that it is hard to justify an expenditure that has not paid off (Krantz and Kunreuther, 2007).

The decision to invest in security by the private sector will consequently take into account these positive and negative effects. The assessment will be grounded on a cost-benefit analysis, whose benefits will be measured by the avoidance of losses related to damages to production and distribution facilities, harm to workers, loss of business, loss of reputation, legal liabilities and indemnification claims.

Private versus public benefits of security investments

But the social costs could go further and include the harm or loss of life of individuals, damage to the environment, and negative effects on other business dependent on the targeted industry (e.g. Internet Service Providers). When private benefits of security are significantly smaller than social benefits, private firms may have insufficient incentive to meet social objectives and companies will not invest adequately in security, thus decreasing social welfare due to an improper allocation of resources. This trend may be easily reinforced against a background of very competitive and cost sensitive markets such as transportation, energy or telecommunications where companies are unable to pass such costs on to consumers without experiencing a significant loss in market share.

---

47 For example, integrated supply chains that feed components and other materials to users just before they are required and just in the right amounts in order to keep low inventory costs. As Huang and Whalley (2006) demonstrate border control delays trigger an inventory raising response.

48 While such investments do increase security, they do not result in large revenues to the security market as is defined in this study.

49 For example ambulances, beds in hospitals or vaccines stockpiles. Yet, the large costs associated with this spare capability explain to some extent the complementary role of armed forces or international cooperation in large emergencies.

50 This may not be the case when customers perceive the transaction as too risky. In such a case security measures may be valued positively by the customer and companies will be interested in investing more. This is the reason of the considerable investment in computer security of e-commerce companies due to the considerable savings and earnings achieved moving on-line these services as well as their assumption of liability for on-line fraud (Anderson and Moore, 2008). In this case, non-dependable payment systems in e-commerce that may result in identity fraud may reduce more benefits in terms of lost gains from trade associated with transactions foregone than the stolen amount.

When market fails to induce agents to properly invest in security up the desired level, then society needs to agree on policy tools to encourage agents to adopt protective measures (Kunreuther and Heal, 2003). They may involve self-regulation to forms of co-regulation and government intervention. Self-regulation uses codes of conduct whose main incentive is prestige and reputation. They are often developed by industrial associations (e.g. IATA) and may allow that an agent does not make business with other agent if the latter has not subscribed the code. Regulation includes mandatory measures which are linked to fines and penalties for those failing to implement such measures. They are often accompanied of imposition of taxes on certain services or products to finance named measures, or fiscal incentives for those that implement such measures. The enforcement of regulations requires some kind of inspection system. Third parties may assist governments in this inspection as for example insurance companies who will reduce the policy premium if measures are properly implemented.

A liability system may also be used to enforce security if companies are found negligent of not providing a secure environment for operations and shall compensate employees, customers or third parties of the damages undergone by a security incident. Although such system has attractive theoretical properties, it faces practical problems due to high transactions costs, because determining the responsibility of the company and the amount of damage can be very costly and extremely time-consuming (Kunreuther and Heal, 2003).

The role of externalities in security demand

Security investments create positive and negative externalities that may influence the demand of market agents. An example of positive externality is the government investment in law enforcement that may reduce the general capabilities of terrorism and organised crime and raise the perceived feeling of security of citizens, lowering their willingness to invest in private security (Orszag and Stiglitz, 2002)[51].

Positive externalities may cause underinvestments of the private sector in security. This may raise concerns when it provides services that are essential to the functioning of society. These services can be considered to some extent as a public good, and hence private losses of a security incident will be likely smaller than social losses as for example some power outages have shown in the past (e.g. Italy 28/09/2003)[52]. Hence, some remedies as the ones described in the previous section may be needed to achieve the desired investment level.

Negative externalities appear when investments in the protection of specific assets may deflect attacks to softer targets, thus raising the insecurity of these potential targets. For instance, if a government responds by tightening security at official sites –such as embassies and government buildings– civilian targets will become relatively less secure and attractive (Enders and Sandler, 2006:83). Being security high on a country, terrorist attacks may be performed against individuals or corporate offices located abroad; and cyber-attacks can be launched against ISP providers with a lax security policy. Another

[51] The provision of government of *ex post* assistance (after hardship) also reduces parties' incentives to appropriately manage risk (before hardship occurs) *ex ante*. This behaviour is known as the Samaritan's dilemma.

[52] The externalities caused by the lack of home computers protection, which are increasingly loaded with malware aimed at harming other computers, is another example (Anderson *et al.*, 2007:19).

example is the selection of airports with limited screening capabilities (lack of inspection equipment or expert personnel) or, being capabilities adequate, the attack can be deflected to metropolitan train networks such as Madrid or London bombings. Europol (2009) reports that in the last years Basque terrorist groups mainly carried out attacks against soft business such as bank offices and government targets such as local administration or police offices. As a conclusion it can be said that investments that divert rather than deter terrorism and crime may be excessive from the social point of view because private investors will only care about their own protection rather than overall deterrence. Furthermore, if those who suffer the negative externality are unable to pay for their own security, then some sort of social exclusion may unfold.

Interdependency and cooperation

Many security measures are more effective when they are jointly applied by all the members of a community, association or coalition. This is because the overall security may be compromised as members do not apply measures and create security gaps while they free ride over the benefits of measures implemented by the remaining members. If there is no assurance that measures will be implemented by all members, a disincentive to invest in security is created (Kunreuther and Heal, 2003).

Coordination is therefore needed to agree on such measures. However, achieving agreements takes time since, as often occurs, preferences and available resources to implement such measures differ across members. In such a case, the agreement may delay –or even paralyse when it fails– the implementation of the desired measure. Such interdependency is a potential source of inertia in the market demand.

Agreements may be between private agents, public and private agents, EU member states or international. For example, the Schengen agreement for suppression of internal borders within the EU is an agreement between member states. International agreements are required for protecting activities with transnational dimension as is the case of transport or telecommunications. They are promoted by international organisations such as ICAO or IMO. They state common or harmonised practices, information exchange standards or equipment performance.

When some members find the security level insufficient, they may launch unilateral actions. This is the case of some USA and European initiatives described in chapter V. The main risk of such actions is that they may discriminate nations that have difficulties in implementing measures. For example (Chalk, 2008:41) reports that the fulfilment of the ISPS code precludes the vast majority of littoral countries. Aids, although, are sometimes given to implement the desired measures as is the case of the US DOE's Megaports Initiative.

The role of technology

While the demand curve can be considered fixed in the short-term, it changes over time as technological advances are able to offer more attractive products and services as for example higher scanning and inspection rates, lower false positives and negatives rates, higher reliability, savings on operating personnel, and fewer inconveniences. Such displacement of the demand curve, when quantum leaps in performance or sharp

reduction of price are achieved, can considerably stimulate the demand, in a similar way as the personal computer or the mobile phone attained in the past.

The role of government

Government plays a relevant role on demand since, being the ultimate responsible of the security of the citizens, it settles the national security policy. Such policy will determine goals and missions and the available budget, which in turn will settle to a large extent the demand of security products, in terms of product features, performance and quantity. Such policy is largely influenced by the societal perception of risk, but because this perception usually differs between social groups, it has to be agreed at political level.

National policy also will influence the non-government demand when incentives for citizens and organisations to invest in security are not enough. Governments may enact laws and regulations that force such investments in order to attain the social benefits that the market is unable to assure. The role of government is discussed in more detail in chapter V.

The demand of the individual / residential market

The individual demand of security focuses mainly in household protection against theft. Inexpensive mechanical locks –and sometimes armoured doors and safe boxes– are used for this purpose[53]. Phones and videophones are usually employed to control access to individual residence. More advanced solutions include the installation of intrusion detectors connected to an alarm system that may trigger a visual or audible alarm and send an automatic warning by phone lines, data lines or mobile net to a central alarm system operated by a security services company. The changing EU housing pattern towards single and double person housing units is likely to lead to an increase in demand for home alarm systems. The other important asset is the vehicle. It is protected using door and ignition locks and keys and may include an intrusion sensor. Its low cost makes that, today, nearly every medium range vehicle is equipped with it. These systems are directly installed by the car manufacturer. The last relevant household element to protect is the home computer. It requires software security packages to safeguard the equipment from attacks through the internet.

The demand of these products is fundamentally driven by the income, assets value and the feeling of insecurity of the householder which is basically influenced by the crime rate. Products tend to be standardized because threats are similar in nature and scope and customers are very sensible to price. Customers are not too literate on security issues and usually receive assessment on what to buy from a local agent or seller.

Home insurance plays a role in the residential market demand. Householders tend to install a basic alarm system to get a deduction from the insurance company. Insurance often is tied to the awarding of a mortgage that is usually needed when the house is bought. This explains that customers do not have a large interest in sophisticated products or technologies or the replacement of an old system. This reasoning is also applicable to small businesses which insure against theft (Frost & Sullivan, 2008a).
Specific demand drivers of companies

[53] The protection of money, jewels, and other relevant assets by bank offices that can provide a safer storage service can be an alternative option.

The security demand of companies is driven by the need to protect business and avoid the economic losses caused by a security incident, which may result in employees or customer damages, assets losses, or business disruption. Major threats include workplace violence, theft, or terrorism. The risk of large companies becoming a target of terrorism may be higher as long as States are increasingly protection their infrastructures and iconic buildings make them a difficult target to hit (see U.S. Department of State, 2004: appendix G).

The demand of companies focuses mainly in surveillance systems, access control systems, fire detection and extinguishing systems, anti-theft systems in finance and retail, and computer security. Small companies usually opt for high-volume, low cost security packages and services, while large companies have more room for solutions tailored to their needs. Investments apart from material and equipment also include security services to operate and maintain the security system as well as guarding services.

Overall large companies tend to be more effective in developing security solutions than medium and small business[54]. Large companies usually have a better knowledge regarding threats and potential solutions than small companies which may find more costly to shop the best value for money product. Since security solutions tend to exhibit economies of scale –i.e. decreasing cost of security per unit protected– the former may spend proportionally a lower quantity than small business in achieving the same security level.

Geographic markets

The security market, following the general trend of other industrial sectors, can be considered today largely globalized. The majority of security services and products including their subsystems and components are sold worldwide with few trade constraints. Controls only apply to certain types of equipment able to cause physical harm such as small arms[55,56] Globalisation affects the whole supply chain where comparative advantages in customer knowledge, system integration, advanced products and technologies and low cost manufacturing allies to provide a system with the best value for money.

This global character of the market is reflected in the existence of large security suppliers with a European or international dimension. This is the case of U.S. companies like General Electric, Tyco or Rapiscan; EU companies like Securitas, Siemens, Bosch, Smith Detection, or Sagem Morpho; or Japanese companies like NEC, Panasonic or Sony. Companies from Korea, Taiwan or China also sell electronic components related to security in the international market. Foreign direct investment rather than awarding production licenses seems to be the preferred way of these

[54] IDC (2009:40) reports this fact in the computer security market, but the argument seems to be valid for other kind of security measures. Being the case, it means that mandatory security regulations may be relatively more costly to implement by small companies and organisations (e.g. a small airport) this creating an uneven playing field.

[55] According to Ecorys (2009:180), export of chemical detection devices is blocked by customer authorities to countries, when they are included in the list that prohibits export of dangerous materials.

[56] The recent Directive 2009/43/EC on intra-community sales is aimed at reducing such controls within the European Union.

companies to increase revenues. These companies have frequently, apart from marketing and post-sale services, production facilities in foreign countries and even research facilities such as Bruker Daltonics facilities in Bremen and Leipzig . These large companies operate in the stock market and their shares can be bought by foreign investors.

Notwithstanding, geographic proximity between buyers and sellers often provide key advantages for selling products and services. Local distributors, suppliers and value added resellers usually have a better knowledge of the market and culture of their customers and provide more efficiently services like design, installation, training, operation, maintenance, or repair in terms of rapidness and cost. This explains the presence of large number of small size local suppliers and distributors and the territorial spread of security companies along the EU Member States.

Is the European security market fragmented?

One question that is often raised is that the European security market is fragmented and unstructured[57] in the sense that markets are national, a level playing field is lacking due to differences in national security policies and regulations[58], and the demand is too fragmented due to the large diversity of customers in some areas such as personal protective equipment (PPE). This question is important since departures from the single market may weaken competition, and impede the achievement of economies of large production and consequently it may negatively impact on market performance[59].

The analysis performed along this study shows that many security companies have a true European dimension as they operate in different Member States. Therefore, at first glance, it seems that artificial barriers, such as specific national regulations or standards that may impede companies to sell products and services in other Member States are not insurmountable (see EU merger 3688) although they could have a more relevant impact in small and medium size companies. Evidence of a large internal trade of security products have been found in Frost & Sullivan (2004: 9-7) where it can be seen that intra-community sales amounts 28,11% of total sales. Openness of the market to imports seem also relevant having in mind that for the same period 12,66% of purchases were made outside the EU.

Still, fragmentation may appear in the field of public procurement, when large systems are acquired and member states want that their industry plays a key role in the supply since the system is considered strategic from the security or the industrial point of view. While this preference is hard to unveil[60], some evidence of this practice may be observed for example in the purchase of emergency communications systems. Such contract awarding suggests that, apart from a preference on national suppliers regarding the provision of systems considered essential for national security, the improvement of

[57] See ESRIF (2009) or EOS (2009).

[58] Market competition across industry may be distorted when mandatory requirements to invest in security differ between member states.

[59] As opposed to the defence market, the appeal to article 346 (ex 296) TFEU in order to avoid common market rules (including State aids) can be considered problematic, even if it is interpreted in a wide way to protect national security interest, since it is restricted to a list of products that are fundamentally related to defence rather than security.

[60] The broad recommendation of many market studies to find a local partner, when bidding for government contracts or large infrastructures operators, may indirectly confirm this hypothesis.

industrial capabilities and employment have priority over best value for money solutions. Public procurement rules may be used to shape the demand and design the market with requirements and awarding criteria where national suppliers enjoy important advantages. Notwithstanding the case may not be general. Countries like the United Kingdom show more flexibility having awarded important security contracts to foreign companies like Sagem for iris recognition, Northrop Grumman for IDENT1 programme for replacing the National Automatic Fingerprint Identification System (NAFIS), or Raytheon for its e-Borders programme. Offsets agreements where some kind of compensation to national industry is provided within a government programme has not been identified, although foreign companies are usually sensible to government desires and integrate national partners in their proposal.

Another kind of fragmentation appears because purchasing is usually less concentrated (more orders but fewer units) than defence due to the large number of ministries, state agencies and public and private organisations and companies in charge of providing security to society. This fragmentation is to some extent inevitable and cannot be overcome easily due to the decentralize nature of purchases and the freedom of these organisations to buy their preferred goods and services.

Fragmentation may also appear in the area of research when programmes are funded nationally. Such fragmentation impact the market in two ways. On the one hand, aids granted may unnecessarily duplicate efforts when research projects are uncoordinated. On the other hand, member states may overfinance these programmes because they do not account for the negative externalities (i.e. market stealing) on the industry of other member states. If aids differ across states, they will distort market competition in the EU.

As a conclusion, it can be said that fragmentation of the security market due to national barriers seems to be lower than expected, whereas fragmentation caused by customers is an inherent feature of this market. However, more studies and quantitative analysis in the field of public procurement, R&D financing, and national regulations are needed to determine accurately any unnecessary fragmentation with negative impact on market efficiency.

Price elasticity and substitutes

Price elasticity reflects how customers will enter or leave the market as the price of goods and services changes and as a consequence the quantity demanded changes. It is measured as a ratio between changes in demand and changes in price. An inelastic demand means that consumers will pay almost any price for the product, whereas a very elastic demand means that consumers will pay a very narrow range of prices for the product. An inelastic demand means that a producer can raise prices and still increase profits since demand will not decrease too.

Being security a very valuable asset, it may be expected that price elasticity will be in general low, probably similar to the defence equipment where trade-off between product cost and performance usually favours the second. Operational requirements may reduce elasticity as long as high (but costly) product performance[61] is considered essential to

[61] Measuring equipment performance, nonetheless, has its own intricacies. For example the efficiency of a sensor depends on a low number of false positives and negatives. This parameter can be often

achieve security, as for example quick screening systems to avoid large queues in overcrowded airports. Other non-price preferences such as reliability, quality, brand identity and the availability of complementary products and services (e.g. operation and maintenance support) may have a large influence on demand making it more inelastic to price.

Sensitivity to price differs between market agents, mainly due to the available budget for security. Individual investors may be more sensible to price than companies since these investments are tightly restricted by their income. Small companies more sensible than large companies since the latter enjoy large revenues. Large companies are more sensible than critical infrastructures operators and the latter more sensible than governments[62]. This fact may explain that certain security products developed for high-end markets do find a hard path to percolate into low end markets. In sum early adopters of new and more sophisticated technologies and services are represented, apart from government, by large companies (e.g. banks, industries, airports) with higher purchasing power and longer experience in product acquisition or services outsourcing. Overall, these companies will upgrade their system more quickly than small companies that will be more inclined to exhaust the life span of their system.

Price elasticity of a product is also related to the presence of substitutes. If substitutes are few or imperfect –i.e. they exhibit differences- then demand will be more inelastic[63]. On the contrary, inelasticity will be smaller if products are very similar in performance such as some standardized electronic sensors used in the security field (e.g. handheld metal detectors). Whereas substitutes are common for some security products (e.g. cameras) they can be very few for some very specialised or complex security equipment (e.g. large portal truck scanners). Furthermore, if there are relevant costs associated with the change of product, buyers will have extra difficulties to switch once the product has been bought.

Many security solutions are integrated developments based on user's demand. In these cases, solutions offered by suppliers tend to be a more imperfect substitutes of each other and therefore with a smaller cross-elasticity. Besides, once started the development, the switching cost of changing the supplier will increase, since even if other product or system has advantages in terms of price or performance, the cost of dismantling the old system, redesigning it, and retraining the operators may be too high and will require additional financing whilst the risk and the uncertainty associated with the new solution will only disappear after entering into service. Such switching costs grow proportionally to the size and complexity of the system. Since the investment will

---

adjusted; however improving one will worsen the other. In addition, sensor performance may be closely related with operator skills and inspection time, where a smaller inspection time may result in larger false negatives. All these features challenge the purchaser capability of selecting the best price / quality product.

62 Within critical infrastructures operators differences can also be appreciated. Airport authorities tend to spend more funds in security than seaport or border authorities, due to the larger revenues generated by air transport in addition to the higher threat level of airports as target of terrorism (it is estimated that security expenditures of airports range between 15 and 20%). Even within the administration price elasticity may differ. Local police of small cities, apart from higher budgetary restrictions, may be more reluctant to buy expensive security equipment if they regard themselves as an unlikely target of terrorism.

63 For example manned guarding may show a higher deterrence capability that electronic guarding equipment.

have a long life and the maintenance of the system including upgrades are usually provided by the same supplier the relationship between supplier and customer tends to be long-lasting subject to conditions of bilateral monopoly. The paradigmatic case is large government security programmes such as an Automated Fingerprint Identification System (AFIS). This low level of substitution assures business continuity and is an attractor for the industry.

Manned guarding services, an activity generally outsourced by many organisations, is an example of service that is easy to substitute, since it does not usually involve large cost for the customer allowing him or her to easily change of company, if he or she is dissatisfied with the service provided. This explains the higher price elasticity of these services. Only when the provision of security services is bundled to a system provided also by the services company, the change must be more difficult.

Market size and growth rate

The size and the evolution of the demand is a relevant parameter to analyse in every economic sector. A large market size combined with a good growth rate is an attractor, while a small market with a shrinking demand discourages entry of new companies.

As has been shown in chapter II, the size of the security market in Europe can be considered modest in relation to the GDP when we compare it with other economic sectors such as the ICT market (tenfold higher). This may explain that large companies do not work exclusively for this market. Data of chapter II shows also that public and private expenditures have moderately grown in the last years with a value above the inflation rate of the European Union. Growth trends, however, differ across market segments.

However, the current economic crisis in Europe may raise attention to more pressing needs and result in a short-term freezing or falling demand. Industry showing fears of demand fall have been identified in some reports whereas others do record such fall[64].

Stability of the demand

A market with a stable or moderately growing demand is more attractive than a market with fluctuating or random demand, since companies will experience changes in expected incomes that will require costly adaptations of the development and production capabilities.

As we have seen demand of security is mainly related to risk perception. This value is mainly driven as we have seen by the number and severity of security incidents. New incidents may raise the need of enhanced security. On the contrary, a decrease in the number of incidents may favour complacency and the demand may stagnate or fall. This may easily occur when other more pressing societal needs largely surpass security needs.

[64] See for example Frost & Sullivan reports in 2009 'The Physical Security Market in Asia Pacific. Surviving the Economic Downturn' and 'Biometrics Market. Surviving the Global Recession'. A press note of the Spanish association APROSER dated 8/6/2010 reports a demand fall of 6% when compared with 2008 revenues. However, according to Gartner, the computer security market will grow 11% in 2010.

Unexpected incidents usually trigger the demand of new measures, which may call for the development of new system and the agreement of new regulations. The latter activities may take time and slows down demand growth. On the contrary, agreed regulations on the provision of security may dampen a demand fall. The demand of some services like operation and maintenance (or renewal) may be more subject to the stock of the security equipment installed base rather than changes on risk perception.

Variations in government demand, as we have seen in chapter II, tend to be slow. This is mainly due to the inertia of the budgetary process. Whereas pressures of constituencies may influence budget size, this process tends to be slow and quantities change only slightly from year to year. However, government demand in certain market segments is mainly driven by large acquisition programmes which show a cyclical behaviour combining periods of great feasts with periods of great famine.

Marketing and purchasing methods

The individual customer purchases security products and services to local brokers or dealers. They play a relevant role in the design and installation of the security solution based upon user needs and standard off the shelf security products (e.g. a alarm unit with different sensors). The assessment and the after-sale service they provide is key to enhance the attractiveness of a rather standard and mature product whose differences with competitors are small. The supply of alarm systems is usually tied with the supply of remote monitoring and maintenance services.

On the contrary, the Public Administration purchases security goods and services as a consequence of programmes that usually follow a planning, programming and budgeting process derived form national policies. The acquisition is made using the rigid (and cumbersome) public procurement regulation in order to assure transparency, accountability and equal treatment to all parties[65]. Transactions tend to be infrequent, large in value and duration. Bidders tend also to be few, often reduced to reputable firms. The preparation of request for proposals, where the list of requirements and the awarding criteria are set, is a complex and resource intensive task. Not less is the formulation of tenders by the industry and the selection of the best proposal. The whole contracting process may easily surpass a year and the supply contract may take years for large systems. Development and production contracts include elaborated formulas to lay down prices, procedures to audit costs, and other clauses to prevent monopolistic rents. The transaction cost[66] is a large part of the total cost due to complexity of the whole process. The Administration often reserve rights in the selection of subcontrators and key suppliers.

While acquisition may be based upon products available in the market, it is not uncommon that it may entail considerable product development integration products to fit user needs. Even feasibility studies and a R&D phase may be required. In such case, government involvement tends to be high. For more complex systems, the government,

[65] It follows the Public Procurement Directive 2004/17/EC. The new Directive 2009/81/EC *on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security* offers a more flexible environment for security provision.

[66] This cost embraces the costs of planning, bargaining, modifying, monitoring and enforcing a contract.

suppliers, regulators and professional bodies tend to work together with users *ex-ante* to negotiate the design, methods of production and post-delivery innovations (Hobday, 1998).
The purchasing method of companies lies in-between. They tend to have a deeper knowledge of their security needs than individuals, be more sophisticated, and use open tenders instead of direct contracting. However, differences may appear between small business and large companies. In the first case the process may be simpler, while in the second the process is closer to public procurement procedures. Anyhow transparency in the awarding process does not go as far as public procurement being enclosed the process by confidentiality. Purchasing usually involves representatives of the different departments in the organization: financial, general management, security, IT, human resources, purchasing, architects or independent consultants. The negotiation process takes time due to the higher complexity of system requirements, considerations of system operation and maintenance, or the desired service level. The contracting and supply process is usually shorter than Public Administration and may be in the range of months.

SUPPLY SIDE

The supply chain

The supply chain of security equipment can be considered large even for single equipment. Equipments are usually composed of different parts and technologies that require specialised and unique capabilities for its design and production that are hardly achievable by a single firm. Industry usually finds advantages outsourcing or buying (instead of manufacturing) parts of the equipment that are cheaper or have better quality when outsourced. This reason explains the deverticalizacion of many industries and the increasing number of companies involved in the supply chain. This chain is especially large in complex security solutions such as a border protection system composed by a large number of systems, subsystems and components. An indicator of the large size of the supply chain may be found in the list of technologies identified in the European Union PASR programme STACCATO having in mind that companies only master a few ones. As it occurs in other economic sectors today this chain easily crosses borders in the search of higher performance or lower prices to improve the competitiveness of the final product or service[67]. Component vendors may come as far as Japan, South Korea, Taiwan or China.

Therefore, a key factor of success in this market is the proper management and coordination of this supply chain to integrate key technologies and maximise product value at affordable cost. This explains the relevant role of companies specialised in system engineering and system integration; the formation of supply clusters, strategic alliances and long term supply agreements; the acquisition of upstream companies who own key technologies by integrators and solution providers; and the interest of companies in developing open (instead of proprietary) standards interfaces to easily integrate security components into the final product.

[67] For example, Smiths Detection is sourcing cabinets for their explosive detection system to Eastern Europe and EADS electronic boards to the Estonian company Elcoteq (ECORYS, 2009:114 and 228). Cogent, Inc. is producing their biometrics readers in China (interview with Cogent representative in Essen Messe 5/10/2010).

Technology

Technology plays a relevant role in nearly all the security market segments. While the ability to clearly understand customer needs and goals as well as the individual pieces of the problem and their interdependencies is required to translate them into system requirements and service specifications, it is equally important to choose the adequate technologies and define the path of progress to satisfy the (sometimes stringent) product features. This may include not only the exploitation of available technologies, but also the development of new (sometimes disruptive) technologies based on brand new scientific and technological advances. The lack of mature technologies, in supporting product performance or cheap manufacturing methods, is often the reason that hampers the development of markets and the diffusion of new products. This is for example the case of face recognition methods in biometry, RFID in transport security, or the combination of two or more sensors or screening technologies to compensate for each other's weaknesses in drawing attention on potential threats.

Electronics[68] and information and communication technologies play a quite relevant role since they are embedded in many security equipments providing the main added value and key capabilities unattainable without them. Different algorithms, processes and user interfaces are able to underpin security measures such as the detection of anomalies that may warn of a threat or the identification of perpetrators based on information retrieval, analysis and fusion from large databases. Computers code and man hours of software development for security systems show a clear growing trend.

Information technologies are also essential to increase the efficiency of the life-cycle processes of a security system from the design to development, manufacturing, test and maintenance since all of them use knowledge and information as for example concurrent engineering and lean manufacturing. They facilitate the generation, processing and distribution of the large amount of information that is needed today to manage the supply chain[69].

Technology enables both product and process innovation which provides competitive advantages in terms of enhanced performance or lower manufacturing or operating cost. However, mastering technology involves a significant effort in which uncertainty in the final outcome (and the potential profits) can be considerably high. This may restraint the investments in new technology and innovation and be a source of poor market performance. This is a question than will be analysed in more detail in next chapters.

The role of research and development

[68] The electronics industry is largely driven by semiconductors. The supply chain of the semiconductor industry is composed of chip design, mask generation, wafer fabrication (foundries), packaging and test. This chain is today largely globalized bringing significant price reductions due to economies of scale, competitive labour rates and large consumer demand (ICAF, 2006). Semiconductors are allowing affordable solutions in many fields such as home protection systems or low-cost personal smart secure portable objects (trusted personal devices). The combination in the early 90s of cryptography and smart cards into Subscriber Identity Modules (SIM) contributed to the wide success of GSM standard for mobile communications, but also to automatic digital identification and security, payTV, e-commerce, e-banking, e-health, or e-governmental and institutional (EPOSS, 2009). Integrated circuits are also essential for microsize and low-power RFID tags.

[69] On the contribution of information technologies on firm's performance see for example OECD (2004:85) 'Understanding economic growth'.

The relevance of technology implies that research and development play a key role in this market. This activity encompasses different levels of effort. It may involve the adoption of an existing technology, the adaptation of a technology to a particular solution, additional developments to fully integrate the technology in the final solution, applied research to shape a technology to an specific security issue, or basic or fundamental research when the current technology performs unsatisfactorily and key scientific advances (e.g. material sciences) are needed to achieve a new capability[70]. Long lead-times characterise the latter activity and periods between 2 and 10 years are not uncommon (DSB, 2004). University departments often collaborate with industry in this activity.

The security industry largely innovates grounded on technological advances developed in other economic sectors including defence[71]. The dual nature of many intermediate and final products used in security favours the absorption of these advances; and the large amount of R&D investments in civilian markets assures a good chance to profit of available and inexpensive scientific and technical opportunities. A good example is the PMR market for emergency communications, which has profited of the advances of cellular commercial market (Ecorys, 2009:218). More uncommon is basic and applied research for unfolding new, otherwise not available, technologies without which product performance would not be improved as could be the case of pulsed fast neutron analysis for cargo inspection equipment.

Research and development requires extensive test and evaluation as well as field experimentation to assess equipment performance and operational utility. In addition to high-skilled personnel, R&D requires specialised equipment for design, development and test, and in some cases the support of State laboratories as for example the testing of chemical weapons detectors. The whole activity consumes hence a large quantity of resources and is one of the main cost drivers of the industry[72].

While technology push explains to a certain extent the development of new solutions, demand pull is also a key driver of market progress. The changing tactics and means of terrorism and organised crime, as we have seen, devaluates over time the utility of available products and services. This stimulates the investment in research and development and product improvement to preserve (and raise) current capabilities.

Security products features

Security products range from very small and isolated standard off-the-shelf equipment for individual use such as a handheld metal detector to large integrated systems as a border surveillance system. In the first case, standardised production methods are used for delivering ready to use products. In the second, the large and complex system is designed and build based on user's demands. This involves the development and integration of building blocks that are manufactured or provided by specialised

[70] A more detailed description of these activities can be found in DOD (2009).

[71] For example X-ray from scientific instrumentation mainly applied to health care and non-destructive quality inspection; computer networks from the telecommunications industry, ATM magnetic cards for access control, or simulation software.

[72] According to Freeman (1986:175), it is more that 50% in the field of electronics, a sector closely related to the security market.

suppliers. These hardware or software blocks are usually standardised commercial off-the-shelf components, yet in some cases they are fabricated under specification requiring some design changes or even a complete development. For example, an access control system is composed of card-readers, doors, a centralized computer system and the management software. The system design focuses in the adaptation of the solution to the specific environmental conditions as for example the architecture of the building for intrusion protection or the development of specific functionalities. The delivery of a security solution often involves a phase of installation, deployment, testing and tuning with a non marginal impact on final cost. Other times solutions require a mobile platform (land, sea, air or space) that has to be conveniently adapted to the specific security mission such as survey and patrol of specific areas, support of special operations, or first response in the aftermath of a security incident.

The technical architecture of a security system is usually composed of sensors, communication channels able to transmit information, central units that collects and process data and a user interface that presents relevant information to the operator about the environment which may compromise security helping to increase awareness and to respond properly. Such kind of products accounts for the fundamental role that electronic, information and communication technologies in this market. As a result it may be expected that some industrial features appear also in the security industry such as the relevance of economies of scale, scope and learning, the need of large capital investments for supporting R&D and sophisticated machinery for efficient production.

Some security measures need the support of large scale space infrastructures which are currently unfolded on the European level such as the Global Navigation Satellite System Galileo[73] for precise location and the Global Monitoring for Environment and Security (GMES / Kopernikus) for earth observation. They constitute a strong and reliable backbone for implementing a variety of security applications. Such markets have been analysed elsewhere[74].

Product durability

Security products are characterised by a relatively long life. Advanced sensors and video systems typically have a life expectancy of 5 to 7 years. Access control and alarm systems can expect to last for 10 to 20 years (TCRP 86, Vol. 4). Emergency PMR systems can extend over a 20 year period. This creates a lock-in effect that may tie the customer to a specific technology or standard for a long time, since the investment will be only replaced after it is fully depreciated.

Durability of security products is subject anyhow to its adequacy to counter threats and its degree of technical obsolescence. While it may be very slow in some cases, it may be rather quick in others. For example, new threats as the rapid and constant development of new computer malware, explains the constant delivery of new equipment and products releases and patches for updating computer protective software. And the

[73] The system is expected to be fully operational in 2013 (European Parliament, 'Getting Galileo into orbit 2013'. Reference 20080414BGK26528).

[74] See for example Ecorys (2009). Competitiveness of the EU Aerospace Industry with focus on: Aeronautics Industry. Within the Framework Contract of Sectoral Competitiveness Studies ENTR/06/054. Final Report. Client: European Commission, Directorate-General Enterprise and Industry.

extraordinary pace of change in electronics (Moore's Law), information and communications technologies ensures that many parts and components of security systems become rapidly obsolete and may undergo lower performance and spare parts shortages, forcing the system update due to the increasing maintenance costs. When the durability of the product is too short the market orients to the provision of a permanent update service where ownership plays a minor role.

Dual nature

Many security products show a clear dual nature, i.e. they have a multipurpose functionality. That means that the product will benefit of a higher utility and demand, and hence its development will be more easily financed. For instance, investment in fire protection systems and incident management systems are useful not only against natural or unintentional man-made disasters but also against terrorism. Personal emergency response systems can be integrated with home alarm security systems. Border management systems may deter terrorism and organised crime, but also speed up the flow of legitimate commerce and people. Air and sea traffic management system may avoid aircraft or vessel collision, but also identify renegade aircrafts and smuggling ships. Systems to track information about merchandise may help to curb cargo smuggling and theft, but also to avoid cargo mishandling and to shorten port or customs clearance time. CCTV in mass transportation may also reduce acts of vandalism in public places. Access cards may be used to restrict the access to a building, but also to verify the presence of a person, or measure employee time and attendance. Matching of airline passengers with their bags may reduce incidents of lost luggage, but also avoid the surreptitious introduction of bombs into aircrafts. Research on mitigating the blast effects caused by explosives can be useful in protecting structures from earthquakes and other natural disasters. Investments in rapid diagnoses, better vaccines and therapies to struggle against emerging infectious diseases may help to counter bioterrorism threats. Filters to protect buildings against CBR attacks will improve indoor air quality and prevent respiratory infections, asthma and allergies among occupants. Water testing to detect chemical or biological agents will also improve overall water quality. UAV can be used to patrol borders, but also to survey forest fires, perform search and rescue missions, or locate illegal fishing activities. High-resolution satellite images of targeted geographies can be used for environmental monitoring and damage assessment; but also to locate terrorist training fields, drugs production areas, illegal mining or oil spills.

Price/weight relation

Security products characterise also by a high price / weight relation. The low impact of transportation cost on the final price facilitates a more international security markets and supply chains.

Security services features

The security market not only provides equipment, but also a wide range of services to satisfy this social need. These services are driven by a subscription based business model and they ensure a continuous flow of revenues and a stable demand to many security companies.

The most relevant service is manned guarding services in terms of revenues, employees and firms. Suppliers of equipment also provide complementary services such as installation, training, operation (remote monitoring), maintenance and repair services, as well as system upgrades.

Consultancy is another essential service. It is necessary to analyse threats and develop adequate contingency plans that may involve market and feasibility studies to identify and select the best option.

The role of standards

Standards perform a range of useful functions in the economy. They provide for compatibility between products and systems. They serve to enhance quality. They may efficiently reduce variety and, more generally, they promote understanding and diffusion of technology by providing information. Taken together these functions, they promote the spread of new technology, a process that economists increasingly see as prone to market failure, since market power and imperfect information may both figure in making a given diffusion path (or indeed the lack of one) sub-optimal. The development of *standards* provides a means by which those failures can be corrected or at least ameliorated. It is reasonable to hypothesise that institutions, which ameliorate those failures, may have an important and quantitatively significant effect on the long run economic growth. Public standardization agencies may add two important qualities to the standards they promote, namely *openness* and *credibility*, which can be essential to the standard success (Temple, 2005:3).

An important point however is that the creation of *standards* is itself subject to market failure, and there are strong presumption that, unaided, markets will underprovide for standards. This last point is probably well understood: the development of standards involves fixed costs, and the gains may not be appropriable by the individual firm which develops one. Together, these give standards properties akin to a *public good* (Temple, 2005). Such failure explains that governments usually promote its development.

Standards are particularly important as means of assuring interoperability, a key feature of many security solutions that are based on information networks whose elements are developed by different suppliers. They also level the playing field decreasing information asymmetries between market agents. An open standard –whether given to the market or under some form of general public licence or cooperatively developed– can enhance competition (by lowering entry barriers) and stimulate innovation (by providing guidelines to developers of complementary products). The adoption of a common standard can enormously stimulate market growth, as GSM in mobile telephony has shown. On the contrary, lack of standards or standards not commonly accepted hamper market growth especially in markets where network effects are so relevant (Katz and Shapiro, 1994) as is the case of the security market.

Benefits from adoption depend upon network effects. These effects are complementary relationships in value creation among adopters of common standards. For example, operating on a common standard allows communications with more users. This is a direct network effect or network externality, if the adoption *per se* confers a benefit to others. Indirect effects are the result of widespread adoption that allows producers to achieve scale more easily (Stango, 2004). If no countervailing factors serve to bound the

increasing return effects, the process eventually will lock-in a single standard (more than one prevailing standard will be less efficient) while others disappear (David and Greenstein, 1990). Hence, companies that do not follow common or interoperable standards will be disfavoured. However, a standard to succeed needs to surpass a threshold number of adopters to assure enough large network gains[75]. In such environment, early adopters will confront higher costs, but will have more chances of winning the standardisation race.

Standards are also important to enhance minimum quality. There may well be demonstrable gains in situations of information asymmetry, where buyers are unable to distinguish between high and low qualities –at least in advance of the purchase without incurring in large test and evaluation costs. If, as is likely, high quality producers face higher costs that low quality producers, they might find it hard to survive in such market conditions, giving us a case of Gresham's Law in which the *bad drives out the good*. In such cases, minimum quality standards may help in mitigating the operation of the Law, helping consumers to distinguish different qualities (Temple, 2005:13). A certification authority will be more efficient, since it will reduce the transaction cost because customers would not need to test the equipment or service[76].

Since much innovation involves the deliberate development of variety on the part of firms, it might be thought that variety reduction standards may constrain innovation. While this may well be the case in some instances, there may be many others where variety is of little benefit to customers and achieving economies of scale may be more important (Temple, 2005:14).

Cards	ISO 7810 Physical characteristics ISO 7811 Recording technique ISO 7813 Financial transaction cards ISO 7816 Electronic identification cards with contacts (smart cards) ISO/IEC 14443 Proximity cards ISO/IEC 15693 Vicinity cards
Identification based on biometrics	ICAO 9303 – ISO / IEC 7501 Machine Readable Travel Document ISO 19784 Biometric application programming interface ISO 19794 Biometric data interchange formats ISO 19795 Biometric performance testing and reporting ISO 24700 BioAPI conformance Testing ISO 24713 Biometric profiles for interoperability and data interchange XML Common Biometric Format (XCBF) – OASIS.
Protection and Security of the citizen	CEN BT / WG 161 replaced by CEN/TC 391 Societal security CEN/TC 384 Airport and aviation security services
RFID	ISO 14223 15434 14443 15459 15693 15961 15962 17363 19762 ISO 18000 RFID for item management ISO 18033 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers ISO/IEC 18092 Near Field Communication - Interface and Protocol ISO 18185 Freight Containers Electronic seals ISO 18186 Freight Containers RFID tags ISO 24729 RFID for item management. Implementation guidelines

[75] Markets subject to network economies always confront with a large inertia in the initial phase. Because there are few users, few products and applications are developed. User do not have incentives to join until there are enough products and applications, but products and application's developers do not want to invest until there is a large base of customers.

[76] This is for example the case of explosive detection systems where probability of detection, probability of false alarm and system throughput has to exceed certain threshold values.

	ISO 24730 Information technology - Real-time locating systems (RTLS) ETSI recommendations EN 300 220, EN 302 208 and EN ERC 70-3 ETSI TR 102 436 449 562 and 649-1 IATA RP 1740. RFID for luggage Electronic Product Code (EPC) global standards
Information technologies	ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management ISO / IEC 27000 family of information security management standards. ISO / IEC 18028 IT network security. ISO / IEC 18043 Selection, deployment and operations of intrusion detection systems ISO / IEC 19770 Software Asset Management. RFC 2246 (Secure Socket Layer – SSL, Transport Layer Security - TLS). RFC 4301 and RFC 4309 (IPsec). Secure Multipurpose Internet Mail Extensions (S/MIME).
Digital certificates standards	ITU-T X.509.
CCTV	Video image compression: H.263, H.264 (MPEG-4 part 10), MPEG-4 / ISO / IEC 14496. Audio compression: G.726.
LAN / MAN / WAN	TCP / IP protocol. Connection of a security equipment to an IT network.
Freight container	ISO 6346 coding, identification and marking of intermodal containers. ISO 9897 (CEDEX) electronic interchange relating to freight containers. ISO/PAS 17712:2003 Freight containers -- Mechanical seals
Passenger Name Record	IATA standard.
Land Mobile Radio communication for Professional / Private Mobile Radio (PMR).	ETSI Terrestrial Trunked Radio (TETRA)[77]. EADS TETRAPOL APCO P25 (ANSI TIA/EIA-102) United States iDEN EDACS
Intruder alarm systems	EN 50130 (2004) EN 50131 (2004)
Video surveillance	EN 50132 Alarm systems. CCTV surveillance systems for use in security applications.
Financial security	Basel II agreement on International Convergence of Capital Measurement and Capital Standards. PCI DSS. Payment Card Industry Data Security Standards.
Security of the supply chain	CEN/TC 379 Supply Chain Security ISO 28000 requirements for a security management system to ensure safety in the supply chain.
Trace Explosive Detectors	ASTM E 2520-07 Standard Practice for Verifying Minimum Performance of Trace Explosives Detectors (International / US) ASTM F 2069. Standard Practice for Evaluation of Explosives Vapour Detectors (International / US)
Radionuclide Detection Equipment	Nuclear Security Series 1, IAEA, 2006. IEC 62244 / 62327 / 62401 Radiation protection instrumentation ISO 22188 monitoring for inadvertent movement and illicit trafficking of radioactive material.
Personal Protective Equipment	EN 469 Requirements for fire-fighters' protective clothing. EN 659 Protective gloves for fire fighter. EN 15614 Protective clothing for firefighters. Laboratory test methods and performance requirements for wildland clothing ISO 11613 Protective clothing for firefighters -- Laboratory test methods and performance requirements ISO 15538 Protective clothing for firefighters -- Laboratory test methods

[77] ETSI is working on new communications emergency standards such as EMTEL (www.emtel.etsi.org) and MESA (www.projectmesa.org) in addition to TETRA.

	and performance requirements for protective clothing with a reflective outer surface.
Fire Detection	EN 54 Fire detection and fire alarm systems.
Building Automation and Control Networks	ISO 16484-5 BACnet ISO 15745-4 Modbus OPC (Open Connectivity)
Road Ambulances	CEN. 1789 Medical Vehicles and their equipment (2007).

Table 13. Some standards applicable to security goods and services[78].

Standards may either hinder or enable innovation according to the business situation. Too early a standard may effectively shut out promising and ultimately superior technologies when technology is immature, forestalling in such a way price and quality competition. Too late and the costs of transition to the standard may be too high impeding diffusion of technology and the development of new or superior goods and services. Innovation and standards play usually a complementary role –both are necessary for innovation to succeed. Anticipatory standard-writing interacts closely with the innovation process helping to raise a common perception of the problems to be solved. The product development process of companies operating in markets in which network externalities are significant is closely related to this kind of anticipatory standards as the telecommunication industry (David and Greenstein, 1990).

Standards, however, are not laid down without cost and it takes a very long time due to the variety of parties that the standard setting body needs to consult and bring to consensus. Standards show path dependence in that the historical sequence of choices made, or the path taken in the adoption process, have a strong influence in the final outcome. Compromises have to be reached between all market participants that are invariably done at the cost of the performance of technology. Vested interests and strategic behaviour to protect proprietary from rival technologies (in the form of know-how, design and production assets) may cause delay and impede consensus. However, in many cases it is the agreement and coordination that a standard achieves that is important –the precise characteristics of the standards and whether it is actually the *best* standard– are far less important. The role of a standardisation body or public agency to solve potential adopters' uncertainty when they can delay committing to a standard and to coordinate the process –favouring openness, inclusiveness, transparency and coherence– may be essential to settle on a standard that is efficient from the societal point of view. Such role can avoid two potential inefficiencies: *excess inertia* –i.e. becoming locked-in an old inferior standard (reverse decision too costly due to long life expectancy of the product) – or *excess momentum* –i.e. too quick adoption based on uncertain assessment. Standardization bodies, however, may be captured by better informed industrial players, amplifying the anticompetitive effect of proprietary non-optimal standards[79]. Standards voluntarily agreed by industry (standardisation consortia) may take longer to spring up and may mask collusion (IPTS, 2005:82).

Standards also call for independent certification organisations that apply comprehensive testing protocols for warranting that developed products comply with them. This may

[78] Security products with electronic components have to fulfil related European Union standards such as Electro-magnetic compatibility (Directive 89/336/EC), low-voltage (Directive 93/23/EEC) or Radio and Telecommunications Terminal Equipment (Directive 95/5/EC) as well as health and safety standards (Directive 72/23/EC and 98/37/EC).

[79] When proprietary IP rights are incorporated into public body standards they shall be subject to fair, reasonable and non-discriminatory (FRAND) licensing commitments as has been the ISO 18185 standard for electronic cargo seals (e-Seals) based on Savi technology.

result in a costly burden for companies (when industry has to finances these organisations), a potential entry barrier to newcomers and an adverse influence on innovation[80].

Governments play also a role sponsoring *de facto* standards when they launch new large security projects that will create a large installed base of a certain product compelling subsequent public and private buyers to adopt the same standard. For example, Machine-Readable Travel Documents (MRTD) are driving global standard settings for biometrics on ID cards to match those being applied for in passports (Frost & Sullivan, 2005:3-7). Two main risks may unfold here. The first is that governments select an inadequate standard and lock the market in an inferior standard before the needs of most users have been clarified and addressed by product designers. The second is that in choosing a proprietary standard they may facilitate a dominant position.

As a conclusion, it can be said that standards are often a prerequisite for a good performing market. Standards developed by European (CEN, CENELEC, and ETSI) and international bodies are required in a market where network effects are relevant and suppliers and solutions easily cross national borders. Their importance is recurrently stated in the ESRIF (2009:198) and EOS (2009) documents. ESRIF suggests a kind of European Security Label that certifies that equipment fulfils standards, and EOS suggests European Reference Solutions to guide industry. The development of certification schemes for ICT security products, processes and services is also recommended by IDC (2009:10). The lack of common standards and certification bodies for security in Europe, a task being today a responsibility of member states, could be a relevant weakness that would need some kind of public action[81]. Ecorys (2009:24) attributes this shortcoming to the authorities' desire to retain control over technology in order to protect domestic industry or avoid dependence on external technology supply, but it may well be due to a weak perception of advantages of a European approach.

ETSI has been particularly active in the development of ICT standards in areas like mobile communications, lawful interception, electronic signatures, next generation networks, algorithms, emergency telecommunications, smart cards and RFID (Brookson and Zemerle, 2006). CEN regularly organises workshops on security issues. This activity is also being promoted in the European Research Framework Programme such as SECONDD on container interface; CREATIF on testing and certification facilities for CBRNE equipment; the Forum for Public Safety Communication Europe (PSCE) on facilitating consensus building in the area of public safety communication and information management systems; STABORSEC, on standards for border security enhancement. Projects related to public safety communications include OASIS (www.oasis-fp6.org), CHORIST (www.chorist.eu), DeHiGate (www.celtic-dehigate.org), LIAISON (liaison.newapplication.it). As opposed to product standards,

[80] For example in UK the Home Office Scientific Development Branch tests most scanning equipment in UK airports. Other example is the National Biometric Security Project Enterprise in the USA. Euralarm, a trade organisation representing manufacturers and installers of fire and security equipment aims also to play a leading role in certifying security products (See Euralarm Newsletter June 2009).

[81] COM (2007) 651 recognises also gaps in certification, testing and trialling schemes for explosive detection systems.

security services standards have not been found, this suggesting that there could be a wide room for improvement in this area.

RESUME AND CONCLUSIONS

This chapter has analysed the conditions and specific features which shape the security market and gives it its own idiosyncrasy. Such analysis is required to understand the importance of these exogenous variables that will influence on the structure, conduct and performance of this economic sector. Governments, companies and individuals have different needs and therefore its demand largely differ. Main demand drivers and restraints have been also analysed. Risk perception, loss expectations, risk aversion, investment required, and user acceptance basically determine the demand. Yet, bounded rationality, externalities, interdependencies and regulations have often not a minor influence on market demand. Geographic markets of security are largely globalized. However, national or local market conditions may give advantages to some domestic industries. Since procurement in this market is not centralized the customer base is larger in the public administration market as opposed to the defence market. Price elasticity of security products is not large due to its essential need and sometimes the lack of substitutes. Yet price elasticity of the different customers differs being lower in government and larger in companies and individuals. Market size in terms of revenues or employment can be considered small in comparison with other sectors like transport or ICT. Demand in macroeconomic terms tends to be stable and growing till 2008, but the actual economic crisis will have a negative impact on the market still unknown. Purchasing methods varies along customers. Public procurement and ruled procedures dominate the high-end market of government and large companies, whereas small companies and individuals tend to use less bureaucratic and formal purchasing methods.

The supply chain of security often involves many companies, especially for large and complex systems since many different technologies has to be integrated for achieving a product and companies only master a few ones. This chain is today largely internationalized. Technology plays a relevant role in the security equipment market, because it is essential to achieve products with better performance and cheaper cost. This implies that research, development and innovation, in one way or another, are key elements for market success; a question that will be analysed in more detail in chapter VII. Product duration is generally large creating a cyclical demand that is dampened with product upgrades and maintenance services. In other cases, duration is rather short (e.g. software) and updates needs to be contracted as a service. Standards play also a fundamental role as a means to achieve interoperability and assure minimum quality of products. The development of standard is subject to market failures and strategic behaviour. This suggests an active role of governments to implement some remedies.

IV. MAIN MARKET SEGMENTS

This chapter analyses the main segments into which the security market can be divided. Security demands a large variety of products and services of very different nature where it is hard to find coherence neither from the demand nor the offer side. Therefore, it is useful to decompose this economic sector in different segments or areas in order to understand them better and identify their regularities. In such segments, we will examine in more detail specific features like the main products and services, technologies, main suppliers, the supply chain, main customers, regulatory conditions and trends. The analysis follows the main capabilities defined in chapter I to curb terrorism and organised crime; namely preparedness, intelligence and surveillance, protection, interdiction, response and recovery, and forensics.

PREPAREDNESS

Preparedness addresses all the tasks related to planning, equipping, training, and rehearsing to have the means and the level of readiness required to forestall, avoid or undergo security incidents. Two relevant markets have been identified in this area: consultancy and training. Government, critical infrastructure operators and large companies are the main customers of these products and services. Economic figures about this market have not been obtained, but revenues would probably be rather small compared with other market segments[82]. Yet, this market segment provides key services to stakeholders and has a large influence on demand.

Consultancy

Preparedness requires know-how for making prospects about and analysing threats and vulnerabilities, assessing risk, developing contingency and resilience plans, designing methods and procedures for managing threats and security incidents, assessing the effectiveness of investments and resource allocations, performing feasibility studies of solutions to deal with insecurity, or managing the implementation of selected solutions. This analysis requires a great understanding of the complex nature of socio-technical systems related to (in)security to devise appropriate solutions.[83]

These knowledge intensive and highly skilled activities are often outsourced to small independent consultancy companies, specialised units of large consultancy companies, or small business units of prime contractors.

Training and rehearsal

Preparedness requires training and rehearsal of security personnel, first responders and decision makers, to prevent security incidents and being unfeasible curtail their consequences. Such training has to be coupled with programmes to test those skills and ensure that personnel remain vigilant even if no incidents have occurred for some time. This training may also be needed to educate people by means of campaigns to improve

[82] The British Security Industry Association (BSIA) estimated this valued in £8 million in 2006 that equates to 0,18% of market revenues.

[83] This knowledge area seems underdeveloped according to Pullinger (2006:5).

their observation capability of anomalies that may foreshadow a security risk, and their ability to adequately respond to a security incident.

Training or consultancy firms, sometimes able to develop training software, are the main market suppliers. Training for operating security equipment is usually provided by its supplier, but also by private security services companies like G4S Aviation Training Services. Training of own personnel is usually made internally by manned guarding services companies.

Modelling and simulation using computers and software able to artificially simulate the incident scenario may reduce long-term training cost while providing a more realistic environment. These systems allow staff to rehearse response and emergency procedures and gain experience in better planning and decision making under crisis conditions. They can be used for example to simulate the spread of a chemical agent after an attack or model human behaviour under stress. These means are supplied principally by companies with a good knowledge of security issues and the capability to unfold the appropriate software. Companies involved in military simulation enjoy competitive advantage due to the similarity of technologies. Products in this market are tailor-made and they do not show a clear dominant design which suggests a market under development with product in prototype stage.

INTELLIGENCE AND SURVEILLANCE

One of the ways of preventing terrorism and crime is through early warning of their hostile actions. The early detection of anomalies and security breaches as well as human intelligence play a central role in thwarting attacks before damage can be done. Equipment that may improve this awareness is of very different nature. It may been grouped in the following areas.

- Closed Circuit Television (CCTV)
- Intrusion detection and perimeter protection
- Border protection
- Identification and access control
- Goods and merchandise
- Intelligence systems
- CBRN detection equipment
- Other awareness products

Close Circuit Television

Close Circuit Television (CCTV) uses cameras that collect and transmit images that can be observed remotely in a monitoring centre. CCTV is probably the most popular surveillance sensor. It is very effective since it allows a centralized surveillance thus reducing the amount of personnel needed for monitoring. It is well suited for perimeter and interior protection against intrusion[84]; access control authorisation; the protection of public places like transport facilities; the surveillance of sports places to prevent hooliganism and soccer violence; or the protection against theft in department stores,

[84] In particular to investigate and confirm alerts triggered by other sensors.

shops[85], banks, casinos, hotels and residential areas. CCTV has a deterrence capability against illicit activities because recorded images can be used as evidence in a trial[86].

A CCTV system is composed of cameras, switching systems, monitors and video recorders. Cameras are composed of image sensor, optic, housing and other hardware to endure harsh conditions such as a box or dome, a wiper or washer, and a heater or cooler. They can be fixed or have a pan-tilt-zoom mechanism. They usually operate in the visual spectrum, but there are also infrared cameras able to see under poor visual conditions. The selection of the appropriate camera for the operating environment (e.g. enough definition to satisfy criminal justice requirements) is critical to attain a good performance. Cameras are today a relatively inexpensive commodity due to technological progress, economies of large production, and strong competition. Night vision cameras are more expensive since their market is comparatively small. The cost of the monitoring and recording system may surpass one half of the total cost of the CCTV system. Many components and technologies used in CCTV are used in other civilian applications, such as entertainment or film making, and largely benefit from advances in these areas.

CCTV technology has substantially changed in the last decade from analogue cameras, video tape recorders and cathode ray tubes to digital cameras, LCD flat panel monitors, and digital recorders able to store images on a disk. The new cameras are able to automatically focus and adapt lenses to the amount of ambient light. They can be remotely operated and transmit images over a local, metropolitan or wide area network –whether public or private– using the TCP / IP protocol. Captured images can be stored in Digital Video Recorders (DVR) or Network Video Recorders (NVR). Most advanced systems based on computers include a complete Video Management System (VMS) able to manage and present images to the operator. The digital transition has increased image quality; has simplified the installation (cabling) process, and has added capabilities to switch, compress, encrypt, store and quickly retrieve images using several criteria such as time, date, camera or location. In sum, more flexibility for exploiting captured images.

The advantages of the digital systems are crowding out the market of analogue systems, but at a slow pace since customers are fairly satisfied with the (large) investment already made (Frost & Sullivan, 2005:7-3). Frost & Sullivan (2008e:57) expects that digital system will have a larger market share than analogue systems in 2013. Major drawbacks of digital cameras are lack of standards and the transitioning of installers and users into the new and more sophisticated technology (Frost & Sullivan, 2005:7-1). As a way to extend the life of the installed base of analogue cameras, some customers are moving to hybrid systems where the analogue signal is digitised before being stored in a recorder or a video server (Frost & Sullivan, 2006a:5-10).

CCTV has limitations for the effective detection of suspicious and anomalous behaviour that warns of an illicit action. Since watching camera screens is both boring and

[85] CCTV is quite useful in small retail shops where the owner or manager has to operate the cash machine as well as keep a watch on customers. It was initially installed in shops selling luxury items, but today, it is enough cheap to be widely diffused.

[86] For example quantitative measures have shown that video surveillance can reduce acts of vandalism by 70-80% (Senger, 2006:35). However, according to other studies (Hempel and Töpfer, 2002) its impact on crime and violence seems to be inconclusive.

mesmerizing, the attention of most individuals degenerates to well below acceptable levels after 20 minutes of viewing. This restriction has stimulated the research in methods to help the operator in identifying anomalies and in reducing its workload[87]. Methods may range from simply motion detection to complex scene analysis, based on the processing of the video signal for recognising and tracking objects such as people and vehicles and monitor behaviour such as spot loitering (Munday *et al.*, 2006:11). Advanced applications include the detection of unattended luggage that may contain explosives; the recognition of persons using biometric analysis; the search of individuals within a crowd, or the association and correlation of discontinuous video tracking sequences. These technologies often require images of good quality. They seem still immature and subject to research. Yet, some companies are offering products to the market (e.g. USA Objectvideo company).

The CCTV market is a very competitive market with a large variety of products where customers may select those that better adapt to their needs and budget. According to Frost & Sullivan (2005:7-5), the European market is heavily saturated with a low demand and a high number of companies[88]. This point is reflected by falling prices and revenue erosion. The report estimates that 10 companies dominate the 65% of the market. These companies are present across Europe and have their own subsidiaries or share partnerships with dealers or installers. Panasonic is the leader, followed by Bosch Security Systems that expanded its activities in this market segment with the purchase in January 2003 of Phillips Communication, Security and Imaging (CSI) –the cameras arm of Royal Philips Electronics NV– as well as the company Vision Communication and Security AG (VCS) in July 2004, a company with good competences in video-over-IP solutions and network based surveillance products. The rest of the market is dominated by specialists such as Sony, Victor Company of Japan and companies offering complete solutions as Tyco, Siemens BT, and Honeywell with the acquired brands Ademco and Ultrak.

The market of IP cameras is led by the Swedish company Axis-Communication followed by the German company Mobotix. These cameras have triggered movements in the sector. Companies like Sony and Panasonic are pushing hard with a range of new IPV6 cameras and GE acquired Swiss-based VisioWave in 2005 to extend its portfolio. These cameras have also attracted companies coming from the information and communications technologies field. For example, Cisco has teamed up with Sony to produce IP-based solutions based on its networking capabilities. International Business Machines (IBM) is also providing consultancy and deployment services to enterprise level customers (Frost & Sullivan, 2005a:2-34). Other companies like HP or Accenture offer also expertise at system integration level for IP video surveillance (Frost & Sullivan, 2009:37). Defence companies, like SAGEM or Thales, are the main suppliers of infrared cameras (Ecorys, 2010).

The screen market is also very competitive and is driven mainly by the large non security demand. Main suppliers are located in the Asia Pacific region. They include well-known companies like Panasonic, LG Philips, Samsung or Sony.

[87] See for example, the 7th European Research Framework Program ADABTS.

[88] According to Frost & Sullivan (2005a:1-9), Europe leads the world in the number of installations.

Distributors and system integrators play also a relevant role in this market segment since CCTV systems are frequently a part of a security system. Examples of these companies are ADI-Gardiner, Thales and Group 4 Securicor, Securitas and ADT.

The CCTV customer base is quite large. Individuals, small commerce, banks, industry, infrastructure operators and government are the main purchasers of these systems.

The deployment of video surveillance in public places is regulated by EU data protection directive and national acts as such system may affect privacy rights. Such laws are not uniform and differ between Member States reflecting national preferences on what is considered an intrusion in personal freedom. For example UK is more permissive, while Germany is more restrictive. This different vision impacts in the CCTV demand and the installed base across the EU Member States. For example, in the United Kingdom there is one camera per 14 British citizens as opposed to one camera for 300 in Switzerland (Gras, 2004).

Intrusion detection and perimeter protection

Sensors are used to warn security staff of potential breaches helping to investigate and contain an intrusion. Its core operating principle is establishing and / or monitoring a norm and detecting or signalling a change in the norm, above or below, or with a preset threshold. The selection of the most appropriate sensor within the large variety available on the market is influenced by the nature and tempo of activity in and around the site or facility to protect, the physical configuration of the facility, the surrounding environment, along with the fluctuations and variations in the weather. Key performance parameters of a sensor are probability of detection, false alarm rate, and vulnerability to defeat. Arrays of networked sensors can be used to cross-check the validity of signals captured by others thus increasing reliability at the expense of a higher final cost.

Intrusion can be detected based on effective and inexpensive technologies. Sensors are able to detect broken window glasses through acoustic or inertial shock; opened doors through magnetic switches; chopping, sawing, drilling, ramming of roofs and walls through the detection of unusual vibrations or sounds; movement inside a hallway / room through simple radars based upon acoustic, micro- or infrared waves; or the presence of human being through the detection of heat measuring infrared radiation or pressure on the floor. Electronic barriers can be created by means of the emission and detection of a set of thin photoelectric beams. Unusual movement on exterior fences can be detected using sensors based on electromechanical, piezoelectrical, electrical or electrostatic field principles. In-ground fibre optic, ported coax buried line, balanced buried pressure line sensors or buried geophones are covert devices for detecting intrusion in places where landscaping or aesthetics are important[89].

Home and small business alarm systems demand very simple sensors such as zone sensors, window break sensors, magnetic door lock, and a smoke detector. Though such a system can be bypassed by a trained professional, it is a credible deterrent from petty criminals trying to infiltrate but without prior knowledge of the system. Solutions for

[89] A detailed explanation of this kind of sensors can be found in (NISE East, 1997).

high-end customers use more varied sensors and requires some engineering and design to tailor sensors to the specific security needs as can be fence intrusion detectors.

Wireless sensors are becoming quite popular since they can be installed quickly and cheaply without drilling walls for routing wires. Their main drawbacks are that they are more expensive, consume more energy, have less life if battery powered, and are less reliable since they may be more subject to interferences than wired ones.

Sensors are an essential element of nearly all security systems based on surveillance. Their integration in an alarm monitoring system able to warn and display the alarm location is a major design issue in the development of a new security system. Once the alarm is reported in the monitoring centre appropriate measures can be taken such as sending a patrol to assess the threat and respond accordingly. The monitoring centre is based on computer systems and software that collect, store and present alarms. Its size ranges from small microprocessors with embedded software to large computer systems depending on the complexity of the asset to protect.

Sensors are usually available as commercial off-the-shelf (COTS) products with standard interfaces (e.g. IP protocol) being easily integrated into a wide range of security systems. Their production is today largely commoditised, especially for technology mature sensors. It cost tends to be outweighed in the final system price by other items such as system engineering and design, installation, system test and tuning.

They are sold worldwide by a large number of companies like Honeywell, GE, Siemens, Bosch, Cooper, or Tyco. Top 10 companies hold 50 per cent of the market (Frost & Sullivan, 2008a:78). Competition, technological progress and the shifting of manufacturing to Far East countries with low labour cost explain the falling prices for many sensors. They are mainly sold through distributors, value added resellers, system integrators and installers. Sometimes easy to install home or small business alarm kits are directly sold by manufacturers to end customers through 'Do It Yourself' stores or the internet (Frost & Sullivan, 2006a).

Border protection

Controls at border checkpoints and the surveillance of unregulated frontiers are good methods to restrict the freedom of movement of terrorism and organised crime as well as illegal immigration. Controls focus in quickly verifying the validity of credentials, authenticate the owner, and check that she or he has no pending claim from justice, as well as the inspection of personal belongings to verify that they do not contain any illegal material. The equipment to support these processes will be analysed in the next section. Here we will address the protection of unregulated borders against illegal entry that is becoming more vulnerable as control over regulated air, sea and land borders tightens. This suggests that demand of border protection equipment will keep growing in the near future[90].

The protection of the large perimeter of borders requires a different approach, since the sizeable physical space that must be protected makes the permanent surveillance along the perimeter too expensive and inefficient; especially having in mind that natural

[90] The US SBInet and the European EUROSUR project may be a clear demonstration of this hypothesis.

obstacles –such as rivers, mountains, or seas– limit the illegal entry of persons and goods. Effective solutions consequently have always to accept some degree of permeability. They are based on stationary systems composed of a network of long range remotely operated all-weather sensors (such as radar, visual or infrared cameras) able to cover the perimeter to protect and complemented with patrolling units. Sensors provide initial targeting information to patrol units that use it to locate and apprehend intruders such as immigrants attempting to reach a landing beach with a small boat.

Patrolling can be made using land and sea vehicles endowed with the appropriate surveillance equipment. However, the wider coverage of sensors from air gives advantage to platforms such as helicopters and fixed wing aircrafts on certain missions, despite of being a more expensive surveillance method.

Products sold in this market are composed of surveillance equipment (fixed or mobile) – based on electromagnetic screening or optronics–, and command centres able to plan and coordinate the collection, analysis, fusion, correlation, and dissemination information involved in border protection. The close relationship with the equipment provided by the defence industry makes that equipment suppliers come mainly from this economic sector. The whole system is supplied by a single prime contractor or system integrator such as EADS, Thales or BAE Systems with the support of defence electronics industry for the supply of the surveillance equipment. Government is the single purchaser of this kind of systems.

Vehicles are provided by the automotive, maritime or aerospace industry. These vehicles require the tailoring and the integration of specific equipment for radio communications and surveillance. Land vehicles are basically all-terrain cars mainly supplied by the automotive industry. Coastal patrols boats are less complex vehicles than military surface ships since they do not need a sophisticated weapon system and other advanced features. Europe has a large shipyard industry able to provide these ships, yet this industry is characterised by small firms, excess capacity and lack of collaborative programmes (Ecorys, 2010:243). The industry is subject to strong competition from Asian countries like Korea or China. Europe has also a well developed aerospace industry able to supply fixed or rotary wing aircrafts as for example BAE, Dassault, or Aerospatiale as well as their main components. This industry characterises by high levels of R&D investments, where high cost and high risk programmes experience long development and pay-back cycles and a high value output, which is manufactured in low volumes (Jackson, 2004).

Unmanned air vehicles (UAV)[91] fitted with video-cameras and imaging radars offer potential advantages since they do not need pilots. Its development is mainly driven by military needs, but civilian applications such as border protection are becoming a potential market for these vehicles. Yet the consolidation of the civilian market confronts with relevant problems not easy to solve such as a life cycle cost that needs to be smaller than manned aircrafts, improved reliability (currently they have a higher number of accidents that manned vehicles), the updating of civil air space regulation to integrate them with ATM systems[92], adequate airworthiness regulation that allow their

[91] Instrumented Zeppelin and aerostatic balloons are other alternatives subject also to research. Another area of intense research is unmanned land vehicles.

[92] This task is being performed by EUROCAE WG-73. The EDA is also contributing and the Steering Board of May 2007 agreed to propose a strategic roadmap for the integration of UAV into the non-

insurance (EC/785/2004 regulation) and the allocation of enough bandwidth in the overcrowded radiofrequency spectrum for the payload data-links (EU, 2007). Therefore, the unmanned aircraft market, although being very promising, is probably still years ahead. The market is led by USA and Israel companies, who in certain cases have partnered with European companies for joint developments. Main European companies working in this field are Sagem, EADS, Dassault Aviation, EMT, Meteor, Alenia Aeronautica and Saab (Frost & Sullivan, 2005).

Maritime surveillance

Maritime surveillance is required to safeguard sea borders, but it is also needed for becoming aware of activities at sea impacting on: maritime safety and security, the maritime environment, fisheries, trade and economic interests of the European Union as well as general law enforcement and defence. Such varied goals make that diverse users and operators are involved in this activity such as port and ship owners / operators, port authorities, customs officials and the coast guard.

The nature of threats in the maritime domain frequently encompasses a trans-national and a trans-sectoral approach. This explains the active role of different European Union agencies such as EMSA, CFCA, FRONTEX or EDA in supporting the development of maritime surveillance systems at European and Member States level. As has been mentioned in chapter III, a key aspect for success in these developments are agreements on standards, interconnections, non-technical processes and procedures that enable information sharing on the basis of established access rights.

Surveillance is mainly performed through the monitoring of vessel traffic based on an automatic identification system (AIS), a ship borne VHF radio that broadcasts to similar transponders and shore-based facilities information regarding the ship's identity, position, heading, speed and destination allowing the tracking of these vessels when they are operating in coastal areas, inland waterways, and ports. The system requires for operating a satellite tracking equipment named Ship Security Alert System (SSAS). The AIS system is mandatory in all vessels involved in international voyaging with gross tonnage above 300 tons and all passenger ships according to the 2002 International Ship and Port facility Security (ISPS) code. Its main purpose is to avoid vessel collision, but it can be used as well to survey sea lanes. Non-cooperative vessel detection requires radar equipment and other sensors to locate and identify them.

As of January 1, 2009, according to the International Convention for the Safety of Life at Sea (SOLAS), all passengers ships, high-speed craft, mobile offshore drilling units and cargo ships of 300 gross tonnage and upwards regulated by IMO must be tracked with a Long-Range Identification and Tracking System (LRIT). According to SOLAS regulation, the contracting governments must implement national LRIT data centres, to which ships will report their position four times a day. Such data is transmitted through a satellite link. Such system is to some extent complementary to AIS. Both may help to track vessels worldwide.

---

segregated European airspace by 2015. An essential component is the development of a light Mid-air Collision Avoidance System (MIDCAS) based on a *sense and avoid* technology. If the cost of these subsystems is too high, it may render UAVs too expensive.

Ecorys (2009) estimates the revenues of both equipment markets in the range between €10-20 million for AIS and €55-80 million for LRIT. The world market of these equipments is led by US and European companies. The EU has financed research projects in this area like Marnis[93]. Thrane & Thrane (DK) is one of the leading players. The market for Mobile Satellite Services, required for communicating LRIT data, is mainly dominated by Inmarsat (UK), however new players have entered the market like Iridium (USA), Global Star (USA), Thuraya (UAE) and Orbcomm (USA).

A maritime surveillance system requires in addition sensors, communications, air/sea patrol vehicles and command centres. These large systems are mainly supplied by integrators such as Thales, Konsberg, EADS, or BAE Systems . This area is subject also to research like for example the EU projects Autonomous Maritime Surveillance System (AMASS) and Security System for maritime Infrastructures, Ports and Coastal Zones (SECTRONIC).

Air surveillance

The detection of border intrusion across air is usually managed by defence forces. However, the detection and management of renegade aircrafts alerts is an area that requires civil-military cooperation across the European Union as is the case of NATO and Eurocontrol. An information dissemination system that collects and distributes information between the main stakeholders involved in the response may help to better manage an air incident such as hijacking. Information will proceed from the air defence infrastructure, the air traffic control infrastructure, standard transponders installed on the aircraft as well as other data sources. This is a market where only technology demonstrators have been developed like the European Regional Renegade Information Dissemination System (ERRIDS).

Identity and access control management systems

Personal identification is a key aspect of security. It allows to recognise a person and verify its right to perform a certain activity such as crossing a border; accessing a building or facility; accessing a computer system, mobile phone or PDA; make an economic transaction (e.g. credit card payment), or receiving services. Identification also allows to check whether a person is being sued by justice. Effective identification systems can improve security raising the burden associated to terrorism and criminal activities.

The identification is based upon: (a) something one has such as documents, cards, tokens whose ownership demonstrates the identity; (b) something one knows such as a pass-code; or (c) something one is based on the comparison of personal biometric features. These methods can be combined to increase the reliability of the identification process.

Identity theft is a main risk in security because it may wrongly identify a person allowing him unauthorised and potential harmful actions. There are different theft methods. Cards and tokens may be counterfeited though watermarks, ultraviolet fluorescence, microtext, microdots, holograms and other techniques may hinder the

[93] See for details http://www.marnis.org.

process[94]. Passwords can be stolen. Personal biometric features are more difficult to steal, although an improper enrolment process may allow it.

For analysis purposes, this area can be divided in three different market segments:

- Mechanical lock, entryphones and key pads
- Card systems
- Biometric systems

Mechanical locks, entryphones and key pads

Mechanical locks and bolts are the simpler access method. They need a key or token to permit the access. They are at the low end of the access control market, yet they are the most common access method. Audio and video entry-phones are also low cost solutions to authorise access in the residential market. Identification and authorisation is made personally by the operator through the phone line, which may include also a video image.

Another access method is through a key pad (usually alphanumeric) with processing electronics designed to activate an electric strike when some keys are pressed in a predetermined order, either sequentially or simultaneously. Sophisticated keypads can log each time a pass-code is entered to record both successful and unsuccessful access attempts, and a duress function where a person being threatened can activate a silent alarm to summon assistance.

These technologies are mature, simple and relatively inexpensive. They are appropriate to solve unsophisticated needs such as a single door access for any kind of customer. There is a large list of companies that produce this equipment. Assa Abloy followed by Simons and Voss are two large players in the European market. Distributors, retailers and installers provide them to the end customer. Frost & Sullivan (2008) estimated the size of the European electronic keypad market for the year 2006 around €64.1 million.

Card systems

Access based on personal credentials requires that a surveyor compares data stored in the credential (normally a facial image but also a fingerprint) to identify and authenticate the person. Afterwards the consultation to an authorisation list will determine if such a person has access rights. Information and communication technologies can help to automate the process and reduce resources and time spent for in this process.

The simpler system use cards to store a code that identifies the owner[95]. The user passes the card on a reader which transfers the data to a computer which authorises the access

[94] Powerful personal computers, scanners, photo editing software, and printers now allows terrorist and criminal groups to produce authentic-looking forged documents and identity photos almost anywhere. Most documents and images produced in this fashion will usually not withstand a detailed forensic analysis, but they may be good enough to withstand cursory inspection by an undertrained or hurried clerk, security guard, or police officer (Don *et al.*, 2007).

[95] These cards, however, do not necessarily verify a person. They only confirm that the owner has a valid card. This creates vulnerability when the card is used by unauthorized persons because the card

after consulting a database. The time and the control point is usually logged for auditing purposes. These systems range from a single gate to a networked solution covering a whole building or a group of buildings.
Complementary hardware of access control systems is the door lock or barrier that is unlocked when access is authorised. There are many kinds of barriers. They can range from such conspicuous physical structures as revolving doors to all but transparent optical turnstiles with higher throughput able to warn of unauthorised attempts to pass.

There are many methods to store information about the card owner that are readable by a computer. While bar codes can be used, the most common method is a magnetic strip, which is widely used in the finance sector in the form of credit and debit cards. These cards are a very mature technology in the edge of obsolescence due to their limitations in data storage and processing. They are being substituted by more sophisticated solutions being the most common those known as smart cards that contain on a chip a small microprocessor with a memory. Such cards are more flexible to changing needs, their data can be encrypted and they are less prone to fraud. They can store biometric information such as face and fingerprint, and a digital signature that enables the signing of electronic documents and financial transactions.

Smart cards are replacing magnetic strip cards in the financial sector for ATM and POS terminals. They use a world standard named EMV promoted by the industry which has allowed the change to a more secure payment system. In the EU region merchants are now liable, as from 1 January 2005, from any fraud that results from transactions on systems that are not EMV capable. This standard, however, does not implement biometric identification.

Proximity cards are based on radiofrequency (RFID) technology. The card reader constantly transmits a low-level fixed RF-signal that provides energy to the card. When the card is held at a certain distance from the reader, the RF signal is picked up by the card's embedded antenna and absorbed by a small coil inside the card that powers the card's microchip. Once powered the card is able to exchange information with the reader. The main advantage is that being contactless the owner is not required to '*do anything*' to gain access. Smart and proximity cards and their readers are more expensive than magnetic strip cards, however their advantages largely surpass the cost difference. In some cases, for keeping compatibility with various systems, a card uses more that one of the abovementioned methods.

According to Frost & Sullivan (2008) the manufacturers of the different elements of an access control systems such as cards, readers, doorlocks and barriers supply them to distributors (55-60%), installers (25-30%) and valued added resellers / system integrators (15-20%). Top market companies are Honeywell, Siemens, Interflex (Ingersoll-Rand), Gunnebo, Kaba, Assa Abloy and Bewator. Other relevant companies are Bosch, GE and Gemalto. According to Ecorys (2009:194) main vendors of smart cards are Gemalto, Sagem Orga, RSA and Oberthur. Giesecke and Devrient is another supplier. Infineon Technologies AG is a supplier of chip cards and security IC.

The desire of integrated solutions where a single card can be used for physical and logical access control, card readers can be connected to the IT infrastructure of the

has been stolen, lost, or counterfeited. Therefore, stand-alone card systems are not considered acceptable for high-level security applications.

company and integrated with the physical security system and other building management systems has opened the market to IT distributors and building technologies companies. The largest value of the system remains in the design, integration, and software development capabilities to make a 'turnkey' system based on readers, cards and other commoditised system components.

Access control systems are of widespread use when security needs are above average and manual methods are inefficient. The customers with such needs are many and include banks and financial services, hotels, industry, manufacturing, commercial retail distribution, transport, military and government.

Biometric systems

A biometric indicator is any biological (anatomical or physiological) or behavioural feature that can be measured and used for the purpose or automated or semi-automated recognition of human beings. Examples of physiological features are face, fingerprint, hand, iris, retina or palm veins. Examples of behavioural features are voice, signature or keystroke sequence. Some biometric features persist over time while others change. All biometric features are deemed *unique* but some are less *distinct* than others. Biometric techniques can be used in two ways: (a) to verify that people are who they claim to be, (b) to discover the identity of unknown people. The first method requires a one-to-one check, whereas the second requires one-to-many checks. Once the identity is confirmed, appropriate decisions can be taken.

Biometric systems are more secure than traditional recognition systems. As such they influence the level of *trust* in any activity that requires identification or verification of identity. In other words they can help to reduce fraud[96]. But they only represent a secure recognition process in that they provide a strong link between physical persons with their identity data. This means that the linking process must be highly reliable. This will depend on the secure operation of each of the four stages of the biometric identification process, namely enrolment, storage, acquisition and matching (IPTS, 2005:12).

In a society that is increasingly mobile, flexible and digital, there is an increasing need of recognition systems. In practical terms, biometrics is mainly applied for four purposes: law enforcement, physical access control (including border control), logical access control to information systems and convenience. With more and more transactions such as e-banking, e-commerce, e-work, and e-government taking place on-line, biometrics offer a promising way of establishing secure identities especially when face-to-face transactions are not feasible (IPTS, 2005:35).

Main biometric technologies are anthropometry, software for template generation, pattern recognition and matching algorithms, and sensor devices to record the biometric features[97]. Fingerprint uses the unique uneven surface of ridges and valleys that form a

[96] As many other security solutions, the degree to which biometrics reduces theft and the possible displacement of fraud to other areas remains uncertain. Its impact on reducing the threat of terrorism could also be rather low (according to Davies and Hosein (2007:9) the UK government argues that a third of all terrorist use multiple identities). However, it is evident that this technology is inherently harder to spoof.

[97] Biometric systems first capture samples of the individual's features that are then averaged to create a digital representation, known as a template. The stored template is used to match the characteristic captured by the identity recognition device. The original biometric characteristics (e.g. fingerprint

unique pattern from each individual. Iris uses the coloured tissue of the human eye surrounding the pupil for recognition purposes based on a black and white infrared image. Retina biometrics is based on the analyses of the layer of blood located at the back of the eye. These three techniques are the most accurate. Yet, retina scanning is too intrusive and invasive as well as too expensive for wide diffusion. Face and iris technologies have the advantage that they operate in the two-meter range and need less cooperation from users. Hand biometrics compares the geometry of the hand such as width, length, thickness, and surface area to confirm an individual's identity. Its strength relies in its durability in extreme environmental conditions, high throughput, ease of use and non-invasive nature. The discrimination capability of hand geometry can be low for a large set of users. Facial recognition has also relevant restrictions[98].

Voice biometrics, also known as speaker verification, is based on the unique geometry of the speaker's vocal tract such as tract length, ratio of larynx to sinuses, resulting harmonics, pitch, and range. It is used when it is the only available biometric recognition method such as telephony and call centres. The effect of ambient noise on accuracy, the fact that voices are not clearly unique, the likely changes over the lifespan of a user (or its temporal change due to a throat illness) and the perceived ease of falsification make this choice less valuable.

Signature recognition measures the dynamics of signature strokes such as speed, acceleration, timing, pressure and direction. It compares not merely what the signature looks like, but also how it is signed. Since the individual signature may vary from sample to sample, the recognition process may have non-ideal performance. Moreover, since a proficient *forger* is quite capable of selectively provoking false accept verifications these systems are less secure. Multi-modal biometry combines less reliable technologies in sequence to strengthen the overall performance, or in parallel to increase flexibility by providing alternative modes for the identification or verification process. The expensiveness of these solutions, however, limits its general use.

Government applications on biometrics focus on automatic fingerprint identification systems (AFIS) for law enforcement as well as to identity verification in passports,

---

image) cannot be recovered from the template. Because the reference template is generated from multiple samples at enrolment, the match is never perfect. Therefore, systems are configured to verify the identity if the match exceeds an acceptable threshold. Consequently, all biometric technologies suffer false rejection and false acceptance rates that vary accordingly to each technology. Normally, lowering the false acceptance rate increases the false rejection rate, i.e. the chance that an authorised person will be denied access. Whereas authentication performs one-to-one match against user credentials to verify identity (usually stored in a smart card), systems that have to consult a central database of templates to identify one individual against a predefined population take longer –the bigger the database, the slower is the search– and are less accurate. Moisture, dirt, grime, or light conditions may also influence the performance of biometrics in fingerprint, face and hand recognition (GAO, 2002).

98 Facial recognition is relatively inaccurate due to the presence of a lot of variability. This variability is due to changes that occur to people over time like ageing, or is simply due to external environmental conditions such as poses, facial expressions, hair, or usage of glasses. Its reliability is also related to recording conditions and the context of applications (static images or video, image quality, with or without uniform background, or lightning conditions). 2D face recognition is the most common by far and the one proposed for passports and visas. Face recognition is not yet ready for outdoor use, and it is unsuitable for a database with a large watch-list. Even for moderately-sized lists it has mediocre performance (IPTS, 2005:48). A short description of main algorithms (principal components analysis, linear discriminant analysis and elastic bunch graph matching) for facial recognition can be found in NTSC (2006) report.

visas[99], personal identity cards[100], driver's license, or e-government services like tax payment, vote, social security or unemployment.[101]. According to Acuity (2009:21) the US-VISIT, the similar Japanese programme and the EU e-passport visa and passport programmes are the largest public procurement contracts in this field. The International Biometric Group estimates that 75% of the market addresses public administration in 2009, a figure that does not seem to fall largely in the next years (Ecorys, 2009: 191). European member states like Italy, France, Belgium and Spain are implementing the new national identity card based on smart cards that store face and fingerprint biometric information. Germany is expected to move to smart cards in 2010. Unfortunately, no agreement has been reached within members states on a standard identity card.

According to Acuity (2009), fingerprint and the AFIS / Livescan systems used by law enforcement for background checks and criminal investigations accounts for the largest market share. The other relevant markets are face and iris recognition, the market of remaining technologies is comparatively small. Frost & Sullivan (2008c) reports that Sagem Securité was the AFIS market leader in 2007 followed by Cogent, Inc., NEC advanced Security Solutions and Motorola's Biometrics Business Unit.

The use of biometric in borders and transport is evolving at a slow pace. There have been many pilot projects, but a wide diffusion is this technology is still pending. For example, iris recognition has been used for frequent travellers in Amsterdam Schiphol (Privium Programme), Frankfurt International Airport, London Heathrow, London Gatwick, Manchester, Birmingham and several Canadian airports as part of the Nexus programme[102]. Fingerprint identification pilots have been attempted in Charles de Gaulle Airport (project PEGASE) and Heathrow (miSense in 2006/2007). New pilots projects in France (project PARAFES) and Spain (ABC System) were launched in 2009 and 2010. The main advantage of such systems is the short-time (around 10 seconds) needed for automatic recognition and the corresponding reduction in waiting time[103].

Biometric is also applied in highly reliable electronic access control as for example the Paris Airport Authority based on fingerprint and contactless smart cards, the four months pilot project implemented in the Fiumicino Airport in 2003 using facial

---

99 Regulation 2252 / 2004 sets the standards for security features and biometrics in passports and travel documents issued by EU Member States. This means that since August 2006, all passport delivered in Europe contain a wireless smartcard storing a digital image of the holder's face compatible with ICAO standards. Since June 28, 2009, second generation of biometric passports integrate also fingerprints. The European Visa Information System VIS and its biometric engine the Biometric Matching System should start operation in 2009 and be fully operational in 2012 (Ecorys, 2009:209). This is a joint development of Accenture and Sagem. The system will be able to store 70 million datasets.

100 According to Acuity (2009:v) Mexico and India have announced plans to issue biometrically enabled national identity cards.

101 Other envisaged areas are the use of biometrics to access electronic health records for the protection of privacy regulated by the Health Insurance Portability and Accountability Act (HIPAA) in the United States <(F&S, N55F)>; and passenger processing based on biometrics. The latter will help to reduce the space consuming check–in kiosks and their related staff creating a more self-service orientated environment, while still maintaining proper security levels. For more details, see Frost & Sullivan (2005:3-16).

102 The system is known as Iris Recognition Identification System (IRIS) and has been developed by the UK Border Agency. Details can be found in www.iris.gov.uk.

103 Apart from fewer personnel for identification, quick passenger checking may pay for itself helping for example to increase the time spent buying in airport duty-free shops.

verification with the template stored in a smart card and rendered secure through a digital signature[104].

Applications related to logical access control are mainly based on finger-scan authentication solutions in mobile phones, PDA's, cars, wireless computing devices, IT systems access, physical access control systems and portable web tablets. Companies like Siemens, Nokia, Fujitsu, NEC, Sony and others have developed such systems. Anyhow, these solutions are not experiencing a widespread use in the market.

Biometric systems are composed of computer systems, secure communication networks, characterization / comparison software (biometric engine), data encryption algorithms, secure data stores and biometric data capturing devices. They are supplied by system integrators and large software houses –such as IBM, EDS, Lockheed Martin, Northrop Grumman, Accenture, or Unisys– in alliance with the suppliers of these components. European companies involved in the supply chain of these systems are Dermalog Identification Systems GmbH, Greenbit S.p.A., Daon (USA but Irish origin), and Automatic Systems (Belgium), Precise Biometrics AB, UPEK (a USA company spin off of ST Microelectronics) according to (Ecorys, 2004:196). Another company is Fingerprint Cards AB.

L-1 Identity Solutions is the market leader in face recognition. Such leadership has been achieved through the purchase of Viisage Technology, Identix, Inc., and A4 Vision (early acquired by Bioscript in 2007). Two important EU companies are Cognitec Systems GmbH and Ommiperception (UK).

Iridian Technologies (now L-1 Identity solutions) was the unique provider of iris recognition technology until the patent fell into public domain in 2005. The company has licensed its technology to several partners for the development of hardware and camera platforms for various applications and environments such as LG Electronics, Oki, Panasonic, Sagem, IrisGuard (UK), Sarnoff, IRIS, Privium (NL), CHILD Project, CanPass, Clear (RT – Registered Traveller), IBM and EyeTicket Corporation.

Retica Systems is the major participant in the retina biometric market. Hitachi, Bionics and Fujitsu (European partner TDSi) are the main suppliers of palm vein scanners, a technology that does not need to physically touch the sensor, a solution mostly preferred in Japan (Frost & Sullivan, 2009).

It is expected that government investment gives way in the future to a wider use of biometrics in commercial and civilian applications due to the falling price of smart cards, readers and software[105]. However, government support has so far been unable to solve current shortfalls and problems that impede the widespread use of this technology such as: (a) total cost of ownership that makes it unsuitable for low demanding identity verification; (b) performance constraints on recognition with a low false alarm rate and quick response in access points with a large people throughput[106]; (c) customer

[104] See U.S. Commercial Service (2005) Italy: Biometric Identification Devices Running Applications and Future Opportunities in the Italian Market.

[105] The EU Research Framework Program has been especially active in financing biometric programs (Hayes, 2009:47).

[106] Some personal disabilities, diseases of illnesses (e.g. finger amputation) may compromise the use of biometrics. These cases require the use of manual procedures to tackle the identification problem.

acceptance; (d) interoperability and lack of widely accepted standards in sensors, templates, and Application Program Interfaces (API)[107]; (e) expensive procedures to manage biometric information since being personal it is subject to data protection rules, (f) the large substitution costs of current systems and procedures in use, and (g) the difficulty to objectively estimate the advantages of higher reliability that blurs the potential benefit (too small) compared with the associated substitution costs. These reasons may explain the slow pace of this technology and the small revenues of the European biometric market estimated by Ecorys (2009:191) in €708.4 million for the whole European industry, whereas Frost & Sullivan (2008:30) estimates the access control biometric market in only €23.8 million for 2009. They also explain the setbacks suffered by widely heralded biometrics programs such as the US-VISIT Exit program (two failed pilots), the scaling back of the US Transportation Worker Identification Credentials (TWIC™)[108], the transformation of the UK National ID card to an opt-in, and the commercial implosions of Pay-by-Touch in November 2007 and CLEAR Registered Traveller projects in June 2009 (Acuity, 2009).

The slow maturation of the market is causing considerable changes in the market structure with frequent mergers and takeovers. Some examples are the agreement between Cross Match technologies and Smith Heimann Biometrics GmbH in 2005; the creation in 2006 of L-1 Identity Solutions merging Viisage, Identix, and Iridian Technologies, followed by the takeover in 2008 of Bioscript and Digimarc; the purchase by Sagem of Motorola biometric business unit in 2009[109]; the purchase in 2009 of Atrua Technologies by AuthenTec, or the takeover of L-1 by Sagem Morpho in 2010.

Land vehicles surveillance

Control of vehicles is based in Automatic Number Plate Recognition (ANPR) systems able to optically recognize the characters of the vehicle plate on an image captured by a camera. The technology was developed at the end of the 70s and now is a standard, reliable and widely diffused product as can be seen in the access control of many car parking areas. This information may be linked for example to a law enforcement database to check if the vehicle is stolen, or owned by a suspicious person. But also for checking if the vehicle is not insured or it has not paid a congestion fee. These systems can be installed on a patrol car. This capability can be used also to identify containers. These systems are developed by industrial control or software firms. The United Kingdom is a big customer of these systems.

Screening of personnel and their belongings

Screening is necessary to verify that persons do not hide any dangerous, illegal or hazardous material –such as weapons, explosives or drugs– below clothes or within their personal belongings that may be used for terror or criminal purposes. Manual screening methods tend to be slow, invasive, and labour intensive. Detection equipment may improve these shortfalls leaving costly manual search to solve inconclusive

[107] See for example the Windows Biometric Framework and the standards developed by the bioAPI Consortium. Interoperable standards are a prerequisite to the wide diffusion of biometrics in large commercial applications such as bank ATM.

[108] This program focuses on longshoremen, truck drivers, port employees and others requiring unescorted access to secure areas of ports.

[109] This unit was acquired in 2000 from Printak, the first provider of AFIS systems.

inspections. Standoff detection, out of the range of offensive weapons like an explosive, is other desired feature, however, technology is still immature to meet this goal and the person or their belongings shall be in close contact with the equipment to be effective[110].

Metal detectors are very effective to identify firearms and knives. They can be walk-through portals that may include light bars to highlight the locations where the highest metal concentration is detected, or hand-held detectors to explore the body when the first system gives a warning. The equipment generates an electromagnetic field that causes metallic (or other electrically conductive) objects in the proximity to produce their own distinct magnetic fields altering the initial field that is sensed by a detector. This is a very mature technology that accurately detects the presence of most types of weapons with a portal throughput of 15-25 people per minute. Cooperative individuals can typically be scanned with a handheld detector in about 30 seconds. Companies like Smith Detection, CEIA, Rapiscan, L3 and GE Security are the main market suppliers in Europe.

Equipment to quickly identify illicit material in bulk quantities is based on images generated by X-rays using single energy, dual energy[111], backscatter, or diffraction techniques; nuclear techniques involving neutron[112] or gamma ray bombardment, or millimetre and terahertz[113]electromagnetic waves. Some techniques, like millimetre waves and low power X-rays backscattering, can be used to safely see through clothing. Examples of these systems are AS&E BodySearch and the Rapiscan Secure 1000 (GAO, 1996 and Theisen *et al.*, 2004).

The scanning equipment does not identify the material for the operator. It only provides him or her with tools (usually images) to examine persons and their belongings. Its throughput depends on: the amount of clutter in a bag or on a person, and the operator efficiency. Clutter occurs where several dark items are grouped together creating a dense image. Operator efficiency is influenced by the monotony of the task, fatigue, time pressure, training level and working conditions. Best throughput today is not higher than thirteen bags per minute, seven passengers per minute, and one vehicle per minute (GAO, 2002). This slow performance and limited number of inspection points

[110] The EU 7th European Research Framework Programme Project Optix goal is stand-off detection at a distance of 20 meters.

[111] This is the most common method to screen luggage. A colour code two-dimensional image is created by comparing the relative transmission of high and low X-ray beams to highlight substance density and distinguish between metal and organic material (Theisen *et al.*, 2004:48).

[112] Neutron (three-dimensional) radiography, based on thermal or fast neutron activation, represents a promising technology. These systems use a source of neutrons to generate the emission of gamma-ray of the cargo. The signature obtained from scanning can be compared to a library of gamma-ray signatures to detect substances with high content of nitrogen and oxygen in most explosives, and the high chlorine content and high carbon to oxygen ratio in certain drugs (NRC,2002b:vi). Main limitations are depth of penetration and its ability to characterise certain explosives. Other practical limitations are large size and weight, long detection time for a small explosive quantity, the need for radiation shielding and regulatory and safety issues associated with nuclear based technologies (NRC, 2002b).

[113] Terahertz can be used to detect non-metallic weapons. This technology is still immature due to the lack of efficient and low / moderate cost sources and detectors (EPOSS, 2009). Smith Detection and Teraview have signed an agreement to develop detection equipment based on this technology. The project TERASEC has been financed by the PASR.

generate queues that prevent the use of screening equipment in high traffic places such as commuting rail stations.

Computer axial tomography provides the best capability for detecting and identifying materials due to its ability to see in three dimensions and measure object density with precision. Example of such equipment is GE CTX family of products or L-3 eXaminer 3DX 6000. While this equipment was limited initially to large international airports, they are widely used today in US Airports where around 1,500 units are deployed (Ecorys, 2009: footnote 136). According to Elias (2008: 33) bag screening equipment has shortfalls in its capability to screen air cargo due to object size, false alarm rate and throughput.

Nuclear quadrupole resonance (NQR) is a non-imaging technique that can be used for explosive detection. It is based on the analysis of the weak radiofrequency signal emitted by the nitrogen quadrupole nuclei present in the explosive when a pulsed radiofrequency field is applied to the suspicious object. However this technique is unable to detect liquid explosives[114]. Invision / Quantum Magnetics, today a subsidiary of GE Security supplies screeners based on this technology. Lack of product diffusion suggests that the technology is still immature[115].

The analysis of the residual traces of drugs and explosives deposited on the person or the carry-on luggage may indicate a recent contact with such substances. It uses separation and detection technologies to measure the properties of vapour or particulate matter collected by the equipment and compare it with the signature of drugs and explosives and signal an alarm if the probability of match exceeds a threshold. Some examples are colour change of test papers (chemical reagents), electron capture detection (ECD), field ion spectrometry (FIS), gas chromatography / chemical luminescence (GC/CL), gas chromatography / electron capture detection (GC/ECD), gas chromatography / ion mobility spectrometry (GC/IMS), gas chromatography / mass spectrometry (GC/MS), gas chromatography / surface acoustic wave (GC/SAW), ion mobility spectrometry (IMS), or Raman spectroscopy. Current technologies are capable of detecting most militarily and commercially available explosives and drugs. However, most systems are designed to detect only a subset (GAO, 2002:12). Ion mobility spectrometry is the most widespread technology (GAO, 1996). This kind of detectors is mainly used as a secondary screening method due to longer inspection time[116].

[114] According to Time, the 2006 transatlantic plot attempted to detonate non-nitrogen liquid explosives, namely acetone peroxide, that are undetectable by current systems forcing to increase control of liquids inside personal belongings. See http://www.time.com/time/nation/article/0,8599,1225453,00.html retrieved May 13, 2009.

[115] Details of this technique can be found in Fraissard, Jacques and Lapina, Olga (2009) Explosives Detection Using Magnetic and Nuclear Resonance Techniques.

[116] Attempting to reduce this time the USA has deployed 93 explosive detection portals in 36 airports in 2006 that have been supplied by GE Security with Entry Scan and Smith Detection Ionscan Sentinel II. The portal detects explosive particles using a small blast of air siphoned through a vacuum to laboratory equipment. See pages 3, 4 and footnote 11 of CRS (2007). In 2007, 17 portals where installed by GE in the Warsaw airport.

GE, L-3 Communications and Smiths Detection control approximately 90% of the screening market according to Frost & Sullivan (2005:4-12)[117]. Other companies are Rapiscan Systems, Bruker Daltonics, and Gilardoni (Ecorys, 2009: 113).

Main purchasers of these equipments are essentially transport organisations such as airports, airlines, freight forwarders, customs, railroad companies, private companies, and security services providers, which is sometimes responsible to purchase the equipment used to carry out their operations (Ecorys, 2009:96). Government organisations such as prisons, military installations, embassies, public offices as well as companies may use also screening systems in their facilities access points and mailrooms. Ecorys (2009:104) provides an estimate of the market size of around 100 units per year for air cargo screening that is probably the main purchaser.

Luggage and cargo screening equipment performance is subject to certification according to EU regulations. Equipment standards are set by the European Civil Aviation Conference.

Dogs can be used for detection since they can be trained to respond in specific ways to smells of narcotics and explosives. They have the advantage of being highly sensitive in comparison with artificial sniffers and less susceptible to masking interferents. Furthermore they are mobile and thereby able to follow a scent to its source. For said reasons they are ideally suited for drug or explosive detection that has a significant search component such as building, properties, vehicles or large containers. Main limitation is their duty cycle that requires a break after one hour of work. They are not usually used to screen people, since some people fear dogs and because a dog may bite someone. Labrador retriever is perhaps the most common. Other breeds used are golden retrievers, German shepherds, Brittany spaniels, German short-hair pointers and mixed breed. The cost to train a dog and a handler is about $17,000 and the annual operating cost of the team including the handler's salary, is about $60,000 (GAO, 1996). Police forces or guarding companies usually train dogs in-house and consequently this activity does not create a big market around it.

Goods and merchandise

The products in this market segment are aimed at two main goals. The first is the detection of illegal goods and merchandise such as weapons, drugs, nuclear materials, explosives, C/B agents, legal goods subject to duty or subject to import or export restrictions –e.g. antiquities, ivory, hard wood, or strategic products– and goods that fail to meet health and safety standards. The second goal is to safeguard the logistic supply chain from theft and loss of merchandise including shops and department stores. Because containers are the main transportation method of merchandise[118], many products in the market are oriented to assure the integrity of the container from the loading to the delivery point, and to facilitate the inspection process to quickly verify that the cargo manifest corresponds to the actual load. The first is the responsibility of

[117] These three large companies entered into this market through acquisitions. GE bought Invision in 2004, L-3 acquired Perkin Elmer's detection system in 2002 (Perkin Elmer had itself acquired Vivid Technologies in 1999), and Smith detection acquired Heimann Systems Gmbh in 2002 and Barringer Inc. in 2001. OSI acquired UK based Rapiscan Security Products Ltd. in 1993.

[118] According to Eurostat, the EU ports handled 69.8 million containers in 2009 (value measured in TEU, i,e. Twenty-foot Equivalent Unit).

the shipper who is the main beneficiary, whilst the second corresponds mainly to the government due to the negative social impact of smuggling.

The metallic structure of the container protects it from hole-cutting and the use of seals from unnoticed door opening, thus avoiding the introduction of illegal cargo. However, these measures are insufficient to assure container's integrity *en route* since they may be easily circumvented by criminals. Seals can be broken and rebuild, and the container can be cut by the side or the hinges for gaining access and later on wielded and painted (Van de Voort and O'Brian, 2003).

Advanced technology can help to solve these security shortfalls. The container's integrity can be monitored through an electronic sensor able to detect the opening of the door or inside movement and send out a signal to a control centre by means of a mobile communication line. The container may also incorporate a remote location tracking systems (RLTS) based on GPS. Because these systems are quite costly, only containers carrying high value loads can be protected through this way[119]. As we will see later the preservation of container integrity is still a technology under development.

Verification of container's load is a time consuming process involving four hours using 15 to 20 inspectors or three days for five agents (Martonosi *et al.*, 2005). Therefore, methods are needed to speed up the inspection process and avoid significant delays. The technologies used are similar to the screening methods user for personal belonging, but with higher energy due to the size and thickness of containers. The captured image is cross correlated with the cargo manifest to assure that what is seen is what it is expected and declared by the shipper. A container can be scanned is thirty seconds, but an operator may take up to 15 minutes to review the image (Martonosi *et al.*, 2005). Even being quicker, a rate above 30 containers per hour seems hard to achieve. The high cost of the screening equipment in the range of several million $ (Theisen *et al.*, 2004:66 and Elias, 2008:34), the time required to scan, and the relatively high false positive rate that results from the inconclusive visualization are the main restraints for a wide diffusion of this equipment. Notwithstanding, they are very profitable since they generate a large income due to the imposition of fines and taxes in detected contraband (Van de Voort and O'Brian, 2003).

Examples of X-ray equipment include CX 3800M from L-3 Communications and, the Silhouette Scan CAB 2000 from Smiths Detection. A system based on Gamma-ray is the VACIS imaging system of SAIC. Systems based on Thermal Neutron and Pulsed Fast Neutron Analysis were manufactured by Ancore Corp., a US company bought by OSI Systems Inc. in 2002 and later on integrated in Rapiscan Systems. Equipment for the detection of nuclear material is described in the CBRN early warning section.

Computers can facilitate the tracking of containers and the electronic exchange of cargo manifest and thereby the inspection process. For example, SAIC provides with VACIS a system called Integrated Container Information System-ICIS to automate the process. However, such systems require for widespread success the establishment of standards for information exchange. The United States Customs and Border Protection (CBP) is strongly investing ($1.7 billion) since 2001 in the development the Automated

[119] For more details see Van de Voort (2003). See also the research made by the FP 6 EURITRACK project that includes a non-intrusive method, named Tagged Neutron Identification System (TINS), to identify the chemical composition of suspicious material detected by X-rays inside the container.

Commercial Environment (ACE), a system able to manage an electronic truck manifest (e-manifest) that facilitates the border processing of cargo. It is reported that the new system processes 30,000 trucks a day (DHS, 2009:26).

The limitations of inspection methods means that 100% inspection is still a hard goal to attain[120]. Known Shipper Programmes are aimed to qualify shippers that follow good practices in order to assess risk better and perform inspection only when the consignor or shipper is not qualified. Profiling, a method to identify potentially suspicious merchandise based on risk analysis and intelligence information, may be used to avoid inefficient random inspection. Automatic profiling can be quickly performed using information systems and the electronic transmission of container data[121]. Yet, this method has limitations as we will see later on.

Tagging systems

One way to protect goods and merchandise against loss and theft is the attachment of coded tags that can be read and processed by computer system helping to identify and monitor efficiently the corresponding object. Optical character recognition (OCR)[122] and bar codes may be used for this purpose. However, the advantages of electronic tags based on radiofrequency make them the preferred method due to their flexibility and performance[123].

Radiofrequency identification (RFID), often referred as the internet of things, embraces a set of emerging technologies in widespread usage, with progressive application in various economical and societal domains such as security, supply chain management, and assets tracking[124]. RFID may be used to identify and collect attributes about a certain object or person, including its location and environmental information when integrated with sensors. This provides enhanced visibility and as a consequence better predictability[125]. The technology helps to: (a) reduce inventories and lead-time variances; (b) prevent the loss of merchandise; due to mishandling, theft and counterfeiting, (c) spare resources for control including labour and as a consequence raise productivity.

---

[120] There is a mandate in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) that requires 100% screening of all cargo placed on passenger aircraft by August 2010, with an interim requirement of screening 50% of such cargo by February 2009. The Security and Accountability for Every (SAFE) Port Act also requires that 100% U.S.-bound cargo containers be scanned using non–intrusive imaging equipment and radiation detection equipment at foreign seaports as soon as feasible. On the difficulties to implement such measures see GAO (2008).

[121] The European Commission's Joint Research Centre has, in cooperation with the European Antifraud Office (OLAF), developed a software tool named Contraffic, which is able to perform a risk analysis on the likeliness that a container is transporting illicit material. U.S. Customs uses a similar system called the Automated Targeting System since 1999 (GAO, 2010a).

[122] It can be used to read ISO-codes of containers, truck / lorry license plates, and railway wagon codes.

[123] Such as automatic identification independent of position and direction of object and without requiring line of sight and a short distance (few inches), simultaneous reads of numerous tags (50 per second), low error rate, better protection in harsh environment, long lifetime in re-use applications, and additional functionality such as read/write capability, and integration with other sensors.

[124] Other applications are their use for access control in highways (toll collection), public transport, stadiums, or private vehicles (keyless entry).

[125] RFID can be used to control perishable goods like temperature compliance of pharmaceuticals between thresholds during transport.

The main components of a RFID system are the tag or transponder, the reader or transceiver, and the middleware. The tag is composed of an antenna, a wireless transducer and encapsulating material. Active tags have a rewritable memory that can be used to temporarily store data and transfer it when required to a reader. They usually have batteries and may be connected to sensors (e.g. temperature, intrusion, location). Passive tags carry a unique set of data. They have a longer life span and are lighter, smaller, and cheaper. Readers consist of an antenna, a radiofrequency module, a control unit, a coupling element to interrogate electronic tags via radiofrequency and an interface to convey the collected data to the processing system. The middleware is the software required to link readers with the applications (EC, 2008:22).

Active RFID[126] tags can be combined with other technologies to create intelligent containers able to guarantee their integrity[127]. Prototypes and pilot projects have been initiated as for example the Smart and Secure Tradelanes Initiative in 2002. The project was started by three of the world's largest port operators, Hutchison Port Holdings (HPH), P&O Ports, and PSA Corporation. These corporations manage over 70% of the world's containers at their port facilities. Savi Technology, a company acquired in 2006 by Lockheed Martin was the technology provider of the RFID tag named Sentinel. Yet, the initiative failed[128]. According to GAO (2010a) the DHS has financed since 2004 developments in container protection and tracking such as the Advanced Container Security Device (ACSD), the Container Security Device (CSD) and the Marine Asset Tag Tracking System (MATTS) with uneven success. According to Ecorys (2009:144) companies and products under development are Savi Networks and SaviTrack product, Motorola / IAS Container Visibility System, SPC Global Track (USA) Container Monitoring Unit (CMU) and European Datacomm (EDC). The JRC has also developed also a prototype called the Remote Monitoring System (RMS).

RFID can be used for baggage tracking. According to AeroAssist (2008), some airports have made attempts to introduce this tracking method. They include pilot programs in Amsterdam Schiphol, London Heathrow, Paris Charles de Gaulle, Osaka Kansai Int. Airport and Hong Kong Int. Airport, McCarran Airport (Los Angeles) and other US airports. These pilot projects, however, are not experiencing a wide diffusion. This may suggest that this technology is not always cost-effective for luggage tracking (IATA, 2008). Hence, it may well be that bar-code technology still remains as the dominant baggage tracking technology at airports for many years.

Electronic Article Surveillance (EAS) actually is mainly based on magnetic tags, a simpler technology than RFID. Articles attached with such tag raise an alarm if they are not retired or deactivated before leaving the shopping centre. This market is dominated worldwide by two large manufacturers Sensormatic – Tyco, and Checkpoint Systems, Inc. Big box retailers are the main purchasers of these equipment. Low-cost passive RFID tags are also been successfully applied for article surveillance, because this technology is also able to trace articles and avoid counterfeiting (the tag becoming an

[126] Since RFID use radio and their signal can be eavesdropped, encryption is required for certain applications. Adding such feature increases final product price (OECD, 2003). Stolen RFID tags may be used for false identification.

[127] Active tags can monitor the status of the container (where it has been, and how and by whom it has been handled, and other environmental conditions) and transmit this information over long distances. They may also store the manifest of cargo.

[128] According to Elias (2008:31) cost of electronic reusable seals is about $2,500.

authentication mark of the good) reducing in such a way the losses from the manufacturing facility to the store. The massive deployment of this technology started in 2005 when Wal-Mart Stores, the world's largest retailer, required some of its largest suppliers to use RFID technologies (Frost & Sullivan, 2005:5-8). Main European retailers such as Marks & Spencer, Metro Group, Tesco or Carrefour have implemented or are evaluating this technology through pilot projects.

According to Frost & Sullivan (2006b:2-31) main passive tags producers are UPM Raflatac, Avery Dennyson, Sokymat, Texas Instruments and HID. Active tags include companies like Savi, Tagmaster or WaveTrend. RFID chips producers include Philips Semiconductors, Texas Instruments Radio Frequency Identification Systems (founded in 1991 and the market leader), ST Microelectronics and Infineon Technologies. Manufacturers of readers are Intermec Technologies Corp., Datamars SA and Checkpoint Systems Inc. according to Frost & Sullivan (2005:5-12). Middleware is provider by companies like IBM, Intel, or Sun Microsystems.

Prime contractors are large companies able to integrate tags, readers, computers, data networks and middleware with database system, application software and interfaces with other IT systems (e.g. ERP) to provide complete solutions. Examples of these companies are IBM, Raytheon, SAP, Microsoft or Savi Networks (Ecorys, 2009: 145). Other solution providers include Samsys, Sybase Inc, Scan Source, TCS, Alien Technology to name just a few .

As a conclusion, it can be said that the slow transition of pilots to widespread systems suggest a RFID security market still in its infancy. Revenues estimates were only achieved from Frost & Sullivan (2007a:4-8) that measured world revenues of container tracking devices market in only $183.5 million, a value that seems certainly low. Yet, according to EU (2008:6) the RFID market is growing fast (27% estimates for the period 2007-2009). The leading users are the transport (27%) and the retail sector (26%); this indicating a steeper trend in non-security markets. This is an area where research is intense due to the large expected size of the market[129]. However, important restraints to the development and widespread use of this technology remain. The first restraint is probably a fledgling, but not completely proven technology, still immature for certain applications where reductions in tag size and cost are needed in comparison with the inexpensive bar-code[130]. The reduced margins into which transport companies operate due to competition limit nowadays the application of this technology to high-value merchandise such as computers, microelectronic components, pharmaceuticals or weapons. The second may be due to the lack of stable standards[131] and regulations in a market where network effects are essential for success[132]. The third is the replacement cost of large legacy systems, based on less powerful but still effective technologies as the named bar codes. These conditions explain the prudence of customers to bet in this technology. According to Frost & Sullivan (2007a:5-5) we are probably still a decade behind conditions are met for a wide diffusion of this technology.

[129] See for example, EU Framework Research Program projects SToP (Stop Tampering of Products) and Bridge (Building Radio Frequency Identification solutions for the Global Environment). The latter program provides some estimated of expected growth and size of this market: 3.2 billion tags deployed in 2012 and 175.000 readers.

[130] Price today is in the range of 10-15 cents (EU, 2008:72). It is thought that price should be below 5 cents to be competitive <(F&S, D387:21)>.

[131] Present standards are too fragmented and valid up to 10 years horizon (EU, 2008:8).

[132] See (EU, 2007:136).

CBRN early warning equipment

Chemical, biological, radiological agents and nuclear weapons may be used by terrorist groups to meet their goals. Organised crime may be also involved, but being profits its main goal, it will be more focused on profitable smuggling or extortion schemes. CBRN attacks may entail massive response and recovery expenditures and may easily overwhelm available capabilities. Even if the number of casualties is modest, the emotional, psychological and economic impact of such action may be enormous as the 2001 anthrax attack in the US showed.

Preventive measures focus mainly in the protection, accounting and surveillance of materials, that can be used in an attack, throughout their life cycle, i.e.: creation, transportation, distribution, handling and disposal. Because these measures can be imperfectly implemented, equipment is needed to unveil illicit traffic quickly warning of the agent release in the case of the attack in order to accelerate the deployment of preventive measures and the distribution of life saving treatment with the aim of decreasing casualties, injuries, illnesses and contamination.

Many of the technologies and products in this market segment are applicable to defence. In fact most of them were originally developed for defence needs and still defence largely funds research in this area. Basic research is made sometimes in government owned facilities and often in conjunction with the private sector. In particular, government support is needed to access agents and secure testing facilities such as BSL-3 and BSL-4 laboratories (Knobler *et al.*, 2002: 10).

The chance of a CBRN attack has been a matter subject to intense analysis. See for example Rapoport (1999), GAO (1999), Jackson (2001), Ackerman and Moran (2006), Meade and Molander (2006), Enders and Sandler (2006:250) and Rossof and Von Winterfeldt (2007) to name a few. A general agreement exists in that the hurdles to obtain and use these weapons in an effective way are significant and that the likelihood of an attack is smaller than popular literature claims. A confirmation of this hypothesis is the short number of incidents –the subway sarin attack in Tokyo in 1996 by Aum Shinrikyo[133] and the unidentified anthrax attack in USA in 2001– and the short number of fatalities.

The technological difficulties and barriers to unfold an effective weapon of mass destruction (WMD) –where funding could not be the biggest[134]– cannot be dismissed. To fix these problems a terrorist group will have to amass considerable organisational capabilities, financial and logistic resources, knowledge, materials and technological skills. While a crude weapon could be made with less sophistication, it would be less likely to cause mass casualties.

Examples of technical difficulties are many. Some virulent biological agents and precursor chemicals are difficult to obtain, and others are difficult to process or produce, especially in the quantities needed for mass casualties. The handling of these

[133] Aum Shinrikyo endeavour was supported by an extensive scientific staff and nearly a billion dollars in assets (Rapoport, 1999).

[134] According to Ackerman and Moran (2006) a few hundred thousand dollars is the amount needed to develop a biological weapon.

materials requires specific equipment to avoid contamination that is not easy to pass inadvertently. A failure to follow safety rules in the use of highly toxic or virulent agent may cause an accident, hurting group members and raising the chance of being detected, putting in danger the whole organisation. These groups need to test their weapons to assess their effectiveness: a challenging task when they are trying to conceal their operations. Furthermore, it is not a trivial matter to disseminate and disperse efficiently biological and some chemical agents across large populations (NRC, 2002:67) and because of their sensitivity to weather conditions, these weapons also have significant risk of simply failing; this unpredictability could be a very significant barrier based on the psychological characteristics of a given group[135]. Initiation of a multi-month to several-year research program to perfect a chemical weapon is incompatible with a group which may disintegrate unless it begins its operations immediately (Jackson, 2001:35).

Organisational problems are not smaller. Enders and Sandler (2006:250), for example, state that Al-Qaida's decentralized structure protected it during the post-9/11 attacks, but at a price of not being able to develop CBRN weapons. In the same sense, Jenkins (2006) states that major operations require cooperation, coordination and structure, which in turn require a basis for trust that is difficult to establish on a decentralized structure and a communication network like the internet. Religious groups which tend to isolate themselves from the world will hardly adopt the technologies required to develop such weapons (Jackson, 2001:14).

The complexity of obtaining a nuclear weapon is analysed in detail by Mueller (2007). He concludes that the likelihood a terrorist group will come up with such weapon seems to be vanishing small. Daly *et al.* (2005) reports also the difficulties of Aum Shinrikyo to purchase a nuclear weapon in Russia in early 1990. The technical challenges dissuade it to build a nuclear weapon and devote its resources to acquire a chemical weapon. Al Qaeda attempts to acquire a nuclear capability was plagued also with problems and ultimately failed.

The basic restraints already commented represent the most likely explanation for the limited use of these weapons by terrorists organisations to develop and use CBRN weapons able to cause massive destruction and casualties. This rationale, that is expected to continue in the future, should be considered when analysing methods to cope with this threat.

Box 4. The chance of a CBRN attack

The main European supplier of CBRNE early warning equipment is Smith Detection (Ecorys, 2009:172). CBRN detection equipment is produced by Bruker Daltonics, a USA based company, in their facilities located in Germany. Environics Oy, a Finnish company, is also a producer of chemical detection equipment. ICx technologies is a USA based company with offices in Europe. Company size and revenues in this market are small (€32 million Bruker Daltonic according to Ecorys (2009:172)). Products are usually sold directly to the end customer.

Ecorys (2009:169) estimates the size of the world market of CBRN equipment between $2 and $5 billion of which 20% could correspond to EU demand.

[135] Of twelve attempts made by Aum Shinrikyo with chemical and biological agents, only one succeeded partially (13 deaths) and ultimately Aum itself was crushed (Rapoport, 1999).

Main purchasers of detection equipment are governments and public agencies as well as first responders in charge of homeland defence. The private demand of CBRN equipment is rather small having in mind the very unlikely nature of this kind of attack.

There is no regulatory framework for the certification of CBRN detection equipment, neither at global level, nor within the EU, probably because it is still a nascent market.

Chemical agents

Chemical agents are substances used to kill, seriously injure or incapacitate people through their physiological effects. These agents attack organs of the human body in such a way that they prevent those organs for functioning normally. The results are usually disabling or even fatal. Based on their effects, they can be classified in nerve, blood, choking and blistering agents. Common toxic industrial materials such as ammonia or chlorine used in refrigeration, water purification and other commercial applications also have harmful effects on human beings (Fatah, 2000:5).

The most plausible use of chemicals as weapons is in attacking aggregations of people in enclosed spaces (e.g. subways, airports, and financial centres) in ways that would cause disruption to crucial infrastructures services and render them unusable. Small quantities of chemicals would usually be all that would be needed (for nerve agents, a few hundred of grams would suffice). Use of a chemical agent in a non-enclosed space, however, is perhaps of less concern, because a toxic cloud would be subject to the vagaries of wind direction and thermal currents, thereby requiring large amounts (many kilograms) of the agent to cause numerous casualties (NRC, 2002:108).

Another form of attack could be the release of a chemical agent from industrial facilities (e.g. petroleum refineries, chemical plants, and oil and liquefied natural gas supertankers) or pipelines using explosive charges or simply by cutting pipes or opening valves. Under some meteorological conditions, release from production and storage facilities could permit a toxic plume to pass over heavily populated areas. Terrorists could take advantage of the frequent proximity of vehicles for transport of hazardous chemical to potential targets like trains that travel under cities or barges located in harbours (NRC, 2002:112).

Box 5. Plausible ways of a chemical attack

Stand off detection of the agent is the most desirable method. Infrared images and laser technology (LIDAR, Laser based Raman, vibrational spectroscopy, laser-induced breakdown spectroscopy, and tunable diode laser spectroscopy are being used for such purpose, however these promising technologies are still not completely ready for practical use. Point detection methods to measure the presence of the agent on the surface of an object include ion mobility spectrometry (IMS), flame photometry, infrared spectroscopy, electrochemistry, colorimetry, surface acoustic wave (SAW), photo ionization, thermal and electrical conductivity, or flame ionization. The detectors based on these technologies are used by first responders to provide a first warning that is subsequently confirmed by more sensitive analytical instruments to accurately identify and quantify the agent. These instruments include technologies like Mass Spectrometry, Gas Chromatography, High Performance Liquid Chromatography, Ion Chromatography and capillary zone Electrophoresis (Fatah, 2000:13). According to

OHS (2002:39) the technology to achieve affordable, accurate, compact and dependable chemical sensors is still immature.

The development of chemical sensors is heavily supported by the industry. Many industrial production facilities are routinely equipped with instruments to detect and identify the release of toxic materials (NRC, 2002:116).

Biological agents

People or livestock can be exposed to biological agents from inhalation, through the skin, or by the ingestion of contaminated food, feed or water. After exposure to a pathogen or toxin used as a biological weapon, physical symptoms can be delayed and prove difficult to distinguish from naturally occurring illnesses. Similarly, crops can be exposed to biological weapons in several ways –at the seed stage, in the field or after the harvest (NRC, 2002:65). These agents have the capacity to infect thousand of people, contaminate soil, buildings and transport assets, destroy agriculture and infect animal populations and eventually affect food and feed at any state in the food supply chain. At least, theoretically, highly contagious and lethal pathogens can present an even greater danger than nuclear weapons in that they are not limited to the geographical target area, and can continue to spread indefinitely (Ackerman and Moran, 2006). Biological agents include bacteria, viruses, rickettsiae and toxins such as anthrax, smallpox, plague, botulinum toxin, tularaemia, and viral hemorrhagic fevers (Fatah, 2001: 5)[136].

The means to combat such attack include environmental detection of agents together with preclinical, clinical, and agricultural surveillance and diagnosis (NRC, 2002:69). Because, no single sensor is able to detect all the agents of interest, several different technologies are needed as components of a detection network. Most biological detecting systems have significant logistic requirements, due to the use of wet chemistry and expensive and sensitive reagents[137]. Sensors should be able to detect agents on the air, on the surface, or on the water supply.

The challenge to an effective detection of these agents is the extremely high sensitivity –some highly infectious pathogens only need the inhalation of 1 to 10 organisms to cause disease (NRC, 2002:72)– and the unusually high degree of selectivity that the equipment shall have due to the large and diverse biological background environment. Air detection is the main early warning equipment since the primary infection route from exposure to biological agents is through inhalation. The detection system needs to discriminate between all of the naturally occurring particulates (such as dust, pollen, engine exhaust) and the biological agent particulates. For this purpose, it samples air and measures some inherent properties of the dry aerosol particles triggering a warning when it changes. Examples of detectors are the Aerosol Size and Shape Analyzer (ASAS) system that measures the particle shape from laser scattering, the Fluorescence Aerodynamic Particle Sizer (FLAPS) system that measure size and the presence of ultraviolet induced fluorescence and the Biological Alarm Monitor (MAB) which

[136] A terrorist biological attack will most probably be based on an agent without genetical modifications, since otherwise it will increase the complexity of introducing changes, and the need to test the new agent in animals to confirm its efficacy without affording any other relevant benefit.

[137] A reagent is a test substance that is added to a system in order to bring about a reaction or to see whether a reaction occurs.

measures the elemental decomposition by flame spectrophotometry. These detectors can reach close to real-time warning but have relatively low specificity, sometimes resulting in false alarms (Myers *et al.*, 2010). The identification process requires additional sensors. Due to the large variety of agents they are limited to a preselected set and can only identify others with the addition of new chemistry equipment or pre-programming. These systems can be installed on a mobile platform like a helicopter or UAV (Fatah, 2001:33).

Laboratory approaches to identify agents include microbial cultivation, immunological (e.g. antibody based) assays[138], and nucleic acid detection schemes, especially amplification methods such as the polymerase chain reaction (PCR). The last two approaches seek molecular evidence of agent components, such as characteristic immunological markers and genome sequences. A fourth broad approach relies upon the response of a subrogate host – such as cultivated cells from humans animals, or plants. Each of the mentioned approaches has its advantages and disadvantages. It is important to note, however, that even though cultivation is slow, limited in scope (by ignorance of appropriate grow conditions in the test tube and in human tissues for many pathogens), and the least technologically sophisticated approach, it provides the most ready assessment of complex microbial phenotypes (behaviour) such as drug resistance. It also is the most widely used approach in laboratories throughout the world specially in developing nations, and hence is currently the most common identification method for international surveillance (NRC, 2002:71).

In short, the technology to detect efficiently biological agents today is still immature, due to the high requirements than an effective system demands such as large variety of agents, short detection and identification time and expensiveness (*ibid.*:71). Such limitations impede a widespread use and the creation of early warning networks. Hence, considerable research is still needed in this area. Robust disease surveillance, as a second best solution, is the most appropriate method to early identify a bioterrorism attack. Classical epidemiological analysis like white blood count, fever, and relatively simple observations will remain the first line of defence in protecting human health (*ibid.*:74).

Information systems networks may be rather useful in such cases to post and share information between organisations involved in public health such as hospitals, emergency rooms, laboratories, public health departments, as well as law enforcement agencies for early warning. These systems may include medical records of patients with uncommon symptoms that might be related to the effects of a biological (or chemical) attack, records of biological incidents and so on. The information and communications industry is the main provider of such systems whose development is based on standard equipment and software (web-based). Customers are the different EU and national Rapid Alert Systems in charge of warning of biological contamination and pandemics.

The United States is seriously committed in improving their early warning capability of a dangerous release of biological agents into the environment. With this purpose, it launched in 2003 the Biowatch project within the National Bio-surveillance Integration System (NBIS). The system, which operates in more than 30 major metropolitan areas, periodically collects and analyses samples of air to detect pathogens. The system's

[138] Immunoassay detects biological agent using the reaction of cell antibodies to the pathogen. The reaction usually liberates a substance that can be measured like luminescent proteins.

sensors are being subject to intense research and continuous upgrade due to current shortcomings of the deployed sensors and analyzers that can require up to 36 hours in identifying a biological agent (GAO, 2010:48). Europe has not felt the need of such system and there are still no developments in this area.

Radiological agents

Protection against radiological agents is mainly achieved securing the life cycle of radioactive sources through adequate regulations, preventing in such a way the unauthorized access to radiological sources[139] which are most dangerous and capable of weaponization. Since, despite measures, such material could be stolen and smuggled, a capability for detecting its illegal trade is needed. Non-intrusive devices can be used to support this capability and warn of any abnormal radiation which may recommend further inspection.

Radiological attacks using a dispersion device could be carried out in several ways. Radiation sources could be hidden in facilities frequented by large numbers of the public (e.g. sports stadiums, subway systems) or dispersed taking advantage of the building ventilation systems. A radiation source could also be combined with an explosive to quickly disperse radioactive material over areas on the order of hundreds of square meters to a few square kilometres, depending on meteorological conditions[140] (NRC, 2002:49). Although these attacks would not probably disperse large quantities of radioactivity, they could cause public panic, especially if the attack takes place in a high populated urban area. Anyhow, a radiological attack lacks sufficient media coverage of bloody bodies and smoking rooms (Brown, 2006:21).

Detailed studies of Radiological Dispersion Devices (RDD) suggest that few if any human deaths would be expected from dispersed radiation, although the explosion itself could cause casualties. The presence of dispersed radioactivity in the attacked area could, however, confound rescue efforts. The most severe effects on human health are produced if the material can be efficiently dispersed in respirable form. For optimum particulate size, inhaled material can remain lodged in lungs, leading to either acute or chronic effects, depending on the amount and type of material respired. Even though there are methods to construct a RDD to obtain good dispersion of inhalable particles, they require expert knowledge and access to university level laboratory facilities (NRC, 2002:49).

If an RDD attack were to occur, the casualty rate would likely be low, and contamination could be detected and removed from the environment, although such clean up would probably be expensive and time consuming. It is clear that the aim of a RDD attack would be to spread fear and panic and to cause as much disruption to society as possible. Given the public fear of anything *nuclear* or *radioactive*, even a minor terrorist attack could have greatly magnified psychological and economic

[139] A wide variety of radiation sources are used in the civilian economy for, among other things, industrial radiography, radiation therapy, university research, energy power plants, and natural resource exploration. These sources contain penetrating gamma emitters like cesium-137, cobalt-60, and iridium-192; alpha emitters like radium-226 an americium-241; and beta emitters like strontium-90 (NRC, 2002:48). A radioactive waste shipment could be more easily stolen while in transit.

[140] Food and beverages can be poisoned with radioactive isotopes. Yet this method seems to be less likely due to the inefficiency of the spread method.

consequences. In general, public fear of radiation and radioactive materials appears to be disproportionate to the actual hazards. Although hazardous at high doses, ionizing radiation is a weak carcinogen, and its effects on biological systems are better known than those of most if not all toxic chemicals (NRC, 2002:61).

Box 6. Use of a Radiological Dispersion Device for performing a terror attack

The detection of radiological and nuclear material is made passively sensing the emission of gamma-rays or neutrons. Gamma radiation is emitted by all the materials of greatest concern and neutrons are emitted by only a limited number of materials including plutonium. The detection devices can be installed in portals for vehicle and cargo container screening. If the plutonium material is unshielded or lightly shielded, it can even be detected in vehicles at speed. On the contrary, passive detection of objects containing High Enriched Uranium (HEU) is very difficult and varies widely, being limited today to short ranges. In some cases, lightly shielded devices can be detected at portals, but in others, they can only be detected if they are essentially unshielded. HEU can be detected by active monitoring using, for example, pulsed neutron sources and neutron detectors (DSB, 2004 and NRC, 2002:55).

Radiological and nuclear detection equipment has a high technological readiness *vis à vis* chemical, biological and explosive detection equipment. Ecorys (2009: 166) distinguish four types of devices. The first is fixed radiation portal monitors which are tailored to the kind of traffic like persons, vehicles, packages or other cargo. They can be deployed and set permanently at road checkpoints, cargo inspection stations, and ports[141]. The second type is personal radiation detectors, commonly referred to as pagers, which are small handheld devices that detect gamma radiation. They are mainly used by custom officials and police for detecting illicit radioisotopes and could be used by emergency responders as a mean to monitor a large number of people for radioactive contamination after a suspected radiological or nuclear incident[142]. The third type is hand-held gamma and neutron search detectors which provide greater sensitivity and can be used to locate the radiation source. Finally hand-held radioactive isotope identification devices (RIID) are devices designed to determine the identity of the radioactive material through the analysis of the gamma radiation signature. Example of this kind of equipment is GR-135 RIID of SAIC, the personal radiation detectors of Berkeley Nucleonics, or the High Performance Radioisotope Identifier (HPRID) of Smith Detection.

The Domestic Nuclear Detection Office of the USA will develop, acquire and support the deployment of a domestic system to detect and report attempts to import, assemble, or transport a nuclear explosive device, fissile or radiological material intended for illicit use. This Office is spending a large amount, above $2 billion, in the development

[141] This equipment is combined with X-ray active imaging in order to screen suspicious containers. One shortcoming of current radiation portal monitors is their inability to distinguish between legitimate commercial radioactive material (e.g. medical, industrial); naturally occurring radioactive materials (such as rocks, minerals, metals processed, scrap, fertilizers, ceramic or bananas), and potential terrorist weapons such as radiological dispersal devices or improvised nuclear devices.

[142] Sodium iodide scintillation detectors, Cadmium-Zinc-Telluride semiconductor detectors, Germaniun gamma-ray detectors, semiconductor charged-particle detectors, Geiger-Muller counters, ionization chambers, plastic scintillator detectors and high-pressure Helium proportional counters are the main technologies used (Myers, 2010). Dosimeters are also needed to measure radiation exposure of first responders. They are based on quartz fibre, film-badge, thermoluminescence or solid state (Wikipedia).

new detection equipment, namely the Advanced Spectroscopic Portal Monitor (ASP), the Cargo Advanced Automated Radiography System (CAARS) and the Human Portable Radiation Detection System (HPRDS). The first system will be able to identify the isotope causing the alarm thus avoiding a secondary inspection; and the second will be able to detect high density shielding. European companies have important knowledge on nuclear and radiological detection technologies (e.g. CEA, Areva Group, Siemens) and the 7th ERFP considers such topic. Yet, the available economic resources for financing such research seem to be considerably smaller.

Nuclear attacks

Nuclear attacks may include the attack to a nuclear facility, the explosion of a self constructed primitive nuclear bomb fabricated from stolen or diverted nuclear material and components, or the stealing of a state-owned nuclear weapon[143]. The main countermeasure is the early detection of materials used to fabricate the bomb, or the bomb itself, before the attack is made. It includes physical protection measures, control of radioactive sources, and measures against illicit trafficking. These measures have been analysed in the previous section.

Systems to support intelligence operations

Actionable intelligence is essential to defeat terrorism and organised crime. The activities of these groups entails gathering information, selecting a target, planning the attack, recruiting and training executors, purchasing goods, obtaining financial support, travelling to the place where the target is located, performing the attack and disseminating propaganda and revindication material. Whereas these groups attempt to disguise their identities and remain invisible against the backdrop of an enormously diverse and mobile society, they always leave in performing said activities, voluntarily or involuntarily, traces in large quantities and in dispersed ways, inside different public and private organisations including the web. The timely and thorough collection, analysis, interpretation and dissemination of information about the activities and plans of these groups allow the government to take immediate- and near term action to disrupt and prevent their actions and to provide useful warning to specific targets, security personnel or the general population.

Such capability can be enhanced with the aid of information and communications systems. These systems can store large databases of personal identities; information related to judicial, police, immigration and customs historical records of individual offenders committed or likely to be committed illegal activities, as well as complete dossiers of past terrorist or criminal offences including information of suspects, potential witnesses and collected evidences. Simple consultation to these databases may be very helpful to verify identities or pursuit orders[144]. Advanced tools, based on retrieval and correlation of data, such as face images, fingerprint or DNA, may help to build conjectures and verify hypotheses, deriving in this way knowledge about terrorism and organised crime which may be used to identify members, networks, operational means and sources of support.

[143] Attacks based upon stand-off weapons such as ballistic or cruise missiles should be considered out of the capabilities of terrorism and organised crime.

[144] This access may be even done from a vehicle data terminal using a wireless link able to upload the fingerprint template.

There is a general believe that information and communications technologies will largely improve the intelligence capabilities to combat terrorism and organised crime (NRC, 2002:166). The knowledge of these groups is expected to increase through the use of high performance computers and sophisticated algorithms. Yet these expectations are not shared by all and many question the value that can be obtained from this information (Anderson, 2001; Markle Foundation, 2002:2).

The automated analysis of text, image, video, sensor, and other kinds of unstructured data by a computer may enable to sort efficiently massive quantities of data to bring the relevant evidence to the attention of the analyst. Information fusion, data mining and natural language processing are three main areas of research. These techniques may be applied for example to massively analyse online information such as e-mail, news articles, memos, and web sites pages (NRC, 2002:169).

Information fusion is defined as the use of computer technology to acquire data from many sources, integrate these data into usable and accessible forms, and interpret them generating new knowledge. Data mining is the automatic machine-learning of general patterns from large volumes of specific cases. Bayesian network learning and logistic-regression-and-support vector machines are among the most widely used statistical machine learning algorithms. Natural language technologies include information extraction, cross-lingual retrieval, machine translation, summarization, categorization, filtering and link detection (NRC, 2002:168). Yet, the performance of these advanced tools to improve intelligence capabilities is, for the time being, largely unreported.

Box 7. Promising technologies in intelligence based on computers

Traces of suspicious activities may be recorded in private data bases such as phone calls, e-mails, economic transactions (e.g. credit cards), hotel and car rental record data, or passenger name records. Systems able to automatically access this information have been forecasted. Whereas this capability is so far hardly achievable due to the complexity and cost of developing the appropriate interfaces, the main issue is likely the adequate protection of privacy and civil rights[145] and the financing of the compensation amount for retaining and supplying such information by private agents. The principle that the access to private information shall be proportionate and necessary calls for a prior (judicial) authorisation mechanism granted on a case by case basis, to preserve these rights and impede the indiscriminate data retrieval from such databases. Only a change in citizen's preferences between privacy and security could make feasible this kind of developments, a change that is not envisaged for the time being.

Banking information can be especially useful to fight against money laundering, terrorism financing, and other illegal transactions such as armament or drug trade. The source and destination of the transfer may be correlated with available intelligence (e.g. financial sanctions lists) to identify and trace suspicious transfers and proceed to freeze or confiscate these assets[146]. Directive 2005/60/EC and Regulation (EC) No 1781/2006

[145] See on this issue the opinion of the EU art. 29 data protection working party 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Project PRISE concluding Conference Statement Paper (undated) demands that access to such information should be based on specific suspicion and should require court orders.

[146] Terrorist attacks are relatively inexpensive. For example according to the European Commission (2004b), the Madrid bombs did not cost more than €8.000; Hoffman (1998) reports that the cost of the 1993 World Trade Centre bomb was only $400, but caused over $500 million in damages; and the

provide support for such activities. Finance Intelligence Units of member states are customers of information and communications systems applied for such activities. The EU FIU-net system is aimed at sharing such information among member states.

Sharing intelligence across agencies and nations provides important advantages, but it requires the development of interoperable standards and software tools that allow the exchange of information between these agencies and nations (Munday *et al.*, 2006:14). This entails the agreement on interfaces and the development of translation gateways to automate the data access when standards did not exist at the time the system was made. Success in information sharing has been achieved in the Schengen Information System (SIS) [147], the Visa Information System (VIS), the EURODAC (the EU asylum applicants fingerprint database), or the European Custom Information System (1995) for exchanging of information on smuggling led by the European Anti-Fraud Office (OLAF). Yet, there are areas where interconnection has not been still been achieved as for example AFIS systems of Member States (IPTS, 2005:117). Europol, as an organisation aimed at improving cooperation in combating terrorism and organised crime, and Eurojust, as an organisation aimed at increasing judicial cooperation such as the access to criminal records, are two essential institutions in the development of these systems.

These intelligence tools help to discover recurrent patterns or 'profiles' permitting the classification of people, objects, or actions into different categories. Some of these categories may be considered to deserve further attention or special treatment, helping in this way to more focused searches and inspections. They can be applied to identify trustworthy (low risk) people or cargo and circumvent routine inspections that are always costly and of limited efficiency[148].

Main suppliers of these systems are prime-contractors and software companies which implement the system with the support of specialised companies that provide software modules and computer hardware. Governmental law enforcement and intelligence agencies are the main customers of these systems. Data on this market segment is unavailable since procurement programmes are usually classified. Basic technologies used are mostly of dual nature and are applicable to other areas like business intelligence and knowledge management.

Other markets related with intelligence and surveillance

Economist (2003, p.45) reports that the 9/11 attack cost less than half million dollars. However, terrorist groups need a constant financial flow for propaganda, recruitment, facilitation, etc. that requires methods to covertly collect and transfer funds. They may include the electronic transfer of small amounts of money that will not raise suspicion, cash payments, or informal cash transfers like the *hawala* (also known as *hundi*) system that makes difficult to disguise who is making the transfer to whom. The development of anonymous payment technologies, such as stored value-type smart cards, poses new risks since they may be abused by money launders and other financial criminals. These transfers of money are hard to detect since bank intermediation is unnecessary (Molander, 1998).

147 This system contains information about persons to be arrested and surrendered, stolen passports, objects to be seized, persons or vehicles to be searched, etc.

148 Whereas profiling is not inherently bad, the classification based only on external indicators is always subject to error giving way to false positives. This rate can be enough high to reduce inspections to an affordable level. Even a low rate may not be too helpful for large flows such as people or cargo crossing borders. Profiling may give way also to false negatives, and, once the system is learned, features that will not raise a warning may be used to improve this rate (Martonosi and Barnett, 2006).

In addition to the abovementioned market segments, there are other segments with some relevance whose size is comparatively smaller in terms of revenues as for example: communication interception equipment, microphones and transmission system used by intelligence operations, special radars to locate people behind walls, devices attached to suspect vehicles to allow their tracking, GPS based bracelets to control prisoners on parole, or banknotes counterfeiting testing equipment.

PROTECTION

Protection is needed should intelligence, surveillance and other preventive measures fail. It means hardening potential targets so that their disruption or destruction becomes difficult to attain. In the field of protection the following areas have been identified:

- Building protection
- Vehicle protection
- Personal protection
- Manned guarding services
- Information systems protection

Building protection*[149]*

The protection of buildings mainly focuses the most likely kind of attack, that is to say explosives. The protection is based on the design of a layered architecture composed of different physical barriers (e.g. fences, bollards) and obstacles, as well as perimeter surveillance and access control systems to screen individuals, vehicles and other objects entering into the building, as the ones that have been previously described. When feasible, appropriate buffer/safe zones and forward holding areas for visitors are drawn up to reduce effects of an explosion within a dangerous distance of the building, especially when a (suicide) car or truck bomb is used[150]. Yet these measures have to be balanced with other constraints such as accessibility, cost, or aesthetics[151]. The design is also aimed for limiting and mitigating damages and facilitating rescue efforts. It includes measures to resist effects on the building façade (e.g. limiting flying debris), reinforced structures to resist progressive collapse, and the maintenance of emergency functions (using for example redundancy) until evacuation is complete. Reinforced concrete and laminated glass (to avoid glass laceration) are some of the materials used for this purpose. Access control, surveillance systems, and early fire detection and extinction are nowadays integrated within the building management system that controls all the relevant building functions such as lightning, elevators, power supply or communications.

The second most probable kind of attack would be a chemical, biological or radiological attack. Protection is mainly achieved through improved design of the Heat, Ventilation

[149] For more details see FEMA (2003).

[150] However, the number of attacks with large trucks loaded with explosives has been rather small. Air attacks by small crafts loaded with high explosives as 9/11 can be feasible as well. The protection against this threat is only partially achieved through air space control able to early warn of a renegade aircraft.

[151] For example, the access control system cannot be so rigid that it prevents the safe exit of a building's occupants during emergencies such as a fire.

and Air Conditioning (HVAC) system such as hard-to-access outdoor air intakes, air filtering using HEPA filters and air cleaning using sorbent filters[152].

The construction sector is the main supplier of secure buildings. Specific designs to reinforce the building do not substantially differ from similar methods used for protection against natural or man-made disasters such as earthquakes, floods, hurricanes or fires. Specific security enhancements are usually provided through the subcontracting of specialised companies in areas like intrusion detection, fire detection, or voice communications systems. Examples of this kind of companies are Siemens Building Technologies, Schneider Electric, or Software House (Tyco). A secure building may raise its total cost between 5 and 15%. However, only a limited fraction of buildings (e.g. embassies and some critical infrastructures) deserve such protection. No economic figures have been found of this market segment.

Vehicle protection[153]

Vehicles for the transport of cash and valuables and vehicles for transport of VIPs are the two kind of vehicle protected against terrorism and organised crime. Both are based on a standard vehicle design modified to endure an attack such as runflat tires and the use of steel or reinforced glass to protect passenger area, fuel tank and batteries. Since protection adds extra weight, the car suspension and brake systems are usually reinforced. The vehicle changes to integrate these elements are made by the proper car builder or by small specialised companies.

The number of vehicles that require protection is rather small. The main customers of vehicles for cash and valuables transport are guarding companies that provide this service. VIPs vehicles are reserved to a short number of high rank public officers as well as presidents and CEO of large companies. Examples of suppliers are SVOS Company, or Hartmann Spezial Karrosserien GmbH.

Electromagnetic shielding is also required to neutralize radio controlled improvised explosive devices. Such weapons may be easily activated using modified cell phones, cordless phones, or remote garage door openers. Such equipment is mainly provided by suppliers of electronic jamming equipment for defence as for example Warlock made by EDO Communication and Countermeasures Inc. (a subsidiary of ITT Corporation), ICE made by Raytheon, or K9 International Corp.

After a CBRN attack, adequately protected vehicles may be needed for reconnaissance within the contaminated area. They are based in an overpressure in the sealed interior of the vehicle combined with a filtering system to avoid the entry of agents thus avoiding that the crew dresses special protective suits. The defence industry that supplies battlefield vehicles with this protection also supplies the civilian market as can be the company Rheinmetall AG. Civil protection organisations are the main purchasers of these vehicles.

[152] Air filtering is used to protect against agents that travel in the air as an aerosol whereas air cleaning is used against agents that travel as a gas. Further details can be found in NIOSH (2003).

[153] The sophisticated equipment under development to protect airliners from missile attack is being developed by the defence industry. Wheeled armoured vehicles for police special operations are also supplied by this industry (e.g. Dingo 2 vehicle of Krauss-Maffei Wegmann).

Personal protection

Personal protection equipment (PPE) is aimed at protecting police and first responders from:

- Small arms and shrapnel of explosives.
- Fire to rescue people from heat and flame.
- CBRN contamination.

The equipment, especially designed to resist the different threats, includes clothing, gloves, boots, a mask or helmet, respirators, and sometimes shields. The heaviness and bulkiness of the equipment means a physiological burden –due to limited mobility and vision as well as heat stress– that interferes with the operational duties of the user.

Clothes are made using high-resistance fabrics such as aramids[154]. For protection against bullets and shrapnel ceramic tiles can be used. The heavy weight of vest limits protection to the more vulnerable parts of the body such as the thorax. Chemical and biological protective clothes use special tissues, such as active carbon, to avoid that chemical or biologic particles reach the skin. A mask with a breath filter is required to protect the face and avoid the entry of noxious agents into the lungs.

Vests are made by the apparel industry which normally provides uniforms and dresses to armed forces, police forces, or guarding companies. The company size has to be enough large to supply in time the number of units demanded. Sales are made directly from manufacturers to the customer. Fibres are dominated by a group of global market players like Dupont (USA) and Teijin Aramids (JP). European fabrics manufacturers are Tencate (NL), Ibena (GE), Utexbel (BE), Seyntex (BE) and Klopman (IT). The high value of these fabrics, which require large investment and specific skills, makes that this industry is still competitive against Far East countries more focused on low-end quality fabrics. Main suppliers are Seyntex, Sioen industries (BE), Lion Apparel (USA), Bristol Uniforms (UK), Remploy Frontline (UK), Cosalt (Ballycare), Arlen (PL). Some small companies provide also support services such as cleaning (Ecorys, 2009: 258).

Main customers are police forces, fire brigades and manned guarding companies. Purchases are very fragmented since customers are many times local or regional. The industry also supplies this kind of equipment in other civilian markets like chemicals, oil and gas. This is a '*replacement market*' with a limited amount of new customers and a vegetative growth. Ecorys (2009:247) estimates the revenues of this market in Europe between €525 and €875 million. Research on light materials for this kind of equipment is a permanent need for the reasons mentioned before. Nanotechnology and smart or intelligent textiles seem interesting research areas, still without practical results.

Manned guarding services[155]

[154] Aramid fibres are very frequently used in civilian products like sails, cables and wings of aircrafts. Most known trademarks are Kevlar, Nomex, or Twaron.

[155] In this section, we analyse only Private Security Companies as opposed to Private Military Companies based on mercenaries that provide security services to firms (e.g. BP) with interest in foreign countries involved in some kind of armed conflict. On this issue, see Holmqvist (2005).

Many market agents that are willing to pay for improving their security, due to the benefit they perceive or because regulations impose them the implementation of some security measures. In such a case, guarding services can be hired to specialized private companies when in-house provision is more expensive and less effective such as for example the screening of passenger personal belongings that airports usually outsource. The main services these companies provide are:

- Protection of people and property, and the maintenance of law and order (De Waard, 1999) in a wide variety of environments such as factories, warehouses, offices, shopping centres, hospitals, transport hubs, car parks, concerts and sports venues, official sites or residences.
- Transport and storage of cash and valuables.
- Operation of security equipment, including intrusion detections systems, access control systems and personal inspection of belongings.
- Remote surveillance based on home alarm equipment connected to a central monitoring centre[156].

According to Frost & Sullivan (2008b) report the market of guarding services is large in Europe. Revenues in 2007 accounted for €24.5 billion with an expected growth rate of 5.4%. This steady growth is also noted by Van Steden and Sarre (2007) that attribute it to the perceived need of higher security and the advantages of outsourcing these services.

According to this report static guarding is the main service supplied representing the 68% of total revenues, alarm monitoring and response follows with 19% and cash services is around 13%. Services are sold to the industrial (32%), commercial (49%) and government [including public transport] (19%) sectors. The demand of individuals is not recorded, probably because it is not significant. Revenues, employees and number of companies in 2007 are resumed in the next table:

Country	Rev.	Rev./GDP	Empl.	Companies	Concentration
Austria	212	0.08%	10,000	200	
Belgium	715	0.21%	18,000	300	90-95% top 4
Bulgaria	55	0.18%	33,000	960	Dominated by few large companies
Czech Republic	240	0.19%	42,000	5,600	70% among top 10
Denmark	345	0.15%	6,000	350	56% top 2 companies
Estonia	140	0.88%	6,500	10	70% one dominant player
Finland	300	0.17%	8,000	150	70-80% top 4
France	4,050	0.21%	150,000	4,600	less than 30% top 4
Germany	4,300	0.18%	171,000	3,300	less than 20% top 3
Greece	223	0.10%	48,000	1,027	Fragmented market dominated by 15 companies
Hungary	859	0.85%	80,000	3,000	Dominant player 36%
Ireland	400	0.21%	12,000	300	
Italy	2,510	0.16%	52,000	1,300	36% top 9
Latvia	110	0.52%	5,500	360	80% top 6
Lithuania	90	0.31%	10,000	135	Dominant player more than 30%.

[156] The operator of the system can investigate the sensor triggered by the alarm and, being the case, send a patrol to the household or warn police. The patrol sent to respond to the potential security incident is usually in constant contact with the control centre via radio.

					Top 5 80% share.
Netherlands	1,135	0.20%	35,000	500	60-65% top 3
Poland	1,435	0.46%	200,000	4,000	38% top 6
Portugal	664	0.39%	36,000	105	51% top 5, 82% top 10
Romania	219	0.18%	92,000	1,055	60% top 6
Slovakia				1,730	
Slovenia	1.3	0,00%	6,300	100	
Spain	3,350	0.32%	89,000	1,134	80% 18 members of APROSER
Sweden	669	0.20%	17,000	250	85-90% top 3
United Kingdom	2,520	0.12%	140,000	1,600	47% top 4
Total[157]	24,541	0.20%	1,267,300	30,236	
Source: Austria, Ireland, Slovakia and Slovenia (CoESS), remaining member states Frost & Sullivan (2008b). Revenues in million €.					

Table 14. Guarding services market in the European Union (2007).

As can be seen from the table, the sector is highly atomised with a large number of companies of small and medium size (nearly 96% in 2008 according to Eurostat *sbs_sc_1b_se_r2* table) and only very few of large size and with a large market share (47% using the same table). National preferences on guarding services largely differ across member states as the rate between revenues and GDP shows.

According to INHES and CoESS (2008), there are one and a half times as many public security employees in Europe as private security employees. Yet, deviations of this average value across member states are considerable[158]. This profession is very unattractive due to routine and uninteresting work, lack of career opportunities and low salaries. Nevertheless, the sector provides job opportunities to individuals with little or no skills and some shelter in time of crisis. These factors result in very high turnover in most European countries. Yet, this rapid turnover becomes a quite convenient management method to companies for adjusting their workforce based on demand.

Today, private sector employees are globally recognized as vital partners in preventing and detecting crime (Van Steden and Sarre, 2007). The majority of member states have specific legislation regarding this industry, but no EU regulation still exists on this issue. Authorisation to operate in the market is conditioned to have sufficient working capital, and suitable qualified personnel. Staff members' judicial records, personal circumstances and conduct must be such that they do not present any risk to the organisation. Staff members are required to receive training in order to guarantee their professional skill. Training programmes (basic and follow-up) have often to be approved by the governmental authority in charge to ensure a reasonable quality of service. Other operating conditions ruled are the use of uniform, identification badge and weapons. Companies, often, must submit an annual report based on a prescribed model (De Waard, 2009). Yet, the behaviour of the industry in Eastern Europe has raised concerns[159].

[157] INHES and CoESS (2008) provides different numbers: 1.7 million jobs, 50,000 companies and €15 billion of revenues. Eurostat *sbs_na_1a_se_r2* table estimates this value in the same year in 31,743.

[158] In the United States private security guards outnumber law enforcement personnel in the early eighties according to Amy Goldstein, Washington Post January 7, 2007.

[159] According to Van Steden and Sarre (2007) the Czech Republic lacks of a regulatory framework on this sector. And SEESAC (2005) reports that there is a growing professionalization and legislative efforts to introduce controls in the industry located in South Eastern Europe.

Network and information security (NIS)

The business of many agencies, organisations, companies and individuals requires the assurance of the availability, authenticity, integrity[160], and sometimes the confidentiality of information. This market segment encompasses the goods and services required to solve this need whether the information is stored on paper or in digital form. Paper documents are stored safely using armoured safes and boxes. Safe transport is usually made by security services companies. Sealed envelopes and containers are the common method of preserving confidentiality of this information. This is a rather mature market with a slow evolution and growth with only small technological advances in electronic locks. According to Eurostat *prodcom* table the production value of the EU was €762 million in 2009.

The societal trend to store information in digital form, the development of the worldwide web, and the appearance of new data transmission means such as wireless networks (e.g. wi-fi and mobile PDAs) have created a new set of vulnerabilities and have leveraged a complete new market of products and services to fight the new threat already known as cyber crime. This is one of the areas where illegal organisations can accrue important benefits if they copy, modify or destroy key information; execute unauthorised operations such as the electronic transfer of funds, cause harm to computers reducing their performance or use them to perpetrate other attacks using malicious software (malware) such as virus, spyware, worms, Trojan horses, backdoors, keystroke loggers or root-kits. This problem could be particularly important if the attack is against information and communication systems that support critical infrastructures since such attack can impair or even disrupt the essential services they provide to society[161]. The magnitude and losses of cyber attacks are hardly known and most companies do not publish their figures on the basis of a potential loss of customer confidence. According to OECD (2008:6 and 39) malware has evolved from occasionally *exploits* to a global multi-million dollar criminal industry. Direct damages of malware were estimated in €9.3 billion in 2006.

Cyber crime can be defined as *criminal acts committed using electronic communication networks and information systems or against such networks and services*[162]. It involves three types of criminal activities related to information systems. This first covers traditional forms of crime such as fraud and forgery but made over electronic information and communication networks systems with the aim of procuring, without right, an economic benefit such as identity theft or information copy which may be labelled with copyrights as for example digital films. The second concerns the

[160] Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Source: An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12 (1995).

[161] SCADA systems are used to control the physical elements of such infrastructures. Since these systems are increasingly being linked with other systems (such as electronic business) through the internet, they are more vulnerable to attacks (NRC, 2002:208). Whereas such attack seems not to be easy, OECD (2008:43) reports that malicious hackers in Russia used a Trojan to take control of a gas pipeline run by Gazprom. The U.S. Central Intelligence Agency analyst Tom Donahue announces at a meeting hosted by the SANS Institute on January 16, 2008 that web hackers penetrated overseas power grids, compromising service while demanding payment in exchange for cessation.

[162] COM (2007) 267 final. Towards a general policy in fight against cyber crime.

publication of illegal content over electronic media (e.g. child sexual abuse material or the incitement to racial hatred). The third includes crimes unique to electronic networks and against the confidentiality, integrity[163] and availability of data and systems[164]. The aim of these often well organised attacks is sabotage, extortion, or political and ideological goals. Cybercrime uses different techniques to gain computer access and perform their misdeeds. For example, it can exploit inside information, use dictionary or brute force attacks, use social engineering[165], as well as signal interception and the deciphering of information to get passwords.

Computer crime may involve the physical access to computers. Such access may be easily restricted through some of the physical protection measures commented in previous sections. The majority of attacks, however, are made through communication lines and the protection is fundamentally achieved by means of software modules and programs able to identify and authenticate users, grant their access, track their actions, as well as detect malicious software attempting to find a backdoor of the system through which it can attain its goals.

Specialised software companies offer a large set of products and services to counteract this threat. They range from software to protect personal computers to large enterprise integrated security solutions. Products include: (a) methodologies to design and develop software systems without weak points; (b) middleware for dependable user identification and authentication based on passwords, cards, tokens or biometrics to authorise the access to data, systems and software applications; (c) strong encryption algorithms for secure exchange and storage of data[166]; (d) network real-time monitoring and data flow analysis to detect anomalous users or unusual traffic patterns which may indicate an attack; (e) filters that avoid suspicious data packets (firewalls), malware, unsolicited mail (also known as spam), or access to harmful material (through web browsers); (f) logs and audit data tools to perform forensic analysis, and (g) tools to easily recover from an attack, using some kind of data or equipment redundancy (off-site backup / storage system). Their ultimate objective is that the system's user enjoys a *trusted* on-line environment.
The increasing complexity of developing and maintaining effective security operations and the lack of in-house expertise explain the development of a wide range of services by the industry, which includes: (a) consultancy in areas like strategy and planning, assessment on best practices, audits, forensics; (b), implementation of tailored solutions that may encompass activities of design, development, integration, test (e.g. system

[163] For example malware is designed to encrypt or scramble users' data so that the owner cannot retrieve it. Often the owner will be asked to pay a ransom (OECD, 2008:16).

[164] The most common type of attack is the well-known Distributed Denial of Service for companies that provide just in time services (e.g. e-commerce) and risk losing significant revenue for every minute their website or network is unavailable. This is also the case of government agencies who rely on websites to provide services to citizens. The attack uses a larger number of compromised computers called *botnets* to send massive amounts of queries and overwhelm the system (OECD, 2008:15). Botnets are also used to distribute spam and phishing attacks, distribute spyware and adware and harvest confidential information that may be used in identity theft. The plethora of launch points and routes for cyberattack greatly complicates the ability to counteract it, as well as to identify the source (NRC, 2002a).

[165] Social engineering refers to techniques designed to manipulate users into providing information or taking an action which leads to the subsequent breach in information systems security (OECD: 2008: 12). It involves for example the masquerading of a trustworthy person or web site to obtain password or credit card details to steal an identity.

[166] Like the ones used in Virtual Private Networks (VPN) such as IPSec and SSL protocols.

penetration), or migration; and (c) operations such as managed security services[167], hosted services, outsourced services (e.g. incident response).

IDC (2009:2) estimated the value of the European NIS market in 2007 in €10.7 billion of which €4.8 corresponded to software products, €4.7 to services and only €1.13 to hardware[168]. Average forecast growth rate was estimated in 13.1% for the period 2007-2010. The demand of these products concentrates in the Member States where the information society is more evolved. The market is dominated by a small group of global vendors, differentiated by application area, competing with a high number of smaller European or international suppliers. Dominant players are Symantec (US) for the software solutions segment, IBM (US) for security services and Cisco (US) for hardware security. McAfee (US) and Trend Micro (JP) are also relevant players. These top five vendors had 20% of the EU NIS market in 2007. According to the IDC report main EU suppliers, while showing a positive dynamism, are not global players. No single vendor is capable of addressing the full spectrum of security issues, primarily due to the fact that the investment in skills required to develop such a broad range of products is prohibitive (IDC, 2009:31). They operate in their native country and some other markets only. The cumulative market share of EU suppliers was 16.5% of the total EU NIS market revenues. New entrants in the market are large players diversifying into security from their native markets like Cap Gemini or Atos Origin, or telecom operators and ISPs such as BT Global Services, Telefónica, Deutsche Telecom (T-Systems) or Telecom Italia. To be competitive in this market companies need to be aware of the future growth of the internet and their threats on a worldwide basis.

Total		Hardware		Software		Services	
Symantec	7.9	Cisco	23.1	Symantec	17.9	IBM	6.5
IBM	4.5	Juniper	8.9	McAfee	7.0	Accenture	4.0
McAfee	3.1	Netasq	4.3	Checkpoint	4.3	Cap Gemini	3.9
CISCO	2.5	Fortinet	3.7	Trend Micro	5.0	EDS	3.4
Trend Micro	2.2	Gemalto	2.4	IBM	3.6	HP	3.4

Table 15. Top 5 vendor in the European Security Market and revenues in million € (2007). Source: IDC (2009)

The network of distribution channels is rich and complex. It includes direct distribution, distribution through the web, and third parties such as retailers and OEM. Telecom and ISPs also offer security solutions embedded with their subscription and services (IDC, 2009).

[167] Valued in $1.9 billion in 2009 according to Gartner (2009a).
[168] Gartner (2009) estimated for 2008 a smaller value for software, namely $3.2 billion.

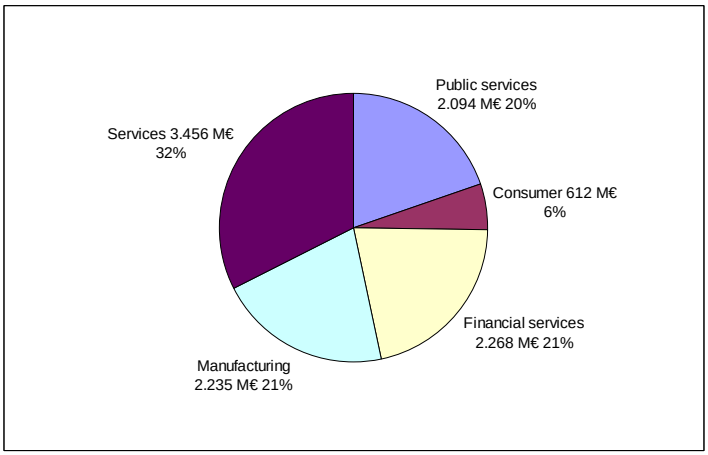

Figure 5. Market demand distributed by sectors.
Source: IDC (2009)

As can be seen from the figure above, the demand for protection against cybercrime is dominated by the business sector (public and private) playing the individual consumer demand a minor role. The main customers are companies supplying basic internet services as well as companies providing e-commerce, e-government applications and other on-line services such as banks, virtual stores, tax agencies or ministries because they are high-pay off targets to cybercrime. Small companies are less likely than large corporations to implement controls (EU, 2005:7). Individual demand is mainly supplied with standard low-cost security products.

Computer Emergency Response Teams (CERT) plays an essential role in the NIS market. They are specialised organisations financed by governments to monitor, prevent and detect computer security incidents and circulate information about them. Such services are provided for free or at subsidized rates. These teams facilitate the development of products and services to respond to new identified threats. The CERT® Program is part of the Software Engineering Institute (SEI), a federally funded research and development centre at Carnegie Mellon University in Pittsburgh, Pennsylvania. In Europe, it has been created the European Governmental CERT Group (EGC) an informal group of governmental CERTs that is working out effective co-operation on incident response matters between its members.

INTERDICTION / CRISIS MANAGEMENT

When an impending security incident is discovered means are needed to frustrate it before it can create any damage. Personal equipment and vehicles are the most relevant goods.

Personal equipment

Personal equipment is composed of surveillance gear (e.g. night vision equipment), personal protective equipment; communication radios; and effectors to neutralise potential offenders and their weapons. We will comment here briefly effectors, since personal protection equipment has been discussed formerly, and communication equipment, being the same as the ones used for response and recovery, will be commented in that section.

Effectors are based on different type of light weapons, some of them of low lethality such as tear gas or stun grenade launchers. The most common weapons are small arms such as pistols, rifles and submachine guns. Main suppliers work simultaneously for defence and security and sometimes for sport and hunting. Examples of these firms are FN Herstal (Belgium), Heckler and Koch (Germany), or Beretta (Italy). Europe is also a large producer of high-quality (following NATO design and safety standards) ammunition for these guns such as for example RUAG Anmotec or Namno A.S. The low technology and skills needed for manufacturing explain that small arms production facilities is spread worldwide, where some nations may enjoy competitive advantages due to low labour costs and a softer environmental protection legislation in comparison with advanced countries as could be the case of Singapore and Brazil. Police forces (national, regional or local) and guarding companies, apart from armed forces, are the main customer of light weapons. The production and sale of this material, with clear military use, is subject to administrative controls.

Vehicles

For certain operations land vehicles, helicopters or maritime craft are needed to interdict criminal actions and prosecute malefactors. These vehicles are usually standard vehicles with small design changes and specific mission add-ons such as increased surveillance or communications equipment (e.g. radios, night lights, vision equipment, and locating radars). Some of them are specially prepared for coordinating the operation (see next section) with increased command and communication capabilities. The main supplier tends to be the company who has the largest share in the total value that usually is the system integrator. This role is played by the vehicle manufacturer (automotive, aerospace or shipyards industry) or the supplier of the electronic equipment.

Robots are of special utility in security due to their ability to sense and manipulate the environment with great precision –in the absence of such human limitations as physical vulnerability, fear, boredom and discomfort– make them ideal tools for some security missions such as close-in surveillance (in which small size is critical); sampling of nuclear, biological and chemical contamination; urban search and rescue; ordnance disposal; decontamination; debris removal, or fire fighting.

Products in this market are tailored to security needs based on civilian designs. Units demanded tend to be small with the only exception of law enforcement land vehicles. Advances in the area are coming mainly from civilian developments, such as for example, an area that is subject today to an intense research.

RESPONSE AND RECOVERY

Response to a security incident or disaster provides for the immediate protection of life and property, the re-establishment of control and the minimization of effects. It encompasses the issuance and dissemination of predictions and warnings; planning and preparation immediately before the event; evacuation and other forms of protective action; mobilization and organization of emergency personnel, volunteers and material resources; search and rescue; care of casualties and survivors; damage and needs assessment; damage control and restoration of public services; and maintenance of the political and legal system (Rao *et al.*, 2007:17).

Disaster recovery encompasses both short-term activities intended to return vital physical and social systems to operation and long-term activities aimed at restoring the situation to its pre-disaster state. The concept of recovery encompasses both objective measures, such as reconstruction and assistance efforts, as well as the subjective experiences of disaster victims and processes of psychological and social recovery (Rao *et al.*, 2007:17).

Means for response and recovery are indistinctly used for any kind of emergency or disaster independently of its source (nature or man-made) including those originated by terrorism and organised crime. The industrial analysis will focus in the activities and means needed in the aftermath of an attack that has been grouped in the following ones:

- Firefighting
- First response health care
- Logistic support
- Coordination and management

The main customers of these systems are first responders and emergency units of the public administration. These units have local, regional, national or European nature and they will enter into action depending on the disaster size. Hence purchasing capabilities and products and services preferences will differ across the different units.

Firefighting

Fire protection within buildings and facilities is achieved primarily using own capabilities based on fire detectors, alarms, and extinguishing systems which are mandatory according to building regulations. However, fire-fighting units and brigades are needed when the fire becomes large and out of control. The main equipment used to fight against fire is industrial vehicles (such as MAN, IVECO, Renault or Volvo) that integrate movable turrets with built in pumps that project water, foam or powder on to the fire. Sometimes these vehicles are modified by SMEs that sell them to the final end customer (municipalities, civil protection units, airports). The most common version is for urban fire, but there also exists for forest fire or air crashes. The special fire-fighters garment market has been described in the Personal Protection Equipment section.

The rescue of survivors also requires additional equipment such as special vehicles for cutting reinforcing concrete and structural steel and removing debris and rubble. The equipment is of the same kind used by public works and demolition industry and has a dual nature.

First response healthcare

First response healthcare requires advanced medical posts or even field hospitals for large disasters. Equipment includes first aids to stabilise injured people and being further aid required carry them to a hospital. Products include burn care, bloodborne pathogens care, cardiopulmonary resuscitation and automatic external defibrilators, eye care, ointments, antiseptics, pain relief products, over the counter medications, protective equipment including gloves, examination gloves, ear protection, head and body protection, respirators and face masks, safety glasses, etc. Such kind of standard

equipment is provided routinely by the health care industry. Hence, a market segment in this area for security can be hardly considered.

Affected public and crisis responders have to deal with different forms of (post-traumatic) stress disorders and other psycho-social strains, thus requiring quick and professional psycho-social support to preserve their mental health. Yet, this support is one of the activities of professional psychologists to care mental distress and is not mainly bound to security issues.

The CBRN case

CBRN attacks require therapies to treat contaminated people. For example, radioprotectants that block internal absorption can help against acute and long-term radiation exposure[169] (Civitas, 2007). Drugs, antibiotics and antivirals can be administered to reduce or palliate effects of chemical or biological agents, and vaccines can be used to avoid further spread of a biological disease.

The biotechnology and pharmaceutical industry is the main supplier of these remedies. The development of drugs and vaccines is a very risky business, since it requires large investments. A new drug may cost hundreds of millions euros and may take years until it is ready to use. Rate of failure is considerably high and return of investment of commercialised products is not always assured (NRC, 2002:99). Therefore, the traditional market mechanism for the development and production of pharmaceutical products to respond to a terrorist attack may consequently fail since incentives for the private industry as we have seen are few. Even success may not be welcome with a large demand. Only products with potential application to natural and common diseases may have a better chance to receive private funds for research (NRC, 2002:100).

Governments are able to remedy this market failure. This is the reason of project Bioshield signed the July 21, 2004 by President Bush. The main goal of the project is: (a) relaxing procedures for some CBRN terrorism-related spending, including hiring and awarding research contract; (b) guaranteeing a federal government market for new medical countermeasures; and (c) permitting emergency use of unapproved countermeasures. Total appropriations are $5.593 billion for fiscal year 2004 to 2013. The act is designed to guarantee companies that the government will buy new successfully developed CBRN countermeasures for the Strategic National Stockpile[170]. This guarantee reduces the market risk for the company, but does not affect its exposure to development risk, i.e. the risk that the countermeasure will fail during testing and be undeliverable. Critics of such programme suggest that because of the high product failure rate in advanced development, the government will inevitably fund unusable products (Grotton, 2009). There is no similar programme in the EU.

[169] Like Prussian blue to help block internal absorption of cesium-137, calcium- and zincdiethylenetriaminepentaacetate (Ca-DTPA and Zn-DTPA) to treat internal contamination from radioactive elements, and potassium iodide (KI), which blocks thyroid radioiodine uptake. However, they are not effective to treat acute radiation sickness, guard against DNA mutations, and mitigate other health consequences of acute radiation exposure (Civitas, 2007:13).

[170] Rapoport (1999) questions the rationale of the stockpiling of vaccines and drugs because toxins and pathogens used in an attack will be very different in the next and they usually are only effective for the agent they were designed for.

Logistic support

Logistic support is required to attend people after a security incident, especially in the case of large and catastrophic incidents. This support may include: (a) transportation capabilities to move people to a safe place; (b) infrastructures like public buildings to provide shelter and a living and sleeping place to the population; (c) an emergency supply chain of food, water and health services.

Ambulances are the main equipment required to transport injured people to hospitals after a security incident. Such vehicles are the same used for medical emergency services. They are supplied by specialised companies that adapt the vehicle inside from different manufacturers to integrate the first aid medical equipment to the special needs of the purchasing health care organisation in a similar way as fire-fighting equipment. There are a large number of industries operating in this market[171].

CBRN decontamination

Decontamination of personnel, equipment and facilities is an essential step in the response and recovery of an attack. The complexity of this task may delay normalization of activities and create social disruption and economic losses in particular when the strictness of the environmental regulations that govern post-attack decontamination and reoccupation are high (Zimmerman and Loeb, 2004). Non-volatile chemical agents, radiological particles and some persistent biological agents require decontamination processes that may take months or even years (Rossof, 2007). Wind dispersion and chemical reactions with the surface in contact may hinder the decontamination process.

Decontamination aims at destroying, reducing or removing contaminant to an acceptable level. Main methods consist of physical, chemical and thermal processes. Physical processes are used to remove CB agents from surfaces. High pressure systems, sorbents (simple inert), and solvent washes are examples of physical processes. Chemical processes involve the use of reactive or catalytic chemicals to neutralize CB contaminants. Thermal processes remove CB contaminants through vaporization. Means to detoxify the agent or store the contaminated material in a safe place are necessary. Shelters are also needed to host the decontamination processes (NIJ, 2001).

Main limitations of decontaminants are that they do not fully neutralize all the agents, and they are not completely safe. Strong neutralizers tend to destroy parts of decontaminated element. Some decontaminants have shelf-life or storage issues, some are flammable, and most are not friendly to the environment (ESRIF, 2009:146). Such limitations suggest potential research needs in this area.

European companies operating in this area are Kärcher Futuretech, OWR AG, Jervän SEDAB, NBC Sys or Hughes safety showers. USA companies operating in this field are Bioquell, Inc., Certek, Inc., and CDG Research Corporation, or Advanced Sterilization products (Ethicon Inc.). Due to the specificity of the demand, this industry is likely to be of small size. Products have dual use either to manage industrial accidents or decontaminate hospitals.

[171] Rettmobil the large Europe's largest exhibition of rescue and mobility vehicles and equipment in 2010 hosted 350 exhibitors from 12 European countries.

Coordination and management

The coordination and management of emergency operations pose some issues. First, response to disasters can only be anticipated, and so planned, up to a certain point. Yet despite the sheer diversity of disasters, it would seem that certain generic conditions tend to apply that make for more effective responses. Beyond that point, however, effective response depends crucially on the ability of all concerned to react flexibly and in an innovative fashion to the situation as it unfolds since each disaster will to some extent be unique (OECD, 2003b:182). The availability of means to gather and share information about the overall situation, authorise and coordinate the use of resources into something like a supply chain, and track execution to adjust and alter prior plans and commitments based on the evolving situation can make the difference in the effectiveness of the response[172].

Systems able to support these essential capabilities, popularly known as Command and Control systems, are based on a network of communications and information systems. The communication capabilities (voice and data) facilitate the sharing and distribution of timely and accurate information to the various response teams and agencies involved –as well as the general public–, keeping them aware about the extent of the damage[173], continuing threats and actions to take. Such networked environment facilitates cooperation and joint / distributed decision improving the consistency and coherence of the response and speeding up the response time and action to save life, limb and property and curtail economic and environmental damage. Specialised software is also used for precise location of personnel and assets based on maps and cartography.

Desired features of the communication's backbone are robustness, easy deployment, mobility, priority-sensitive and large broadband. Professional Mobile Radio networks provide some of these features by means of redundancy, use of specific frequencies of the spectrum, as well as special services to subscribers like group call, emergency call, direct call or broadcast call (Ecorys, 2009:217). These networks have also encryption capabilities to ensure confidentiality. The infrastructure is composed of radio base stations, switching and control nodes, managing centres, applications, and interface elements. TETRA is the most extended standard, however there are others operating in the market. Motorola is the leader on the high-end PMR market (50%), followed by EADS (20-25%). Other European players are Thales (FR), Selex (IT), Rohill Engineering B.V. (NL), Sepura Ltd. (UK), Frequentis (AU), Rodhe Schwarz (GE), and Teltronic (SP). There is a market pressure to increase bandwidth (to support for example videoconference). Technologies like secure-WiFi and secure-Wimax or IP-based communications like Thales are pressing to enter into this market (Ecorys, 2009:230). Communications satellites may provide broadband communication deployable in a very short time to back up / substitute (damaged) terrestrial communication infrastructure. However, they are of no use in enclosed and indoor areas and allow an inferior number of parallel users and connections. Moreover, the cost of this service is so far too expensive.

[172] According to NRC (2002:277) the accumulated body of research of natural disasters reveals all too many instances of scarce information, deficient communication, poor coordination, and jurisdictional conflict among nominally coordinating organizations.

[173] For example, access to list of injuries and casualties of relations and friends and their whereabouts.

The capability of these systems to interoperate across jurisdictions and among emergency service units –like fire, police, or medical– is an essential requirement. However, acquisition of this communications equipment is characterised by local, agency-level acquisition and deployment driven by local budgets from local taxing bodies and by local priorities. The outcome is that often different public safety agencies are unable to communicate and share information with each other. Since interoperation is not typically considered when these systems are acquired, it is not surprisingly that often limited technical interoperability exists (Rao *et al.*, 2007:41). In brief, lack of standards and coordination mechanisms combined with a fragmented demand may be detrimental, at the end of the day, for the development of the market.

This is an area of intense research due to large market opportunities of products with improved capabilities and is a priority in the ERFP. Examples include reliable radio communications inside (destroyed) buildings, software defined radios[174], data fusion and data mining tools, decision support to select the best course of action, deployable sensor networks for awareness, damage assessment, and computer-assisted disaster simulation tools to predict the evolution of the situation and point out new impending threats and risks. Most of these developments are still in the infancy stage being implementations of limited functionality.

The purchaser of this kind of systems is the Public Administration. Frost & Sullivan (M453-16) estimated the European market revenues around €1.5 billion in 2009. Suppliers of Command and Control systems are usually prime contractors with strong capabilities in ICT and system integration. Thee large similarities with defence Command and Control systems makes that the main suppliers in this market are frequently defence companies as the ones we have mentioned in border surveillance.

FORENSICS

Forensics refers to the set of activities aimed at investigating crimes and terrorist events and getting evidence which combined with intelligence information may help to identify perpetrators and present the case to the Court. Forensics involves a large set of disciplines that includes general toxicology, firearms / tool-marks, questioned documents (e.g. forgery and alterations, handwritten signature), trace evidence (e.g. hair, textile fibres), controlled substances, biological/serological screening, fire debris/arson analysis, impression evidence (e.g. fingerprints, shoe/tire prints), blood pattern analysis, crime scene investigation, medico-legal death investigation, and digital evidence (NIJ, 2006).

Equipment

Most common forensic tools are laboratory equipment for analysis such as equipment to test the presence of blood fluids, DNA[175] analyser, blood and urine analysers, magnifying glasses and microscopes, photographic and digital imaging equipment,

[174] These radios are able to use different waveforms and communication protocols due to programmable hardware.

[175] DNA identification is based on techniques using a specific part of the *non-coding* DNA regions (regions that do not bear genetic information). It is mainly used in forensic laboratories as it does not allow real-time identification. DNA identification is expensive (around $4.500), time consuming (4-5 hours) and needs skilled human intervention (IPTS, 2005:17).

equipment for detecting the presence of different substances as drugs or poisons, equipment for collecting items of evidence, software tools to examine digital evidence stored in computers and electronic devices[176], laser equipment for diagramming crime scenes, x-ray screeners to locate radio-opaque objects like bullets, etc.

This kind of equipment stems for different sources, mainly from scientific, medical, biological, chemical and industrial laboratories without specific differences. The demand of this equipment can be considered rather low in comparison with other security equipment, with the exception of Automatic Fingerprint Identification System (AFIS). The main difference of these systems is that they do not require real time response, but a high level of accuracy to determine whether a person is in a database of several million records (NTSC; 2006:8 and 80). Only a short number of companies have the capability to develop such systems.

Current limitations of forensic technologies to identify perpetrators of radiological and nuclear attacks (DSB, 2004:14) are stimulating research in this area in the USA (Civitas, 2007:13). NRC (2002:8) has also identified attribution gaps in bioterrorism attacks. Yet, no research programme to overcome these limitations has been identified.

Investigation services

Detectives and private investigators are mainly demanded by companies to investigate security incidents such as theft, fraud, due diligence, background checks and system break-ins. There is a European Council of Detectives and Private Investigators. However, the association does not provide any economic information about it or its members. According to Eurostat *sbs_na_1a_se_r2* table investigation activities employs 24,295 people across the EU. Revenues are in the range of €1,217 million.

RESUME AND CONCLUSIONS

This chapter has analysed the different segments into which the security market can be divided. At first sight, it can be observed a market that provides a large variety of security goods and services which do not share any pattern due to their diversity. However, when segment are analysed, a more coherent picture appears where some specific features can be pointed out.

Many security needs are often supported by unspecific products that are sold in other markets, being even security not the biggest demander. This dilutes the identified security market segment into a broader category impeding a deeper analysis. In other cases, the demand is rather small and do not generate large revenues of any economic relevance, being information about them scarce. Government purchases often involve tailor made developments giving way to a new market segment which usually fades after acquisition ends.

It has been shown also in many areas that technology immatureness is impeding the formation of markets. Companies and customers tend to explore these markets through the development of prototypes and pilot projects to assess demand and unfold more advanced solutions. Governments and large companies are the main customer of this

[176] For example: address and phone books, audio/video files, calendars, databases, documents, e-mails, text / voice messages, graphic files, spreadsheets, etc.

R&D market. The formation of these new markets seems often to follow a rather low pace.

Some market segments largely benefit of network economies in which the development of standards do play a key role. Large projects like national identity cards or passports show a large maturation time. Yet, they seem essential for the consolidation of some trade activities like e-commerce.

When we examine capabilities of the European industry, we see a prominence of the industry of the more industrialised Member States, namely the United Kingdom, France, Germany and Italy being ensued by far by other nations like Sweden, Spain or the Netherlands. Other European member states play a marginal role in the security equipment market and often have to purchase the equipment from abroad.

When we compare the industry with other parts of the world, we see that there are important industrial capabilities of Europe in the majority of market segments. However, it seems in many areas that U.S. industry enjoys a technological lead. The United States shows more advanced capabilities such as border control using biometrics, early warning of biological and chemical attacks, radiological detection equipment at ports of entry, baggage inspection using computer tomography, explosives inspection system, customs cargo inspection (e.g. ACE), container security, unregulated border protection (e.g. SBInet), computer security, PMR emergency services, AFIS systems, unmanned air vehicles (UAV), or remedies against chemical or biological agents, to mention the more relevant.

Japanese companies seem to be also very competitive in certain market segments such as biometrics, computer security, or CCTV surveillance equipment. Korean companies, such as Samsung, LG and Hyundai, are also suppliers of security equipment. Finally, Chinese companies are everyday more present in international markets, mainly competing on price rather than on quality. This is the case, for example, of Nuctech, a company specialised in inspection equipment.

V. THE ROLE OF THE GOVERNMENT

This chapter analyses the fundamental role of government in the security field. The four main roles are as entrepreneur, main supporter of the industry, main purchaser of equipment, and market regulator. All these roles have a relevant effect on the market in both the demand and supply side, which may even extend to the whole economy, as for example some security policies with large impact on transport and trade. EU legislation with impact in the security market is shortly described. EU and European unilateral initiatives are also briefly commented. Since government behaviour may generate rents, industry may behave strategically with the aim to appropriate such rents. Such conduct, with a potential effect on market performance, will be analysed in chapter VII.

GOVERNMENT AS ENTREPRENEUR

Public ownership is more uncommon in the European security market than in the defence market. Ownership, however, appears in companies that operate simultaneously in the security and defence market as may be the case of Thales, Finmeccánica, or EADS. Ownership do also appear in companies involved in the production of documents hard to counterfeit like national identity cards, paper money, or software certificates such as *Bundesdrückerei* GmbH, the *Fabrica Nacional de Moneda y Timbre* in Spain, or the *Istituto Poligrafico e Cecca dello Stato* from Italy. The desire governments of keeping a tight control of a business strongly related to national sovereignty is probably the main rationale to explain public ownership. Yet, such ownership may nourish inefficiency due to the absence of important incentives such as capital market pressures in the form of the threat of take-overs and bankruptcy and the lack of competition in the products or services provided (Tisdell and Hartley, 2008:chapter 8).

INDUSTRY ASSISTANCE AND R&D FINANCING

The security industry, as any other kind of industry, may receive State aids according to regulations established by the European Commission whether regional or horizontal aids such as R&D, training, SMEs and so on. The most important source of aids is probably R&D where the state finances totally or partially the project, or provides tax relief for amounts allocated to this activity. In this way, government raise incentives for industrial innovation, an activity that is frequently underprovided by the market mechanism (Arrow, 1962) achieving in such a way a more optimal outcome from the societal point of view.

As we have seen in chapter II, outlays of member states for security R&D are not too high with the exception of Germany and UK. The German national Research programme for Civil Security has a funding of €150 for the period 2007-2011. It focuses in the protection of the transport and the supply chain as well as the protection and rescue of people. The EU is been very active in coordinating and financing security research with European dimension. This support started with the Preparatory Action on Security Research (PASR) and the Security Programme of 7th European Research Framework Programme, which finances DG Enterprise and Industry. These research activities are done through European consortia formed by Member States companies. Advices on research topics was given by the European Security Research Advisory

Board (ESRAB) and its successor the European Security Research Information Forum (ESRIF) which aims also at collecting and harmonizing needs and priorities on security research across European Member States. A Security Advisory Group with a relevant participation of the industry provides advice in the preparation of the programme calls. The active role of industry in setting this agenda is critically assessed in Hayes (2009).

Industrial state support, however, has a potential distorting effect on competition that may have undesired effects on market performance. This question is analysed in more detail in chapter VII.

LARGE PURCHASER

Government plays an important role in the security market, since it is the main buyer of some security goods and services and sometimes the unique purchaser (monopsony). Its power to purchase novel and advance products and its capability to finance precompetitive R&D through public procurement, can help to ensure the rapid transfer of the best results of innovation to market, breaking the barriers of companies to invest in the production of new equipment and facilitating their achievement of economies of scale. This can be done financing pilot projects to validate solutions that, being successful, may be followed by large purchases. The returns received by the industry will help to reduce prices, and raise innovation and the company portfolio. This will contribute to stimulate the demand of similar or derived products by (private) market agents and thus contribute to the consolidation of new markets (e.g. computer security). A demanding and sophisticated buyer, as governments can be, able to request the fulfilment of tough standards may improve the international competitive position of the industry (Porter, 1990:651). A paradigmatic case may be for example biometrics; a technology that was pushed forward by the FBI in the USA for crime investigation during the decade of the 70s and now is being massively used in national identity cards and e-passports as well as access control for private organisations.

REGULATION

The security market is an economic sector subject to government regulations. Such intervention is justified when transactions costs and other barriers can lead to significant coordination problems (Coase, 1960), as the case of standards mentioned in chapter III. Government regulation may compel the implementation of minimum security measures by market agents and in some cases like air transport the use of qualified equipment. These norms stimulate the purchase of security goods and services when they provide effective solutions in terms of fewer resources, less inconvenience and enhanced security. Regulations may be accompanied with aids or incentives to soften the burden of implementing such measures, such as low interest loans or tax deduction of the amount invested in security when public security is at stake. This is the case of TSA that, according to Ecorys (2009:104), provides a reimbursement of $375,000 per facility for Certified Cargo Screening Facilities (CCSF) under its Certified Cargo Screening Program (CCSP). Another example is the security fee charge of flying tickets since 9/11 in the USA to finance improved security measures.

Regulations concerning minimum security practices

Examples of such regulations are many. For instance, inspection of personal belongings and passenger identity verification are mandatory in air transport. Regulations for the protection of dangerous goods[177] define requirements for handling facilities and transportation, such as physical protection, access control and strict accounting methods to avoid the illegal stealing, selling and trafficking of such material. Nuclear power plants have strict security requirements defined by the IAEA. Fire detection and protection measures are compulsory in the construction of new buildings. CBRNE capabilities for civil protection are stated in Decision 2008/73/EC. Directive 2008/114/EC states two main obligations to EU critical infrastructures: the establishment of an Operator Security Plan and the designation of a Security Liaison Officer, however it does not state any specific investment obligation in security goods and services.

Regulations need to be carefully assessed since they may have several unintended consequences on production capability, competitive position and innovation, whose outcome may be an overall reduction in social welfare that cannot commiserate with the security improvement (Ghose and Rajan, 2002). For example, mandated air cargo inspection may place an undue financial burden and reduce the competitive advantage – speed– that it has *vis à vis* other modes of transportation (Riley, 2006). The rather inflexible nature of regulations may easily lead to a misallocation of resources (Spulber, 1989:92).

Regulations concerning the provision of security goods and services

Government regulation may call for specific conditions to operate in the market that are not usually requested in other economic sectors, as is the case of manned guarding services companies. Such regulation assures the quality of service within the market and avoids negative effects on customers and other collateral effects on society such as an improper management of a security incident. Government monitors compliance with regulatory requirements and can rescind or suspend a company's license or exact fines if the company infringes operating provisions. This intervention is required, because the market mechanism may be unable to crowd out of poorly functioning companies, especially in a growing industry. Keen competition may, in fact, force margins down to the point where companies are strongly motivated to undercut competitors by paying under-award wages and misrepresent service levels (Van Steden and Sarre, 2007).

Government may also set regulations on performance, quality or fulfilment of standards of products and services without which they cannot be sold. For example, EU security equipment that process and store personal information, as is the case of surveillance and video recording equipment in public areas shall fulfil the rules related to the protection of individual privacy rights as stated in the data protection Directive.

Regulation demands the monitoring of goods and services provided in the security market. This means on the one hand that the industry will undergo additional costs and delays to have their products and services certified, and on the other hand a social cost in terms of government organisations or agencies in charge of this monitoring that should be netted out from the benefits of compliance with the regulation.

[177] Like explosive precursors, chemical agents, collections of dangerous pathogens and cultures, and fissile and radiological materials.

International conventions and resolutions related to terrorism and organised crime

Many security regulations are the result of agreements within international regulation bodies with a direct or indirect effect on the security industry. The following table shows the most relevant.

ICAO	1963	Convention on Offences and Certain Other Acts Committed on Board Aircraft.
ICAO	1970	Convention for the Suppression of Unlawful Seizure of Aircraft.
ICAO	1971	Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation.
UNO	1974	Convention on the Prevention and Punishment of Crimes against International Protected Persons, including Diplomat Agents.
UNO	1979	International Convention against taking of Hostages.
IAEA	1980	Convention on the Physical Protection of Nuclear Material.
ICAO	1988	Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation.
IMO	1988	Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.
IMO	1988	Convention for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf.
IMO	1988	Convention for the Safety of Life at Sea (SOLAS).
ICAO	1991	Convention on the marking of Plastic Explosives for the Purpose of Detection.
UNO	1997	International Convention of the Suppression of Terrorist Bombing.
	1999	International Convention for the Suppression of the Financing of Terrorism.
UNO	1999	Security Council Resolution 1267. Imposing limited air embargo and funds and financial assets embargo on the Taliban.
UNO	2000	General Assembly resolution 55/25. Convention against Transnational Organized Crime.
UNO	2001	UN Security Council Resolution 1373: Combating Terrorism.
IMO	2002	International Ship and Port Facility Security Code (ISPS), amendment to the Safety of Life at Sea (SOLAS) Convention to enhance the security of ships and port facilities. IMO (2002). Entered into force in July 2004.
UNO	2003	General Assembly Resolution 58/4 Convention against Corruption.
UNO	2004	UN Security Council Resolution 1540: Counter proliferation initiative on WMD.
UNO	2005	International Convention for the Suppression of Acts of Nuclear Terrorism.
UNO	2005	UN Security Council Resolution 1617: Threats to international peace and security caused by terrorist acts.

Table 16. International Security Agreements

European initiatives

The EU promotes measures aimed at improving the security of the whole Union based on the TFEU where it is stated: an area of freedom, security and justice (article 67); a framework for administrative measures to combat terrorism money laundering (article 75); judicial cooperation in criminal matters (article 82); minimum rules concerning the definition of criminal offences and sanctions with cross-border dimension (article 83); measures to promote and support the action of member states in the field of crime prevention (article 84); Eurojost mission (article 85); European Public Prosecutor's Office from Eurojust (article 86); police cooperation (article 87); Europol mission (article 88); civil protection (article 196), and a solidarity clause in case of a terrorist attack (article 222).

The EU action materialises in leading and coordinating activities of member states. It involves the launching of security programmes, the promotion of research and development, the enactment of directives and regulations that shall observe member

states, and the development of standard. Such action has a relevant impact on the industry.

The development of directives and regulations is essential for two main reasons. On the one hand they are needed to avoid weak points due to different level of protection stated by member states like the ones agreed by the European Civil Aviation Conference. They are developed as a consequence of international agreements on security issues. On the other hand, common or harmonised rules are needed to provide a level playing field where market agents have same opportunities, otherwise differences may negatively impact on competition since companies will endure different burdens (and overhead costs) for providing the nationally stated security level.

In the following tables EU main general policies and strategies, directives and regulations are depicted.

COM (2001) 298 final	Network and Information Security: Proposal for a European Policy Approach.
	Council Framework Decision of 13 June 2002 on combating terrorism.
	Council Resolution of 28 January 2003 on a European approach towards a culture of network and information security.
COM (2002) 233 final	Towards integrated management of the external borders of the member states of the European Union.
COM (2004) 221 final	Communication from the Commission to the Council and the European Parliament on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information.
COM (2003) 63 final	Proposal for a regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency.
COM (2004) 262 final	Communication from the Commission to the Council and the European Parliament on the prevention of and fight against organised crime in the financial sector.
COM (2004) 698 final	Communication from the Commission to the Council and the European Parliament – Prevention, Preparedness and Response to Terrorist Attacks.
COM (2004) 700 final	Communication from the Commission to the Council and the European Parliament on the Prevention of and the Fight Against Terrorist Financing.
COM (2004) 701 final	Communication from the Commission to the Council and the European Parliament on the Preparedness and Consequence Management in the Fight against Terrorism.
COM (2004) 702 final	Communication from the Commission to the Council and the European Parliament. Critical infrastructure protection in the fight against terrorism.
	The European Union Counter-terrorism strategy 14469/4/05 (2005).
	EU Plan of Action on Combating Terrorism 9809/1/05 (update of 2001 Action Plan Against Terrorism)
COM (2005) 113 final	Proposal for a Council Regulation establishing a Rapid Response and Preparedness Instrument for major emergencies.
COM (2005) 232 final	Developing a strategic concept on tackling organised crime.
COM (2005) 565 final	Global Monitoring for Environment and Security (GMES): from concept to reality.
COM (2005) 576 final	Green Paper on a European Programme for Critical Infrastructure Protection.
COM (2006) 251 final	A strategy for a Secure Information Society – "Dialogue, partnership and empowerment".
COM (2006) 474 final	Green paper on detection technologies in the work of law enforcement, customs and other security authorities.
COM (2006) 688 final	On Fighting spam, spyware and malicious software.
COM (2006) 733 final	Reinforcing the Management of the EU's Southern Maritime Borders.
COM (2006) 786 final	On a European Programme for Critical Infrastructure Protection.
COM (2006) 787 final	Proposal for a Directive of the Council of 12 December 2006 on the

	identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.
COM (2007) 96 final	Radio Frequency Identification (RFID) in Europe: steps towards a policy framework
COM (2007) 267 final	Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime.
COM (2007) 399 final	Green paper on bio-preparedness.
COM (2007) 651 final	Communication from the Commission to the European Parliament and the Council on enhancing the security of explosives.
COM (2007) 654 final	Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes.
	Council Decision on 5 March 2007 establishing a Civil Protection Financial Instrument (2007/62/EC).
	Commission Decision 2008/73/EC of 20 December 2007 amending Decision 2004/277/EC, Euratom as regards rules for the implementation of Council Decision 2007/779/EC, Euratom establishing a Community civil protection mechanism.
	Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
COM (2008) 68 final	Examining the creation of the European Border Surveillance System (EUROSUR).
COM (2008) 69 final	Preparing the next steps in border management in the European Union.
COM (2008) 130 final	On reinforcing the Union's Disaster Response Capacity.
COM(2008) 360 final	On a common immigration policy
COM (2009) 149 final	On critical Information Infrastructure Protection. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.
COM (2009) 273 final	On Strengthening Chemical, Biological, Radiological, and Nuclear Security in the European Union – An EU CBRN Action Plan.
COM (2009) 538 final.	Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain.

Table 17. General policies and strategies

1989/686/EEC	On the approximation of laws of the Member States relating personal protective equipment (note: does not include law and order PPE).
1995/46/EC	On the protection of individuals with regard to the processing of personal data and on the free movement of such data.
1999/93/EC	On a Community framework for electronic signatures.
2000/31/EC	On certain legal aspects of information society services in particular electronic commerce in the internal market.
2001/97/EC	Amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.
2002/19/EC 2002/20/EC 2002/21/EC 2002/22/EC	Access, authorisation, framework and universal directives on electronic communications networks and services.
2002/58/EC	Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
2004/82/EC	On the obligation of carriers to communicate passenger data.
2005/60/EC	On the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
2005/65/EC	On enhancing port security.

2006/24/EC	On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
2008/68/EC	Inland transport of dangerous goods. This Directive replaces Council Directive 94/55/EC, Council Directive 96/49/EC and Council Directive 96/35/EC.
2008/114/EC	On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Table 18. EU Directives

45/2001	On the protection of individuals with regard to the processing of personal data by the Community institutions and on the free movement of such data.
2580/2001	On specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
178/2002	Laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.
2320/2002	Establishing common rules in the field of civil aviation security. Replaced by Regulation (EC) No 300/2008 (the latter being supplemented by Regulation 272/2009).
622/2003	Measures for the implementation of the common basic standards on aviation security. Amended by Regulation 1546/2006 and replaced by Regulation 820/2008. The latter replaced by regulation 185/2010.
1217/2003	Laying down common specifications for national civil aviation security quality control programmes.
1486/2003	Laying down procedures for conduction Commission inspections in the field of aviation security.
725/2004	On enhancing ship and port facility security.
884/2005	Laying down procedures for conduction Commission inspections in the field of maritime security.
648/2005	Amending the Community Customs Code and introduction of Authorized Economic Operators (AEO) and 24 hours advance notification.
1717/2006	Establishing an Instrument for Stability.
1781/2006	On information on the payer accompanying transfer of funds.
1875/2006	Amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code.

Table 19. EU Regulations

Reg. (EC) 1683/1995	Laying down a uniform format for visas and successive amendments.
Reg. (EC) 1334/2000	Setting up a Community regime for the control of exports of dual-use items and technology.
Reg. (EC) 1030/2002	Laying down a uniform format for residence permits for third country nationals and successive amendments.
	Proposal for a Council regulation amending (EC) 1683/95 (uniform format for VISA) and (EC) 1030/02 (uniform format for residence permits).
	Council decision (2004/512/EC) establishing the Visa Information System (VIS).
Reg. (EC) 2252/2004	On standards for security features and biometrics in passports and travel documents issued by Member States.
	Commission Decision C(2005) 409 on the EU – Passport Specification

	(28.02.2005).
	Commission Decision C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.
	Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band.
	EU – Passport Specification. Working document (EN) 28/06/2006.
Reg. (EC) No 767/2008	Concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (VIS regulation).
	Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, incorporating in the framework of the Union important provisions of the Prüm Treaty dealing with police co-operation and information exchange on DNA-profiles, fingerprints and vehicle number-plates.
	Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.
Reg. (EC) 444/2009	Amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

Table 20. Regulations on interoperability and data standardization

Single sided initiatives

Security initiatives without international agreements may have anyhow impact in other countries as is the case of regulations to travel or trade with such country. The USA and the European Union are two examples. Here we mention the most relevant initiatives.

USA initiatives

- The requirement to send airlines electronically the Passenger Name Record (PNR) within 15 minutes of a plane taking off to the DHS Customs and Border Protection[178]
- The Enhance Border Security and Visa Entry Reform Act of 2002 which requires a machine readable passport, if issued before 26th October 2004, and a biometric or e-passport, if issued after 26th October 2006, to enter the USA without visa (US-VISIT program)[179].
- The 96-hour advance notification of vessel arrival to U.S. ports.

[178] A similar requirement exists for sea passengers.

[179] According to DHS (2009:84) US-VISIT leads the collection, maintenance, and sharing of information, including biometric identifiers, on foreign visitors to assist in determining whether the individual should be prohibited from entering the United States; can receive, extend, change, or adjust immigration status; has overstayed or otherwise violated the terms of admission; should be apprehended or detained for law enforcement action; or needs special protection or attention (e.g. refugees). US-VISIT provides identity management and screening services, offering diverse capabilities, including timely biometric and biographic matching functions to other department stakeholders for immigration and border management as well as other, federal, state, local, and international stakeholders. The program is also charged with the developing of a comprehensive biometric exit solution that will capture biometric information from travellers as they exit the USA. The program was awarded to a consortium led by Accenture in 2004.

- The 24-hour rule advanced manifest rule, launched in 2002 that requires vessel carriers to transmit such data to the CBP Automated Manifest System 24-hours before U.S.-bound cargo is loaded onto a vessel at a foreign port[180].
- The Container Security Initiative (CSI) aimed at inspection of containers in the port of origin before delivering it to its final destination is the United States[181].
- The Customs-Trade Partnership Against Terrorism (C-TPAT)[182] and the Known Shipper Program, a similar version of C-TPAT for air cargo.
- The DOE's Megaports Initiative that provides foreign nations with radiation detection devices to prevent the smuggling of a nuclear weapon or a radiological dispersion device in the United States (GAO, 2008:6).
- The Security and Accountability for Every (SAFE) Port Act launched in December 2006 is aimed at improving maritime and cargo security through enhanced layered defences. A key provision of this program is the Secure Freight Initiative (SFI), a follow up of CSI and the Megaports Initiative, aimed at improving the current container scanning capability through radiation portal monitors, non-intrusive imaging and optical character recognition.
- The Automated Commercial Environment (ACE) trade processing system.

EU initiatives

- The Authorised Economic Operator (AEO) is a similar version of USA C-TPAT.
- The European Passenger Name Record (PNR).

Some of these initiatives do impose an important burden to foreign countries wanting to trade with the USA and Europe in terms of investments to implement measures or transport delays (increased inspection for merchandise that do not follow security rules). For example, a 100% inspection of U.S. bound containers on maritime transport will raise about a 10% the transport cost according to PRC (2009). These measures consequently have a negative impact on trade that will differ depending of the kind of agent.

RESUME AND CONCLUSIONS

---

[180] The cost of the measure was estimated in 5-10 billion year according to OECD (2003c:48).

[181] The main goals of this initiative launched in 2002 are: (a) to identify high-risk containers using automated targeting tools, (b) pre-screen and evaluate containers before they are shipped, (c) use technology to quickly pre-screen high risk containers, and (d) use smarter, more secure containers in order to avoid tampering. As of August 2006, CSI was operational in 44 ports in Europe, Asia, Africa, the Middle East and America (US CBP, 2006). The EU and the US signed an agreement on April 22, 2004 expanding customs cooperation to trade security.

[182] The goal of this programme launched in April 2002 is to push responsibility for cargo security onto stakeholders in the supply chain. C-TPAT is a voluntary program that shippers and carriers can enter to assure CBP that they have put into place the best security practices for the packing, tracking and distribution of all containers and goods en route to the US. In return shippers and carriers are rewarded through quicker processing (e.g. fast lanes) and reduced probability of inspection delays (CBP, 2004). Examples of good practices include: web enabled cameras to monitor manufacturing and the loading of goods onto trucks; credentialed drivers with satellite tracking of trucks to identify deviations from prescribed (and randomly selected) routes; electronic truck locks that can raise and alarm if improperly accessed (Willis and Ortiz, 2004). Such measure, however, will have a different impact between shippers, intermediaries and carriers depending on their current level of implemented security measures, mainly against theft that will impact on their competitive advantage (OECD, 2003c: 52).

In this chapter the important role of government in the security market has been analysed. Four main roles plays the government in the market: entrepreneur, supporter of the industry, purchaser and regulator. Government entrepreneurship is less prominent than in the defence market. It focuses in the development of secure documents. Government is the main supporter of the industry through the awarding of different aids where R&D aids have special relevance. Apart from some member states, the EU is especially active in financing projects of European dimension, nonetheless at the large scale of the USA. Government is also a large purchaser of security products and services this helping to create and consolidate some market segments.

Government is also a market regulator. On the one hand, it sets minimum security requirements that stimulate the demand of products and services as for example manned guarding services. And, on the other hand, it sets minimum quality standards of security goods and services as for example cargo inspection. Main international and European agreements and regulations with some impact in security are shown in different tables. As it can be seen, the European Union is particularly active in the development of regulations, directives and standards (see also last section of chapter III). All of them have an impact on industry.

Government security initiatives may have economic impact on foreign countries. They may be unilaterally set and create a burden, in terms of higher transaction cost, that will suffer those who have relations with such country.

VI. MARKET STRUCTURE

This chapter analyses the structure of the security market after having studied with some detail the basic market conditions, the main market segments and the role of government. Questions that will be addressed are buyers and sellers; conditions with influence on the structure like entry barriers, product differentiation or cost advantages; industrial concentration, and the role of imports.

The analysis of the structure is important since it lays down the degree of competition and the achievement of economies of scale; two characteristics with impact on market performance. An excessive concentration may weaken competition and facilitate, in such a way, the misallocation of resources and a less efficient market. On the other hand, a large market share brings up some important economies related to the firm size that may result in products and services of lower costs and so a better market performance.

As we have seen in the previous chapter the industry related to security is of very different nature, since the products and services it supplies is quite diverse in methods and technologies. Such varied industry explains to some extent the large number of companies in the market and the relatively independence between market segments due to the little synergies that exist in design, production or marketing methods. Nevertheless, some general patterns emerge after a detailed analysis.

BUYERS AND SELLERS

As we have seen in previous chapters the main customers of security products are the public administration, private organisations (mainly companies), and individuals. Public administration and operators of critical infrastructures are the ones who have more resources to spend in security in comparison to private organisations and individuals. Market purchases of the public sector, as opposed to defence, are fragmented between the different state organisations, agencies and critical infrastructures operators thus resulting in a large number of purchasing orders but of smaller value (e.g. first responder equipment). Public administration, infrastructure operators and large companies tend to be well-informed and sophisticated buyers that enjoy an important bargaining power when negotiating supply contracts with the industry, anyhow not to the extent of a monopsony.

The security industry can be sorted out in three different kind of companies. The first kind is companies whose main activity is the equipment manufacturing. They have excellent skills in some niche technologies to design and produce state of the art equipment in large quantities. The equipment, usually very standard, is sold to customers mainly through distributors, retailers and installers since it is and intermediate product of a more complex system, or being the demand too fragmented it is not economical to sell it directly to end users (only for expensive products).

The second kind of companies focuses its business on customers whose security needs are solved supplying complete systems composed of a mixture of different products and services. Core competences of these companies are project management combined with technical expertise to understand client’s needs and offer a complete system with the

desired capabilities. They are able to define the operational concept, evaluate the system feasibility, design and develop prototypes, integrate components and software, manage the full scale production, control quality, deploy and install the system, train the user and provide multi-year maintenance services and in some cases complementary services like system operation. These companies have good skills in negotiation and contracting and are able to manage the large number of specialised subcontractors and suppliers of subsystems and components that the solution requires. Companies with the highest capabilities are the main supplier of governments, infrastructure operators and large corporations, whereas companies with lower capabilities attend less sophisticated and wealthy customers.

The third kind of companies is security services providers. These companies are contracted by organisations wishing to outsource some security services. They perform specialised activities like manned guarding services, operation of alarm system, and remote monitoring.

Consultancy services are also provided in this market, especially in the high-end customer segment. The assessment these companies provide may help to reduce information gaps or asymmetry that security purchasers may experience. They are able to evaluate client objectives and security requirements, write project specifications and support the selection of integrators and vendors.

PRODUCT DIFFERENTIATION

Product differentiation reduces the price elasticity of a good since it is harder to substitute with others, avoiding in such a way a purchasing decision based on price. Differentiation isolates the product to some extent from competence allowing the industry to demand a price premium –i.e. price above marginal cost (Tirole, 1988:277) – increasing in such a way sales and profits. To do so, companies incur substantial R&D and marketing costs reducing bottom line profits.

Market conditions, however, place restrictions on differentiation. On the one hand little diversity is possible among certain products when differences have a marginal value for the customer. In such cases firms may nonetheless seek to differentiate themselves through other means like better services associated to the sale such as marketing, training, support, or after sales services. Advertising or aesthetics may be used also for this purpose but the case is less relevant for the security market where functionality or performance plays a more important role.

On the other hand only few designs are selected even though thousands are feasible *a priori*. This incomplete spectrum of goods is closely related to the existence of fixed costs (capital, personnel, research and development, etc.), because the production of all imaginable goods would imply a huge expense in these costs, and the demand for most of these products would never be sufficient to make them profitable (*ibid.*:278).

Differences are more apparent in the early stage of new equipment. However, as market matures and some designs show a higher value for end-customers, differences tend to play a less relevant role whereas price and the fulfilment of technical standards become more important in the purchasing decision. The achievement of economies of scale also

creates pressure over time for less variety and standardization despite distinct buyers needs.
As has been seen in chapter IV, security products show *prima facie* relevant differences as for example the large variety of explosive trace detectors. Such differentiation may indicate a strong market competition, a relevant role of product quality and performance as well as a relative inelasticity to price. In many market segments, it is noticeable a trend toward the creation of products attempting to outrange competitors' performance and increase market share. Analysing the product variety, there are reasons to believe that, being other things equal, differences tend to be more frequent when development cost are smaller (Martin, 1993:381).

Differentiation occurs also as result of the tailoring process to adapt the security solution to users' needs. These needs translate into operational, functional or environmental requirements (e.g. building perimeter protection) which results in different designs. But even for a single customer potential bidders will propose different solutions in order to maximise the price performance ratio of its providers within the supply chain.

In the case of manned guarding services, differences between providers may be rather small and competition is mainly driven by cost. Conversely, consultancy services exhibit large differences because they are usually tailored to user needs.

Another typical form of differentiation is based on quality dimension when customers have relevant income differences (*ibid.*:295). Such differentiation is clearly reflected in CCTV and alarm systems when customers have different incomes as is the case of large businesses, small businesses and individuals.

ENTRY CONDITIONS

Entry conditions are another important aspect to consider since being difficult they will restraint entry of new companies. A barrier to entry may be defined as a cost of producing which must be borne by a firm which seeks to enter the industry but it is not borne by firms already in the industry (Martin, 1993:174). Large barriers mean that existing players believe they can act without fear of new competition from market entrants, and being few it may suggest that contestability may not be high. This may facilitate the creation of market power that enables companies to set prices above competition level (the more difficult it is to enter a market, the more incumbents[183] can raise price above the competitive level without inducing entry). In such a case, the force of competition cannot be relied upon to ensure optimal market performance.

Entry conditions are mainly driven by the expected post-entry profit. Markets with a large and growing demand will attract new investors, all other things being equal. However, if there are established firms in the market that enjoy relevant advantages over new entrants, expected post-entry profit will be smaller and incentives to enter will not be so high. Main advantages which influence on entry are: economies of scale, product differentiation and absolute cost advantages (*ibid.*: 172).

[183] We will call incumbents to established firms in the market as opposed to new entrants.

It is not just simple these entry conditions which may cause a barrier to entry, but rather these conditions combined with irreversible capital commitments (also known as sunken costs) that will be hard to recover without losses as for example specific assets (e.g. machinery) hard to be reused, or failed R&D cost (*ibid.*:180).

Economies of scale

Economies of scale arise if average cost falls as output rises, and may simply be a characteristic of the technology used (Martin, 1993:173). Economies of high volume production allow a cheaper good due to investments in large fixed costs unaffordable to new entrants. Often, they stem as result of learning curves of larger production that result in improved processes in terms of quality, speed and resource consumption due to an increase in manual, engineering and managerial skills (Tisdell and Hartley, 2008: 144). Economies of scope also arise if large firms are able to bargain with suppliers and obtain inputs at lower cost than small firms as for example electronic components. These economies are common in the case of OEM that produce standard off-the-shelf security equipment such as CCTV cameras, card readers, RFID tags, electronic cards, and sensors.

Research made by Freeman (1986:101) shows that a doubling of output in the electronic industry would result in average costs falling between 20% and 30%. Dowdall and Braddon (2005) even rise this value up to 66%-75%. Since most security equipment is based on electronics, it is reasonable to believe that the security market benefit of such economies. The large size of suppliers of this kind of equipment confirms this hypothesis.

Economies of scale mean that large companies are systematically favoured over small ones that will face larger costs and fewer profits. It would mean also that leading companies may benefit against second entrants that will confront harder conditions, or even no chance. The accumulation of a large capacity allows firms to charge a low price, even if the price is above average and marginal price, and discourage entry, since entrants will not earn profits (Tirole, 1988:306).

Economies of scale, however, cannot realise where production runs are extremely low as occurs in some security markets, whose demand is one-off or small customized batches of 12, 15 or 20 units. This is because manufacturing processes cannot be fully optimised, using for example machinery to automate processes and reduce labour needs, whereas designs may be hardly reusable in new products. In these cases, the efficiency of design and development, rather than production, plays the central role of the supply (Hobday, 1998). These economies arise not only in the production processes, but also in other activities if they are more effective when carried out at large scale such as R&D, marketing, or the management of the supply chain (Martin, 1993:173).

Product differentiation

Buyers might have blunting preferences for established brands and for the products of firms with established reputations. Therefore, entrants would have to spend more than incumbents, per unit of output, to reach the final consumer. Patents might give incumbents temporary legal monopolies over the use of favoured products, which would make duplication by entrants either impossible or possible only on terms of

licenses dictated by incumbents (e.g. biometrics, encryption). Established firms might control access to major wholesale and retail outlets, implying higher per-unit distribution costs for entrants (Martin, 1993:173).

If the current degree of differentiation enjoyed by incumbents depends in part of past design, advertising, and sales efforts, the cost of such activities constitutes a barrier to entry. That is to say costs that must be incurred to create a good reputation, to bear risk of innovation, and to build a scale of operations appropriate to the economical servicing of consumer demands such as the provision of marketing and technical support to operation and maintenance (*ibid.*:174).

Product differentiation often demands in the security market a permanent R&D capacity. It requires investments above a *threshold level* without which it will normally be impossible to develop new products with lead times short enough to survive and eventually grow (Freeman, 1986:146). These differences may be safeguarded by intellectual property rights (IPR), patents and copyrights and hamper rivals' entry. However, such comfortable environment may be crumbled by new competitors through imitation[184] or through the exploitation of new and radical technologies.

Attaining such differentiation constitutes often an insurmountable barrier for new entrants and small companies, which are only able to enter in some market niches upstream of the supply chain. For example in high-end markets incumbents may benefit from domain specific knowledge of systems, procedures and protocols that come only from experience on past supplies. Moreover, demand is often built on legacy dependencies in existing supplies, and in some cases incumbents may have privileged access to *inside information* about government demand. This situation repeats again upstream the supply chain, where new entrants will experience difficulties due to lack of reputation when they try to create links and become suppliers of system integrators (Dowdall and Braddon, 2005).

Absolute cost advantage

Incumbents enjoy absolute cost advantage over entrants if patents or secrets gave them control over the production processes. Incumbents might control access to higher-quality or lower-cost input suppliers. If, as seems likely, the possibility of bankruptcy is greater for entrants than incumbents (banks unable to objectively evaluate the risk), then financial markets can be expected to impose a higher cost of capital on entrants than incumbents[185]. The resulting cost advantage will be greater the more capital intensive production processes are (Martin, 1993:173).

Incumbents enjoy also cost advantages in the management of the supply chain since inputs and intermediate products to manufacture a security system have a large share in

[184] Martin (1994: 373) shows that strong IPR protection is a fleeting advantage. In one of the reports he mentions that 60% of successful patented innovations were imitated within four years of introduction. The second report from a survey of R&D executives concludes that only in a minority of R&D-intensive industries were patents regarded as more important than secrecy, lead time, moving down the learning curve, or sales and service efforts as a way of protecting the competitive advantages associated with new products or processes.

[185] In complex developments sufficient funds and robust financial support is necessary to accommodate the extremely drawn out development and production timeframe and the inevitable gaps between financial investments and returns (Dowdall, 2005).

the final price, a value that often surpass the 50%. Incumbents may have a large knowledge and experience of the supply system and detailed information on capabilities and resources scattered through the supply chain, being able to combine them on a project specific basis to achieve fundamental advantages. This knowledge and experience may help to optimize overall cost because: (a) fewer costs related to the search of suppliers able to provide raw materials or intermediate products is needed, (b) the choice will be better in term of products with good performance and low price, (c) long-term agreements with suppliers may reduce transaction costs. The higher capability of incumbents to manage an international supply chain favours the achievement of cost advantages (see footnote 67).

Sunken costs

Durability and specificity of assets, singly or in combination, give rise to sunken costs. Sunken costs create barriers to entry because entrants must duplicate assets whose opportunity cost is higher than that for incumbent firms and because the assets have limited scrap value which increases the risk of entry (owing to large losses associated with unsuccessful entry). The sunken cost characteristic of the assets also represents a barrier to exit for incumbent firms since the committed assets represent non-recoverable costs (they do not have intrinsic value to other firms). Incumbents are therefore bound to their markets by the inability to divest (Martin, 1993:204).

The amount of capital investment for entering in the security market represents a barrier and explains to some extent the market structure. The large number and small size of installers of security equipment in the residential market is probably a consequence of the limited sunken cost of entry. In effect, products can be bought from a large list of OEMs' manufacturers, skills to design and install the equipment are rather low, and the infrastructure to supply such equipment to local customers can be rather small.

Conversely, the short number of system integrators can be explained by the difficulty to manage the complexity of large projects that requires large investments to be enough efficient and competitive, as can be the case of container inspection equipment. Similarly, a large investment in productive assets is required to manufacture efficiently in terms of quality and cost. This explains the large size and market share of some manufacturers. The cost and the indivisibility of these productive assets make that efficiency is only reached with a minimum production scale. Hence, these costs become a relevant barrier to entry.

Sunken costs explain that market entry is usually made at a relatively small scale, trying to expand over time[186]. It also explains that entry is likely attempted from neighbouring sectors, since entry costs are smaller because companies share similar technologies, production facilities, or sales and distribution capabilities. Such attempts can be more likely when the demand in the new market is growing and there exists some spare development or production capabilities, and the traditional demand is frozen or stagnant. Some illustrative examples found during the survey are:

- Siemens Building Technologies and Honeywell Inc. that come from the electronic and building equipment market.

[186] A minimum scale to achieve an average cost able to successfully compete with incumbents is also required.

- Defence prime contractors with large experience in system integration are leading large security projects such as Northrop-Grumman in the UK AFIS project, or Lockheed Martin in the USA IAFIS system.
- ICT companies like IBM or Cisco are entering in the CCTV market due to the development of IP-cameras (Frost & Sullivan, 2005a:2-34).
- Companies with a large customer base coming from energy, telecom, banking and insurance sectors seeking to complement their portfolio with security services such as EPS in France, Hafslund in Norway or British Gas in UK (Frost & Sullivan, 2006:2-31).

Impact of research and development in entry conditions

Research and development requires facilities such as laboratories, design offices, computers tools, testing facilities and highly skilled personnel that constitute a relevant fixed cost for the industry. These investments, of uncertain outcome and return, raise the minimum efficiency scale, and the capital requirements, thus raising entry barriers to newcomers. These hard conditions are softened when industry benefits from the technological advances that come from other economics sectors, such as video cameras, vehicles or aircraft, which require only slight transformations to be integrated with other components into a security system as for example a truck transformed for demolitions or fire extinguishing. Government may also soften these conditions when they provide aids for this activity, a question that will be analysed in more detail in chapter VIII.

Labour and capital

A specific pattern regarding the intensity of labour and capital in the security market is hard to discern due to the different kind of industries operating in it. Furthermore, no quantitative assessment has been feasible during the survey. However, some patterns can be identified for certain kind of industries.

The massive production of security equipment and the development of complex security solutions are very demanding in capital investments. Mass production usually requires advanced production equipment to satisfy quality standards and reduce the amount and (sometimes) skills of personnel. Even multiple plants may be needed for developing and integrating the different components of a system. The development of complex systems requires also sophisticated equipment for performing the engineering, design, development and test of the system, whereas computer tools are needed to manage the complex supply chain. These needs raise entry barriers into this market. Conversely distributors need a considerably inferior infrastructure to perform its business. These needs still decrease more for small installers of security systems, which needs even less infrastructure.

The development of new equipment is also a labour intensive activity that requires the ingenuity of sophisticated and skilled teams formed by scientifics, engineers, computer programmers and other qualified personnel with high wages this raising fixed costs. Qualification of distributors and installer personnel is considerably smaller.

Companies that provide security services are fundamentally labour intensive with more austere capital needs. Their main investments are armoured cars for funds transport, remote monitoring system for home alarms, personal protective equipment and

communication equipment. Labour cost represents the main proportion of total costs, which includes training that is another relevant cost source in a market with high employee turnover[187]. The weight of personnel cost in the total cost of the service and the limited qualification that security personnel requires help to explain the low wages that are paid in this market segment.

MARKET CONCENTRATION

A market where the industry has a large market share is considered positive since the chance of realizing economies of scale is high. However, research in this field shows that market concentration in most industries appears to be much higher than it needs to be for leading firms to take advantage of all but slight residual scale economies (Martin, 1994:240). Having in mind that large industrial concentration can generate diseconomies of scale and less efficiency as more stages of production are combined in a single management since bounded rationality limits the scope of such management[188], it could be feasible that mergers are more due to strategic motives than efficiency search, in particular considering that it may take years to fully integrate operations and achieve synergies (Martin, 1994:270 and 283). Empirical studies of mergers also produce negative results: they lose market share and suffer reductions in profitability more rapidly than similar firms that do not engage in mergers (Martin, 1993:235).

The existence of many security suppliers integrated into large business groups may endorse the idea that such concentration may be driven by strategic considerations rather than economies of scale. Yet, such concentration shows superior performance. This kind of firms consists of a set of semi-autonomous operating divisions organised on a product basis and is known as the multi-divisional (M-form) structure. Williamson (1985:283) explains that 'this structure removes the general office executives from partisan involvement in the functional parts and assigns operating responsibilities to the divisions. The general office… is supported by an elite staff that has the capacity to evaluate divisional performance. Not only…is the goal structure altered in favour of enterprise-wide considerations, but an improved information base permits rewards and penalties to be assigned to divisions on a more discriminating basis, and resources can be reallocated within from less to more productive uses'. (Martin, 1993:226) resumes saying that these business groups should be thought of as a way of organising transactions that are intermediate between the firm and the market. The firm can economize on the transaction costs that it would have incurred if the transaction had been done through the market, and at the same time, it can avoid the scale diseconomies or control loss that would have occurred if it had expanded internally and performed the transaction within the firm. Tisdell and Hartley (2008:165) confirm also this hypothesis.

As has been said in chapter II, the concentration pattern of the security market in Europe is characterized by a low number of large companies with international and European dimension and a relevant market share. It is followed by medium-size companies operating at national or regional level, and a large number of companies operating in the residential and private companies market. Market share is low in many markets being

[187] According to Eurostat *sbs_na_1a_se_r2* table, the share of personnel costs in production in the private security activities is 64.36% in the EU for 2008.

[188] Coase (1937) cites two reasons of decreasing returns to the entrepreneurial function: the cost of organizing additional transactions within the firm, and the failure to place the factors of production in the use where their value is greatest.

rare a value above 20% (Frost & Sullivan, 2004:3-1). Therefore, there are reasons to believe that concentration is smaller than the aerospace and defence market. Concentration, however, appears higher in certain specialised equipment or components within the supply chain such as cargo screening, CBRNE detectors, or fibres for personal protection (Ecorys, 2009:34). The lack of alternative suppliers helps these companies to negotiate more favourable contracts.

Entry conditions may explain to a large extent this market structure. Economies of scale, product differentiation, and absolute cost advantages tend to favour large firms. Conversely low concentration can be appreciated in market segments where entry is easier as is the case of distributors and installers of security equipment for small businesses or the residential market. Their higher knowledge of local market and higher flexibility provide these companies enough competitive advantages to operate in the fringe against larger incumbents. Start-up companies are common place in new technology-driven market segments such as biometrics or RFID, having the most promising and successful a big chance of being bought by large industrial groups.

Vertical integration

The degree of vertical integration refers to the extent to which successive stages involved in the production of a particular product or service are performed by different firms. Vertical integration may respond to different needs, such as (a) the efficiency increase of integrating successive processes in time and place or economies of information exchange; (b) the saving in transaction cost when the market is not used, such as advertising, inventory, suppliers search, contract negotiation and enforcement; (c) the wish of suppliers in forward integrating to gain access to distribution channels, or (d) conversely firms performing backward integration to guarantee a dependable source or to capture margins normally paid to suppliers[189].

On the negative side, vertical integration may have an adverse impact on efficiency since it can: (a) raise costs when external suppliers can perform more cheaply due for example to economies of large scale production of intermediate products when they are produced for many customers, (b) create inflexibility because the relationship with the supplying unit becomes captive and the market cannot be used to find a more efficient or innovative supplier. Vertical integration may also unfold anticompetitive effects since intermediate product suppliers will have more difficulties to reach the end customer (market foreclosure) and hence it will raise entry barriers, since rivals will need to integrate forward themselves to ensure access to downstream market (Martin, 1993:69).

Patterns of vertical integration are not discernible due to the variety of the security industry. In some cases the end product and a large number of their parts are manufactured internally, whereas in others companies assembly parts provided by first tier suppliers. Yet, integration does not further than two stages of the supply chain. It is reasonable to assume that in-house production will be preferred when its cost is below that of outsourcing, i.e. production plus transaction cost. This internal cost tends to

[189] Strategic alliances, 'teaming' arrangements and other (exclusive and long-term) agreements with preferred suppliers or dealers may be seen as a soft vertical integration.

increase due to the diseconomies of scale of the managerial span of control[190] whilst the digital economy tends to decrease outsourcing cost[191]. Usually core capabilities are preserved, while elements of the value chain that do not require highly specific assets are more easily outsourced (Williamson, 1979).The analysis of Table 21 shows that many mergers and acquisitions do result in vertical integration which is mainly aimed at reaching better consumers or internalising specific capabilities considered essential for business, avoiding in such a way hold-up problems and supply disruptions.

Conglomerates

The suppliers of security equipment in Europe are often divisions of large diversified conglomerates whose core business is rather uniform. Three main reasons explain this structure. The first is the ability of these conglomerates to capture integration economies (economies of scope) associated with the simultaneous supply of inputs common to a number of production processes geared to distinct final firms' products (Martin, 1994:279) such as know-how, specialised indivisible physical assets, and complementarities in production or existing technologies. These synergies seem so far high enough to offset the cost of coordination, compromise, and inflexibility of business strategies for jointly serving different market segments with shared activities[192]. The second reason could be the small size of the security market and the possibility of market fluctuations. As Martin (1993:250) reminds markets for the goods and services of specialised assets are likely to be thin and it is often cost effective for a firm to diversify across sectors in which the assets can be utilized, this providing a kind of insurance against demand changes. The third is the concept of M-firm, already commented. Such internal structure facilitates synergies and cross-subsidisation of activities that may be important in the early stages of the life-cycle of a product.

As could be expected, due to the nature of most security products whose core technologies are electronics, information and communication, these divisions are part of large conglomerates involved in electronic and defence, but also to safety, environmental protection, industrial control, building management, and ICT. This is the case of companies like Tyco, Honeywell, Siemens, Bosch, Smith Detection or General Electric.

Joint ventures

Joint ventures and consortia, which can be seen as some sort of partial or temporal merge, are another figure used to create the industrial structure that large security projects require (e.g. UK IDENT1, Spanish SIVE). This kind of structure is quite common in research projects such as those financed by The European Research Framework Programme, which mainly finances consortia formed by companies of different member states.

[190] This result in a control loss: signals are distorted in transmission from corporate headquarters to the shop floor; supervisors are less effective in monitoring performance the farther removed they are from the level at which productive work takes place (Martin, 1993:214).

[191] As for example CAD design, flexible manufacturing, data communications or electronic commerce.

[192] Flexible manufacturing technology may facilitate the production of different product varieties in the same facility.

Main motives for the formation of joint ventures are: (a) taking advantage of economies of scale; (b) diversifying risk across members; (c) overcoming entry barriers into new markets; (d) pooling complementary bits of knowledge and achieve synergies; (e) allaying xenophobic reactions when entering a foreign market (Martin, 1993: 256 and Ecorys, 2009:227)[193]. All these reasons tend to raise efficiency.

However, *Joint ventures* and consortia may stifle competition when two competing companies decide to form a single consortium for bidding to a supply contract, which may have effects very much likely tacit collusion (Martin, 1993:235). R&D consortia may slow down the innovation pace (fewer research threads), but enhance social welfare since fewer resources are invested and results are available to their members that may compete later on in the post-innovation market (*ibid.*:376). Consortia, however, may not be exempt of rigidities, due to the ex-ante distribution of work between members, which may favour inefficiency (Hartley, 1995:475).

IMPORTS

The capability to import products may play an important role in the market limiting the ability of domestic firms to wield control over price. The existence of foreign competitors with better products may overrun the market when quality or price of domestic manufacturers is not competitive. As we have seen in geographic markets in chapter III, customers of member states may profit purchasing security equipment from other member states or countries outside the European Union. Yet, national security product regulations may put at disadvantage foreign products. Furthermore foreign bidders may be unfavoured in public procurement against proposals that offer a large work-share to national companies especially in the case of large projects.

Imports of security focus onto two kinds of products. The first kind is first-class systems usually bought from U.S., Japan, Israel or other European countries. A large number of examples can be given such as X-ray equipment for personal inspection (L-3), explosive detection devices (GE), video surveillance cameras (Panasonic, etc.), security software (Trend Micro, Check-Point Software Technologies) or UAVs. These non-EU companies often have commercial offices and other infrastructures within the European Union to better sell their products.

The second kind of equipment imported by Europe usually competes on cost rather than brand quality. They usually come from countries like Taiwan, Korea, or China. They are fundamentally video surveillance equipment and intrusion detection components for residential or small business security. These companies attain competitive advantages in price mainly due to limited research effort (based on licenses or copies of mature products), low labour costs, and economies of large production to supply world markets (Freeman, 1886: 179). This is also the case of DVR for video surveillance that is being produced in Eastern Europe (Frost & Sullivan, 2007: 3-3). This capability is attracting some European companies specialised in security components, mainly for intrusion detection, to outsource their production to these countries (Frost & Sullivan, 2006:1-4).

[193] An example of this kind of joint venture is the supply of a TETRA network to the Guanzhou municipal government awarded to EADS and CETC-7 Ltd. (China Electronic Science and Technology Group Corporation No. 7 Research Institute).

As a final remark, it has to be said that unspecific components that are part of the supply chain of security equipment, such as computers or screens, are often imported.

RESUME AND CONCLUSIONS

This chapter has analysed the structure of the security market. While a general pattern cannot be established due to the diversity of the industry, some driving forces and characteristics of the structure has been described.

As opposed to defence the security market shows a large number of companies with lower concentration levels, both from the demand and the supply side. Companies with a large market share (monopolies or duopolies) only appear in a short number of cases. Instead, markets prevail where few companies together have a large market share. The main reasons that explain the market structure has been identified being especially relevant entry conditions. The main entry conditions are economies of scale, product differentiation, cost advantages, and sunken cost. They are the main reasons that impede the entry and the formation of market with a large number of suppliers. Yet economies of scale seem not so large to talk about a market characterised by natural monopolies.

The different forms of industrial concentration in this market like vertical integration, conglomerates, joint ventures and consortia have been analysed describing their positive and negative effects. Concentration as can be expected is higher when entry barriers are important. Suppliers are often conglomerates (M-firms). Vertical integration of the different stages of the supply chain does not show a clear pattern. This may be due to the varied reasons that may make in-house or outsourcing the most economic option.

A special attention is devoted to the role of imports as a mechanism that improves market competition. More sophisticated products tend to come from USA and Japan, whereas simpler and more mature products come from nascent economies like China, Taiwan or Korea.

As a final conclusion, it can be said that the security market structure gives margin to competition. Yet, product differences and intermediate providers with few competitors may facilitate the creation of some power with a potential negative impact on the market. Whereas a low number of suppliers may exist in some markets, competition however may be rather fierce[194]. In other areas, such as distributors and installers of security equipment, suppliers could be considered excessive since their small size impedes the achievement of economies of scale. Anyhow, the derivation of more solid conclusions requires a deeper analysis and suggests an area of future research.

[194] A confirmation of this fact is the considerable variation in market share with the passage of time that can be observed in Frost & Sullivan security industry reports.

VII. MARKET CONDUCT

This chapter analyses the conduct of the security industry. It attempts to investigate the behaviour of companies and determine whether it has a positive or negative impact on market performance. Pricing, product strategy, and mergers and acquisitions are the main areas that will be analysed.

According to Martin (1994:258), it can be thought, without fear of incurring in error, that behaviour of firms is mainly aimed at maximizing some combination of profits, growth and size, being over the long-run, profit maximization probably the best single explanation of firm behaviour. Profit-maximization firms in an oligopolistic market will engage in strategic behaviour –i.e. the investment of resources for the purpose of limiting rivals' choices (Martin, 1993:46)– to acquire and maintain some market power, provided that the expected profit to be gained from such behaviour exceeds its cost (this cost depending of competition policy) (Martin, 1994:538).

Admittedly, strategic behaviour is strongly limited by Treaty rules that forbid agreements and concerted practices with the aim of restricting or distorting competition such as price fixing, market sharing, cartel and production quota, discriminating commercial policies, or restraints to the free movement of goods, services, capital and technology (articles 101-106 of the TFEU). Yet, as we will see, within this legal framework, there are noticeable opportunities to engage in some form of strategic behaviour.

PRICING BEHAVIOUR

Pricing behaviour is influenced by the market structure. In markets where there are many sellers and buyers the chance to raise prices above marginal cost are smaller than in markets where concentration is high, there are entry barrier to newcomers, products are imperfect substitutes of each other, and demand is inelastic. While collusion agreements are forbidden by competition laws, tacit or implicit collusion may appear more easily where suppliers are few and prices can be agreed without direct contact. In addition, companies may use predatory or exclusionary practices such as temporary price reductions to deter or crowd out the market of competitors. Finally, vertical restraints, such as minimum price, can be applied when security products are sold in retail markets.

Competition

Many security products are sold in markets where the number of sellers and buyers are large enough to assure an independent and competitive behaviour which may even increase with the presence of foreign suppliers. Products features and prices are largely publicized, a reasonable number of substitutes exist, and customers have enough information to make a proper choice. This situation impedes that companies exert some kind of market power, since increases in product price will be immediately responded with a demand fall.

Nevertheless, there are cases where competition may be restricted. The first is within the supply chain, where vertical integration or exclusive deals may close markets to

firms downstream the supply chain and become a source of anticompetitive behaviour that may result in some market power. This may be the case of complex supplies where companies offering intermediate products could be excluded from the supply chain, if competition is not used to choose partners.

The second case is when governments, large infrastructures operators and large companies purchase complex security solutions where only a few or even a single supplier may exist. In such a case, situations of bilateral monopoly may easily appear where the bargaining power of each side will decide the final price. But due to asymmetry of information that both sides manage, a situation of adverse selection may appear since suppliers may have a better knowledge of cost, risks and system performance and the novel system may not be well specified (Laffont and Tirole, 1993:10). This implies that market allocations may fail to be ex-post efficient (Spulber, 1989: 62). Efficiency may also be jeopardised when governments force the participation of non-competitive national industry within the supply chain in international public procurement.

The last case is buying additional products or services related to security equipment already purchased, such as for example maintenance or upgrade, that are tied to the original supplier (no alternative supplier exists). This again facilitates the development of market power.

Collusion

Incentives to tacitly collude –and set a price above marginal cost– may appear in concentrated markets, where products and services are to some extent standardised sharing a similar cost structure and where barriers to entry are high. Tactics such as price signalling, price leadership or pricing rules may be used for this purpose (Martin, 1994:156).

Yet, this practice requires the coordination of sellers that is difficult to achieve when they are heterogeneous or follow very diverse strategies as for example when they compete for a fundamental cost or quality advantage to get ahead of their competitors. In such cases, the chance of adhering to such practice may be small. This is a common case for many security products and solutions that largely differ in performance and cost structure. This practice to be successful requires high entry barriers. Otherwise companies that easily enter the market will challenge the collusive agreement. The case of manned guarding services firms or installers of household security systems where these barriers may be not too high suggest a practice hard to be followed.

The use of open bidding for acquisition of security equipment used in high-end markets like government and large companies discourages also tacit collusion since opportunities to enter the market are sporadic, the premium (e.g. a large multiyear contract) is high, and the auction type method only rewards a single company. Moreover, since information about price cuts may be somewhat hidden or delayed, retaliation is less costly and tacit collusion is harder to sustain (Tirole, 1988:241). Collusion may only appear when consortia are created with the aim of reducing the number of bidders.

Predatory and exclusionary practices

Predatory pricing is aimed at eliminating competitors and increase market share through price reductions. While this practice may be beneficial to the customer in the short term, it may be detrimental in the long run when it crowds out the market of rivals and reduces the number of available choices. This practice requires some kind of entry barriers to be profitable. However, predation is hard to ascertain, price reductions may be attribute to other, more innocent, considerations such as fluctuations in demand or cost, or a normal reaction to a decline in the residual demand curve due to market entry (Tirole, 1988:374).

One form of predation may occur if consumers incur costs in switching suppliers. In such case, incumbents may find it profitable to expand sales, as a way of attracting consumers (who are later *locked-in* by switching costs) and tying them to his brand, leaving fewer customers available for potential entrants and making entry more difficult. This involves some sacrifice of short run profit, a strategic investment in customer base (Martin, 1993:72). Whereas, there is a chance of this practice, as for example home alarm systems, no practical example has been found during the survey.

Predatory pricing may occur when only a short number of firms receive state aids. The worst scenario could be when disproportionate aids are improperly used to cross-subsidise general activities of the company that will allow it to set prices below the ones competitors could offer. However, R&D aids, even if properly granted, may nonetheless provide knowledge and experience which provide the industry with absolute cost advantages over non-awarded competitors. Only a case by case analysis could lay down whether firms conduct follows this practice.

Some kind of predation may occur, especially in public procurement, when companies offer products with overstated performance and undervalued costs. Companies may prefer to incur in some risks when they foresee long-term gains after gaining a monopolistic position once awarded. Such company may recover these potential losses by means of engineering change proposals, system upgrades and future production and maintenance contracts where the bargaining may be more balanced. This may be particularly true in the case of complex products that entail considerable development and integration, and where the cost of substituting the supplier, due to large incurred costs, is too high to become a credible alternative. Such practice is well known in large programmes in particular in the field of defence (Marshall and Meckling, 1962).This overoptimism may be the outcome of the large uncertainties of such programmes that cannot always be anticipated in the initial proposal. However, since firm’s optimism will be financed by the government, penalties for underestimation may be absent (Tisdell and Hartley, 2008:384).

Non-price exclusionary behaviour may occur in the case of setting standards when firms are able to influence standardisation bodies based on proprietary technologies subject to some form of intellectual proprietary rights as is the case of Savi e-seals. This case is closely related to what it is known as predatory innovation, where incumbents enjoying market power define or change product interface, making incompatible the accessories developed by independent manufacturers for the old product (Martin, 1994:484). This is a well known practice in the field of information and communication systems. Frost & Sullivan (2008d:46) report similar practices in the security market. This is the case of companies like Siemens and Honeywell that do prefer proprietary systems and protocols incompatible with the products of other suppliers. In this way, they force end users to

rely on a single provider for the whole range of systems and the associated services they might need, instead of using open products (e.g. IP-based) that are more easily integrated in an IT network. Such behaviour may be more related to companies with a superior overall package in terms of product offering, installed base or reputation (Katz and Shapiro, 2004). Nevertheless, this may be a long-term self-defeating strategy in a market that rewards open systems and interoperability. This explains the preference of new entrants to use a more open approach and benefit from network effects. This is the case of Open Access Alliance Program launched by Lenel (a UTC company) to partner with software developers and hardware manufacturers, or the Open Platform Integration Software XProtect of the Danish Milestone company.

A last form of predation is the industry conduct geared towards achieving long term service contracts with the aim to increase customer loyalty and exclude rivals from the market. For example public/private partnership for the supply of certain services like operation, maintenance, or guarding may vest this strategic behaviour.

Vertical restraints

Vertical restraints are conditions set by suppliers to distributors that limit their conduct. The most common restraints are: (a) a minimum retail price; (b) to sell only in a certain territory or from a certain location; or (c) to sell a minimum quantity over a given period of time. According to (Martin, 1993:326) recent work on this behaviour suggests that vertical restraints may serve to certify product quality, may serve to induce retailers to carry a greater range of services, or may be a response to uncertainty. As a conclusion, it can be said that vertical restraints may not always have an efficiency motive, nor are always a support for market power (*ibid.*:350).

Such restraints may be applied by manufacturers to the sale of their products made through distributors. These practices are in general forbidden by article 101 and 102 of the TFEU in order to preserve market competition. Exemptions are only granted when they do not restrict competition or their benefits outweigh any anti-competitive effects[195]. A consultation to DG Competition cases database has not found any sanction on vertical restraint on the security industry.

PRODUCT STRATEGY

Product strategy is mainly aimed at increasing its uniqueness as solid as possible from imitation. This uniqueness will attract buyers' preferences and loyalty thus weakening price competition and commanding a premium (monopolistic) price. Such strategy may raise barriers to new entrants and eventually provide some market power. It includes the development or enhancement of products' performance and quality, the creation of new brands to crowd the product space, advertising, and the promotion or the adhesion to new standards. Non-price competition is likely to be important in an oligopolistic market, since it is less risky than initiate a price war (Tisdell and Hartley, 2008:226).

All these methods are common place in the security industry, but the achievement of product differences grounded on features and performance able to improve deterrence or lessen inconvenience is probably the most relevant. They are achieved, as we have

[195] See also SEC (2010) 411 on EU on guidelines on Vertical Restraints.

seen in previous chapters, through the use of better technologies. The number of varieties will depend, however, on the sunken cost needed to produce a new variety (Martin, 1994:335).

When differences are not easily ascertained, signals of value such as reputation, installed base, or large market share may be an indicator to the purchaser of security. Such indicators tend to favour incumbents.

Economic theory predicts that firms with market power are likely to invest too much from a social point of view in product differentiation (Martin, 1994: chapter 8; Tirole, 1988:282). While this may be a potential risk, an initial assessment suggests that product differentiation in security is often related to the different user needs and budgets, thus favouring the creation of profitable market niches.

Research, development and innovation

Research and development is essential to achieve differentiated products more fitted to customer needs or less expensive, as for example computer tomography to detect explosives and drugs inside travelling baggages. Successful R&D will help to obtain technology leadership and innovate faster than competitors offering more attractive products in the market. This provides companies with an important temporary advantage until imitators begin to deliver similar products. R&D may unfold new or improved production process favouring more massive and cheaper production able to feed a large customer base as for example smart cards or RFID tags. R&D is a desirable market feature with a positive impact on market performance. It may have consequences on market structure propelling successful firms to the forefront.

It can be said that the security sector is a moderate to large investor in research and development in many market segments as can be seen by the large number of new products that are yearly launched into the market. This is because innovative and better products and services which improve security are largely rewarded by customers. Prime contractors, value added resellers and equipment manufacturers are the main investors, whilst distributors and installers are less involved in this activity. Innovation in security services is, however, less visible and no practical examples have been found.

The research and development process

Security systems are usually engineering intensive products that require the integration of different technologies and intermediate products to achieve the desired performance. Technologies may be obtained from other market sectors, but they often require significant developments to adequate them to security needs. Certain products require sophisticated technology research, which usually needs the support of universities and research centres to exploit basic scientific knowledge, like a sensor or a CB agent antidote[196]. Advances are only achievable by means of multidisciplinary teams able to amass enough know-how, expertise and synergies[197]. The formation of R&D consortia is a way to build up such teams as well as to share the large cost and risk associated to

[196] Usually being this research cost not the largest share of the total development cost.

[197] For example, biological detection equipment requires cross-cutting, interdisciplinary science such as microbiology, cell biology, biophysics, electronics, material science, microfabrication, microfluidics and bioinformatics/statistics (NRC, 2002:72).

this activity. Such consortia are usually led by large companies that integrate companies with niche expertise, research university departments or their spin-off companies.

The process initiates establishing a system concept whence the desired product can be defined. This definition will be translated into a set of requirements that will guide the design and development phase. Once a basic design is unfolded, an exhaustive test and evaluation phase starts. The chance to become successful the first time, even with a clear view of users' needs and design options, is low and the process iterates through design changes and improvements until performance offsets current systems' capabilities. Whereas a systemic approach is applied to the whole process trial and error methods predominate. Failure rate is high and many prototypes never pass to the production stage. Successful prototypes still will need further developments to achieve efficient production methods. These methods may include new materials, design changes, new tools or new technologies able to reduce price until the product can be accepted by the market as for example printed Thin Film Transistor Circuits for chipless RFID tags (EU, 2008:79). According to (Freeman, 1986:123) the whole process may take years to mature for very disruptive products and the gestation process –akin to animal reproduction– cannot be artificially shortened easily.

In a nutshell, research and development is an inherently risky, uncertain and wasteful activity. The reasons behind have been deeply analysed in the literature. Rao *et al.* (2007:72) argue that systems requirements and specifications are inherently incomplete and may include ambiguous and contradictory features that, even worse, may change over time. Therefore considerable efforts are needed to understand the entire and non-trivial system in its ultimate form before the system can be successfully developed. System designers need experience to understand the implications of their design choices. But this experience can only be gained by making mistakes, learning from them, and having a mechanism to modify and evolve systems over time as the understanding of both user and designer grows and as requirements and technology evolve.

In his paper, Hobday (1998) analyses the complexity of this activity especially in large and advanced projects where a large number of stakeholders are involved. One of the main problems is that the development of these systems requires coordination and collaboration based on non-market mechanisms to success. It requires multi-firm *ex-ante* agreements on complex technological tasks, throughout the stages of design, development and manufacture. The coordination process requires mechanism for communicating design and architectural knowledge and for dealing with feedback from users and other stakeholders since small changes in one part of the system can lead to large changes in others. The quantity and complexity of alternative system architectures pose significant coordination problems for suppliers, especially when the different stakeholders have to agree *ex-ante* on the path of innovation such as regulators imposing the use of certain standards. Presumably, the larger the number of tailored components and subsystems, the more difficult the architectural choices will tend to be. In this environment, focusing devices are needed to cope with the combinatorial explosion, i.e. the large number of alternative design paths for firms to make any realistic estimate of how to proceed. In the development of complex products the problem of narrowing the design choice can be daunting, especially under conditions of rapid technological change, unclear user requirements and multiple customised components. The organisational and managerial complexity of these projects favour

large companies that profit of the synergies of developing similar projects and the accumulated knowledge to master these processes and their risks.

Leader innovators, defensive innovators and imitators

Innovation in the security market means that the survival and growth of companies depend upon their capacity to adapt to the rapidly changing external environment or to change it. Within these limits, the firm has a range of options and alternative strategies. It can use its resources and scientific and technical skills in a variety of different combinations. It can give greater or lesser weight to short-term or long-term considerations. It can form alliances of various kinds. It can license innovations made elsewhere. It can attempt market and technological forecasting. It can attempt to develop a variety of new products and processes on its own. It can modify science and technology to a small extent, but it cannot predict accurately the outcome of its own innovative efforts on those of its competitors, so that the hazards and risks which it faces if it attempts any major change are very great. Freeman (1986: chapter 8) distinguishes three sort of strategies related to innovation: leader, defensive, and imitators.

A firm wishing to be ahead in the introduction of a new product or process must have a very strong problem-solving capacity in designing, building and testing prototypes and production plants. The innovating firm may have to bear the brunt of this educational and training effort (still the new knowledge not socialized). In these firms the generation and processing of information occupy a high proportion of the labour force, but these activities are the life-blood of the *offensive* innovative firm.

First movers may enjoy of important advantages when the product succeeds, especially if imitators cannot regain easily and quickly market share. Strategic behaviour of first movers will focus on slowing down and delaying the diffusion of its technology through appropriate patenting and other protective measures. A more clever conduct may be the licensing of the owned technology to third parties, increasing the chance that the product becomes an industrial standard when network effects are relevant. The large security investment in the United States makes that first movers often come from this country.

The *defensive* innovator does not wish to be the first, but neither does she or he wish to be left behind by the tide of technological change. He may not wish to incur the heavy risks of being the first to innovate and may imagine that he can profit from mistakes of early innovators and from their opening up of the market. Defensive R&D is probably typical of most oligopolistic markets and is closely linked to product differentiation. For the oligopolistic, defensive R&D is a form of insurance enabling the firm to react and adapt to the technical changes introduced by competitors. The defensive innovator must be capable at least of catching up with the game, if not of *leap-frogging*. The defensive innovator can wait until it sees how the market is going to develop and what mistakes the pioneer make (e.g. profiting of opportunities of improving design or production techniques), but they dare not to wait too long or they may miss the boat altogether. This innovation strategy has been particularly characteristic of European security firms in many market segments, but not in all as for example smart cards.

The third conduct is imitative and dependant strategies, in which companies are content to follow way behind the leaders in established technologies, often a long way behind. At least, they would like to differentiate their products by minor technical improvements. Imitators may enjoy advantages in managerial efficiency and in much lower overhead costs, arising from the fact that they do not need to spend heavily on R&D, patents, training, and technical services, which loom so large for the innovation firm. Unless the *imitators* enjoy significant market protection or privilege they must rely on lower unit costs of production to make headway. Production engineering and design are two technical functions in which the imitators must be strong. This pattern of conduct is seen in many foreign suppliers of security equipment and components coming from Eastern Asia (Frost & Sullivan, 2006a:5-31 and 2004:7-41).

Incentives and restraints to invest in R&D

Market conduct on R&D depends on incentives that industry finds for expending resources in this activity that are basically driven by expected benefits. Hence if this activity is expensive and uncertain, market demand is low, and the innovation is not applicable in other economic sectors innovative products and services will slowly unfold. Investment in R&D is also related to market structure being some empirical support that there is greater investment in more concentrated industries. This may be due to advantages of large size, a large market share, less chance than competitors will appropriate the revenue that flows from successful innovation[198], or some market power because in all these cases the chance of earning large profits will become an incentive to finance risky R&D programs (Martin, 1993:381)[199]. This issue will be analysed in more detail in the next chapter.

Marketing and advertising

Marketing and advertising convey information on product quality or performance reducing search cost of consumers and helping them to make better choices. They stifle product differentiation associated with a lack of information and encourage the production of high quality goods. By so doing, they foster competition and market efficiency (Tirole, 1988:108). However, these activities may also enclose strategic behaviour when they are aimed at artificially increasing product differentiation, create market power and deter entry or induce exit of competitors. In sum, impact of these practices in imperfect markets is complex (Tisdell and Hartley, 2008:236).

Advertising

Advertising is a method of differentiating, in the eyes of the consumer, the products of one firm from those of competitors. It is a method of reducing the scope and effectiveness of price-competition by attaching a strong element of goodwill to each firm (Martin, 1993:136). Advertising may be used to deter entry if for some reason it is less effective or more costly for an entrant than an incumbent. Higher costs for the

[198] Patents and IPR rights may help to solve this problem, because they may provide some monopolistic power to leading firms. This explains the insistence of organizations like EOS (2009:24) on this issue. On the limitation of this method see footnote 184.

[199] This corresponds to the Schumpeterian view that society ought to be willing to accept static market power for the desirable technological market performance that it brings

entrant than for the incumbent, creates the possibility of limit pricing and entry deterrence (*ibid.*:141).

Advertising in the security industry does not play a central role as other markets where sales campaigns based on television, radio or press are essential due to the sensitivity of demand to advertising and little product diversity. This advertising aims for making the consumer familiar with the brand name[200]. Only the advertising of security products for individual or residential markets may play a more prominent role (e.g. Securitas Direct). In general, security goods and services are search goods, i.e. goods whose characteristics can be explicitly described, and hence customers are less swayed by advertising. In particular, large companies and the Public Administration usually have a good knowledge of products and services endowed with high levels of technological competence. Customers will value also other attributes like market share or installed base; reputation of product quality, and past performance in the provision of security solutions.

Advertising is mainly made by means of promotional brochures, web pages, specialized magazines and tradeshows; and for sophisticated equipment presenting scientific results in congresses as a mean to increase reputation. In sum, advertising in this sector is moderately used and is more oriented to inform customers. Hence the resource waste and impact on product price can be considered relatively low.

Marketing

Small industrial and residential markets also demand selling activities to convince the customer of the goodness of a proposal[201]. These activities tend to increase for large purchases where the security solution will be tailored to user needs. Pre-sales activities, before a request for proposal is issued, as well as the elaboration of impeccable proposals may be essential to demonstrate that the bidder is able to produce what the customer needs and attain the best value for money. It requires specialised departments or teams that invest considerable efforts on this activity, where large incumbents may enjoy advantages.

Rent seeking[202] as a special kind of marketing

Government action needs enough knowledge and information to make sound decisions to increase security of citizens, from establishing new regulations to selecting the best alternative to solve a security need. When such action generates appropriable rents, it can be expected a wasteful industry allocation of resources to supply information to influence the government outcome (Spulber, 1989:82). In the limit, competition will drive information production to the point where private expenditures equal publicly created rents (*ibid.*:83). Since firms will not account the negative externality of this behaviour on other firms, investment in this activity may be excessive from the social point of view.

[200] The advertiser does not convey information, but seeks to establish, by repetition a brand identity.
[201] Free trials and money-back guarantees may be examples of this kind of strategies.
[202] This term can be defined as ‘the expenditure of scarce resources to capture an artificially created transfer’ (Spulber, 1989:82).

When government has knowledge shortfalls, industry may behave strategically and provide biased information with a negative effect on market through the wasteful misallocation of resources in developing non-optimal solutions[203] that do not enhance security, this becoming a source of poor market performance.

The industry interest in increasing revenues and profits may work together with bureaucracy maximizing interests to promote security programmes whose utility may be questionable when compared with other societal needs. It is a well proven fact that bureaucracies aim to maximize their budget as a way to increase their power and influence. In their analysis, they may easily depart from reality, overestimating the benefits and underestimating the cost of their preferred policies. In these cases, cost considerations or informed prudence may not play the due role in the decision process, whereas biased threat and consequences assessments –where dangers may be exaggerated and fears exacerbated–, groundless technology capability to get rid of insecurity, and undervalued costs and risks of developing and deploying the foreseen solution may play the main role. Such conduct may be more common than expected as can be seen in many failed pilot projects described in chapter IV as for example biometric solutions, Pulsed Fast Neutron Analysers or RFID tagging systems.

Such behaviour may find a strong ally in the social groups economically involved in security production since large expenditures mean more activity, more income, large facilities, more employees, and more profits. As a result, a budget-maximizing bureaucracy would be inefficient, allocating excessive resources to security and providing too large output. These social groups may thereby benefit at the expense of the whole community.

The industry may underpin this behaviour when it provides pseudo-rationalistic methods instead of objective assessment with the aim to influence in the resource allocation decision (Freeman, 1986:190). The problem is that technological fashions and preferences of industrial designers could capture bureaucrats will over society and citizens wishes. These methods may succeed in building preferences in an environment of bounded rationality and asymmetric information where not all information is known or taken into account by the decision maker. If the industry is able to produce persuasive information or convincing testimony that is not balanced with the competitive supply of information by individuals of opposing views, there could be a chance of an inadequate decision making with an adverse impact for the whole society (Spulber, 1989:85)[204]. Only the political mechanism –through adequate publicity, transparency and (parliamentary) debate where countervailing views and arguments may be pondered about facts, values and uncertainties–, is able to reach consensus and restore the citizen sovereignty which the market mechanism can no longer assure. Only in such case, it can be assured, without serious doubt, that government decisions

[203] Steward and Mueller (2009) and Mueller (2009) papers present examples of non-optimal security investments where costs are not commensurate with benefits.

[204] The report of the Group of Personalities (2004) that requested an annual EU budget on security research of €1 billion to equate USA estimated expenditure may be a paradigmatic example. White paper of associations can be a vehicle to provide this testimony, as for example the European Organisation of Security (EOS) document *Priorities for a future European Security Framework* (2009). On the large influence of industry in setting the agenda of the European Security Research Program see Hayes (2009).

represent the preferred position for the electorate and hence a social welfare maximum[205].

Bundling

Bundling, i.e. the sale of two or more products together is a method to increase brand fidelity. This practice is used in the security market as for example a stand-alone DVR integrated with a monitor for video surveillance; or the embedding of security software in new PC like Symantec, or McAfee (IDC, 2009:34). However, bundling in security is usually associated with some sort of integration between the different products, where end-users benefit from higher performance and better price. This trend is reinforced by the appeal of buyers that want the convenience of one firm taking full responsibility of the security solution (one stop shop) since it reduces the transaction cost of purchasers in terms of supervising just one contractor. This appeal is very common as for example the area of buildings' security where the access control, the fire system, the intrusion detection, and other monitoring systems are integrated to offer an effective and seamless solution to the end user. Such a bundling mainly favours system integrators and value added resellers.

Bundling has important strategic effects and may allow a firm to use the leverage provided by its power in one market to foreclose another market (Tirole, 1988:335). Bundling may allow cross-subsidization between different products and services as a market strategy. This may be a common case in the security market when contracts include the supply of a system together with the provision of operation and maintenance services[206]. For instance, home alarm equipment may be offered for a low price or leased, when a long term remote surveillance service contract is signed (see EU merger 4986).

Unbundling trends may however emerge as industry evolves and matures. The increase of the market size and the development of standardised products that share a common interface (e.g. IP-based cameras and sensors) may allow sophisticated end users to replace system components and equipment with products not manufactured by the original supplier.

CONTRACT EXECUTION

Many transactions in the security market are complex operations which involve large duration contracts. The conduct of industry in the execution of these contracts is another area with impact on market performance. This is because contracts are incomplete and hard to enforce. This raises a variation of the classic moral hazard economic problem, known as the principal-agent where one party, called the agent (the industry) acts on behalf of another party called the principal (the purchaser). In this context the agent has more (private) information about his or her actions or intentions that the principal does, because the principal cannot perfectly monitor the agent (plans, milestones, review and audits imperfectly monitoring agent conduct). In such a case, the agent may have an incentive to behave opportunistically (i.e. seeking self-interest through manipulation of

[205] However, the creation of citizen's groups able to wield countervailing views may be disproportionately expensive in comparison with industrial groups (Tisdell and Hartley, 2008:117).

[206] Rivals would then have to set up their own service department to come into the market increasing the cost of entry and expansion.

information or misrepresentation of intentions) not fully honouring the contract (Martin, 1993:212).

Service contracts are certainly subject to this problem[207], but this negative behaviour may unfold in the development of systems where the system is defined on paper, prices are estimated on budgets and uncertainty regarding the desired outcome is high[208]. In such a case, the allocation of technical and financial resources may misfire and may result in overcosts, delays, underperformance and even complete failure. Three main types of contracts are used in order to manage (and balance) risk between the purchaser and the supplier: fixed price, a target cost fee incentive; or cost plus contract. The first and second case implies a tough budget constraint since the company will have to pay from its own funds the extra cost of the project. The supplier will only take these contracts after attaching a risk premium to the price (Williamson, 1971). Moreover, they may have a negative impact on the quality of the outcome. The last one implies a soft budget constraint since the company will be paid whatever the project costs. In this case the industry will afford greater operational flexibility, especially for the introduction of design changes that may be quite useful when the end product is poorly defined, yet the incentive to be efficient may be compromised and the project may easily derail into a limbo of never quite completed objectives and cost overruns (Markowski and Hall, 1998:21). These problems seem to be rather common as the recent report of GAO (2010) about the DHS shows. Evidence in Europe is scarcer, but the delays and overcost of the Galileo program may be a good paradigm.

MERGERS AND ACQUISITIONS

Market restructuring is often made through mergers and acquisitions of companies. According to Schwartz (1984) firm's desire to merge is a consequence of managers' growth maximizing behaviour tempered by life-cycle effects (firm age, technology age, patent / sales ratio) and constrained by cost of capital or cash flow availability. Yet, other factors as rationalisation, economies of scale, market expansion, and profit increase may play a role. According to Frost & Sullivan (2008: 51) these concentrations may help to: (a) access to geographic regions and countries through local/regional companies with a strong brand recognition, (b) access to innovative technologies that complete the product portfolio[209], (c) access to key end-user sectors and get the knowledge to compete in that space. Other important reason could be the acquisition of a key supplier within the value chain. But, probably the main rational of these operations is their capability to easily surpass the entry (and sometimes the exit) barriers of a new market, that would be inevitably associated to large and uncertain investments, by means of purchasing a company already operating in the market.

---

[207] This could have been the case of 9/11 where hijackers were able to smuggle aboard box-cutters because security companies could have unnoticeable degraded the quality of their service to be more competitive (see page 85 of the 9/11 Commission Report). The Aviation and Transportation Security Act 107-71 Nov. 19, 2001 tried to amend this situation based on federal government screeners and a new programme to qualify private screeners. It also set a security fee on passengers between $2.50 and $5.00.

[208] Since budgets are usually based on a cost plus a fee, companies are more interested in raising budgets rather than seeking cheaper but riskier alternatives as for example those often available from SMEs.

[209] Start-up companies are strong in technology but poor in marketing and installed based. They are attractive to a large corporation since the latter are weak in new technology, but strong in the other business and industrial capabilities.

Successful M&As are socially beneficial when the new company becomes more efficient, but if competition weakens too, it is unlikely that those benefits will be passed on to consumers in the form of lower prices. This explains that industrial concentrations are subject to the scrutiny of national competition authorities to assess if they may create dominant positions that may significantly impede effective competition. This role is performed by the EU Commission when the concentration has a European dimension.

The following table shows some of the main M&As in the security market in the last decade. The last column of the table points out if the operation was deemed of European dimension. Despite efforts to identify the most relevants, the list cannot be considered exhaustive. Large incumbents such as GE, Honeywell, Siemens, Tyco, UTC and Bosch, have been very active acquiring small and mid-sized players with a good foothold in local markets, or with attractive products. This kind of vertical M&As predominates in comparison with horizontal operations.

Acquirer	Ctry	Company	Ctry	Year	Price	Comment	EU
TYCO	USA	ADT	USA	1997			M.915
Honeywell	USA	Pittway	USA	1999	$2.100	Includes Ademco.	
ADT Security Services Inc.	USA	Cambridge protection industries	USA	2001	$1,000	Electronic security services.	
Tyco international	USA	Sensormatic Electronics Corp.	USA	2001	$2,303	Electronic security solutions.	M.2584
Smith Detection	UK	Barringer Inc.	USA	2001		IMS explosive detectors.	
Smith Detection	UK	Heimann Gmbh	GE	2002	£237	X-ray detection.	
Bosch Security	GE	Philips CSI	NL	2002		Communication, Security and Imaging.	
OSI Systems		Ancore Corp.	USA	2002	$14.44	Cargo container scanners.	
UTC	USA	Chubb	UK	2003	$1,018	UTC Fire & Security.	
Honeywell	USA	Ultrak	USA	2003		CCTV business.	
Schneider Electric	USA	TAC	SW	2003		Building automation including security.	
Group 4 Falck	DK	Securicor, plc.	UK	2004		Guarding services.	M.3396
Bosch Security	GE	VCS Video Communication Security AG	GE	2004		IP cameras.	
Cross Match Technologies	USA	Smith Heimman Biometrics Gmbh	GE	2005			
EADS	EU	Nokia PMR	FI	2005		Professional Mobile Radio.	M.3803
Gemplus	FR	Setec Oy	FI	2005	€49	Electronic credentials.	
Halma	UK	Texecom ltd.	UK	2005	£26	Security sensors and alarms.	
Honeywell	USA	Novar, plc	USA	2005		Intelligent building systems.	M.3686
Petards	UK	PI Vision	UK	2005		Network video recording technology.	
Siemens Building	GE	Bewator	SW	2005		Access control and CCTV business	

Technologies							
UTC	USA	Kidde, plc.	UK	2005	$3,000	Kidde owned Guardall Integrated with Chubb.	M.3688
UTC	USA	Lenel Systems Int. Inc.	USA	2005	$400	Security systems and software developer.	
GE Security	USA	VisioWave	SW	2005		Digital video cameras and video content analysis.	
Sagem	FR	Orga-Gunther group	GE	2005		Smart cards.	
Oberthur Card	FR	Set Card	SP	2006		Secure cards.	
Alive Tech. Inc.	USA	Geometrix	USA	2006		3D face recognition.	
ADI Global Distribution	UK	Gardiner Groupe	FR	2006		ADI is a global distributor of security equipment owned Honeywell	
Cross Match Technologies	USA	C-VIS	GE	2006		Face Recognition	
Extreme CCTV	CA	Forward Vision CCTV	UK	2006		Intelligent PTZ cameras.	
Gemplus	FR	Axalto	FR	2006	$928	Electronic credentials	M.3998
G4S Security Systems	UK	AC Controls Ltd.		2006		Access control, security.	
Primion Technology	GE	GET Group	BE	2006		Access control.	
HID Global (Assa Abloy)	USA	Fargo Electronics, Inc.	USA	2006	$337	Identity card issuance systems.	
Bosch	USA	Telex Communications	USA	2006	$420	Communication equipment.	M.1840
HID Global	USA	Integrated Engineering	NL	2007		Access control. Smart cards and readers.	
Robert Bosch GmbH	GE	Extreme CCTV	CA	2007	C$93	Surveillance Systems	
UTC	USA	Initial ESG	UK	2007		Security and Fire Protection systems and services.	M.4671
Schneider Electric	USA	Pelco	USA	2007	$1,540	Video security systems	
Honeywell International	USA	Activeye	USA	2007		Video analytics software.	
EQT V Ltd	INT	Securitas Direct	SW	2008		Security services.	M.4986
EADS	EU	Plant CML	USA	2008		Emergency and mission critical management solutions.	
March Networks	USA	Cieffe, S.p.A.	IT	2008	€14	IP video surveillance solutions.	
Symantec	USA	MessageLabs	UK	2008		Messaging and web security services.	
Sophos	UK	Utimaco	GE	2008	€214	Security and encryption.	
BAE	UK	Detica	UK	2008	$1,100	ICT Security	
ASSA ABLOY	SW	Simon Voss	GE	2008		Wireless electronic locking and access	

						control systems.	
Honeywell Sec.	USA	AV Digital Audio Video-technik GmbH	AU	2008		Public address and notification sound systems.	
G4S	UK/DK	Touchcom	USA	2008	$33	Installation and maintenance of web based electronic security systems.	
Cross Match Technologies	USA	Labcal	CA	2008		Mobile and wireless biometric solutions for identification and authentication.	
Authentec	USA	Atrua Technologies	USA	2009	$4.9	Fingerprint sensors.	
SAFRAN USA	USA	General Electric Homeland protection	USA	2009	$580	Creation of Morpho global leader in explosive detection	M.5539
UTC	USA	GE Security	USA	2010	$1,800	Security systems for commercial and residential applic.	M.5735
SAGEM Morpho	FR	L-1 Identity Solutions	USA	2010		Biometrics.	
3 M	USA	Cogent Inc.	USA	2010	$943	Biometrics.	

Table 21. Main mergers and acquisition in the security market since 2001. Price in millions.

This table shows the more relevant mergers and acquisitions in the security market occurred in the last decade. It has been compiled across the study and confirmed on the internet. As can be seen from the table, there are a considerable number of mergers, being its number close to the defence market in the same period (Marti, 2009). This is a signal that the security market is becoming more European and international.

RESUME AND CONCLUSIONS

This chapter has analysed the conduct of market agents with special emphasis on industry stakeholders and the identification of those behaviours that may have an adverse impact on market performance through rivals exclusion, weakened competition, and reduced efficiency.

Competition plays a relevant role to assure a good allocation of resources. Collusive practices do not easily success and few cases are foreseen where there could be a real risk of this practice. Some kind of predatory practices may appear in large projects financed by the Administration. Standards and innovation can be another form to exclude rivals from the market. Finally, vertical restraints could not always be associated with an increase in market efficiency.

Industry may prefer to reduce chances of rivals using different product strategies, being the main research, development and innovation. Whereas R&D may be beneficial to the end customer –in terms of better performance– and the firm –in terms of increased profits–, high uncertainty, large sunken costs, and low expected profits due to the small market size may discourage efforts in this activity. This may require the helping hand of government.

Leadership, defensive innovation and imitation are three clearly discernible behaviours of companies in this field. If they wish to survive despite all their uncertainties about innovation, most firms shall be on an innovative treadmill. They may not wish to be *offensive* innovators, but they can often scarcely avoid being *defensive* or *imitative* innovators (Freeman, 1986: 170).

Industry conduct on advertising seems to have a positive effect on market performance due to better informed customers. Marketing practices, especially excessive lobbying may, however, have a negative effect in terms of wasted resources and leverage in the choice of non-optimal solutions from the societal point of view.

Bundling is another practice which often raises entry conditions. Some sort of bundling that combines security products and services have been found during the survey. Its main effect is to raise entry conditions to new companies.

Mergers and acquisitions and concurrent divestment are common place in the security industry. These operations facilitate market restructuring and reconfiguration which may result in increased efficiency. However, due to their potential impact on competition they are strictly regulated by the EU and member states. New entrants in this market however seem fewer, and often industrial facilities merely change of company name.

VIII. INDUSTRY PERFORMANCE

This chapter tries to assess the performance of the security market, evaluating to what extent the industry is able to provide innovative and highly valued security products and services in an efficient way (i.e. at lowest cost that the state of the art allows), while adequately remunerating their shareholders. In some sense, market performance is the ultimate arbiter on how well market forces are doing. While cases in which performance may be impaired by basic conditions and the structure and conduct of the market have been given in previous chapters, we will try here to analyse this question in more depth.

Market performance has many dimensions. We will focus on three aspects namely allocative efficiency, productive efficiency and dynamic efficiency. We will discuss specific questions related to the security market, not addressing more general questions on market performance of the whole European industry, as could be the case of rigidities in the labour market. Assessment nonetheless is not easy. Whereas enough information is available to make a qualitative assessment, quantitative assessment is harder to perform since market indicators are not easy to collect.

ALLOCATIVE EFFICIENCY

Allocative efficiency measures the extent to which resources are properly allocated to satisfy the market demand –i.e. the needs of society in terms of products and services– spending the lowest amount of resources being no alternative arrangement that could make better off this provision.

This problem can be split into two. On the one hand, it should assess if society demands the right products and services in the right quantity to increase its security. On the other hand, it has to analyse if industry is allocating efficiently their resources to provide the requested products and services at the best value for money. In the first case, an improper choice may discard other arrangements to safeguard society of potential threats with higher pay off. This is an important question that has been analysed in detail in chapter III. As we have seen there, conditions of bounded rationality may hamper the decision process resulting in a non-optimal choice. In chapter VII we have seen also that industry may have a non-positive influence in the decision process. In this chapter, we will only address the second case.

Proper allocation of resources in the industry is hampered by many reasons. Monitoring by supervisors is imperfect, supervisors have some discretion in the way they carry out their jobs, and because work involves disutility, employees will engage in slack and not carry out their jobs with due efficiency. They will not minimize costs. The more competitive the market environment, however, the greater the pressure on employees up and down the firm hierarchy to minimize cost (Martin, 1993:227). Such fact explains the general thought that social welfare goes up as the number of competing firms grows (*ibid.*:229).

Since incentives to allocate resources efficiently come mainly from competitive markets where entry conditions are not particularly costly, the evaluation of allocative efficiency focuses mainly in analysing market concentration and entry barriers that may negatively impact on competition, create market power and allow industry to unjustifiably increase

prices above marginal cost (monopolistic pricing) providing a premium that is costly and a kind of resource waste from the social point of view in terms of less output and higher prices (also known as deadweight loss). Such market power is also questionable since it impedes an equitable distribution of market benefits across society. Resources devoted to create or preserve this market power may be seen as a source of inefficiency insofar these resources have alternative use in producing more goods and services at a smaller price.

Looking at the structure of the security market, as has been seen, few monopolies can be observed in the supply chain. Competitors are often few (oligopoly) in market segments where economies of scales are relevant. However, these firms do not cover the whole market and frequently a considerable number of medium size companies and still a large number of small companies operate in the fringe. Whereas such concentration may help to achieve a dominant position, where higher prices and some deadweight loss may incubate, in a market essentially driven by technological progress, incumbent firms must engage in intense rivalry (e.g. Smiths Detection, GE, L-3 in CT scanners) to keep pace with progress and not lose market share. The result is that performance is much closer to the competitive market than examination of number of firms and concentration ratios alone would suggest (Martin, 1994:132). Conversely, such market concentration may be more worrying in markets where innovation is low, product or services differences play a marginal role and there are some entry barriers, because the risk of collusion may be higher. Security services firms could approach to this situation, yet more research is needed to assess if there is a real chance for this practice.

The concentration level is also high in the market segments of suppliers of governments and large organisations. This case is also of concern since there may be very few companies (or even a single one) able to present a proposal. Even being few, the selection of the optimal proposal may be compromised since solutions are so different that comparisons are not easily made. In addition, because acquisitions are based on system requirements, the system performance, cost, and development risks can only be forecasted. In this situation, buyers may be at disadvantage in relation to suppliers, because they may lack of enough information to make a proper choice. This environment adds further uncertainty to the optimality of the final choice. The situation of bilateral monopoly after the awarding and the large substitution cost may favour some market power of the supplier. Incomplete contracts, adverse selection, and principal-agent problems may negatively impact on allocative efficiency. Yet the high transaction costs associated, as the imposition of penalties to suppliers by governments, when they do not observe contractual clauses, limit a better allocation.

Collusive practices between bidders in high-end markets however have little chance to unfold for the reasons that we have mentioned in chapter VII. Only consortia may be a method to avoid competition and share the benefits of awarding across members with an agreed distribution. Yet, this kind of agreements are only allowed under the strict conditions stated in article 101 (3) of TFEU.

Resource allocation and excess capacity

The capability to respond to a security incident requires many times some kind of excess production capacity. For example, contracts can be signed with drug-manufacturers for assured access to the necessary quantities within a certain timeframe,

instead of a large and less efficient stockpiling. However, as long as the industry has to invest in infrastructure to deliver the required quantities within the needed timeframe, that it is not routinely used, a misallocation of resources from the economic point of view appears that may negatively impact on the industry performance as an overhead cost (NRC, 2002:99). On this basis, the demand for such capability might be so remote and unlikely, and yet very costly, that its maintenance is not worthwhile (Hartley and Lazaric, 2009:164).

PRODUCTIVE EFFICIENCY

The assessment of productive efficiency tries to answer to the following question: are goods or services provided at the lowest average cost? Productive efficiency is mostly related with industry size. The average cost curve of many security goods and services in relation to the units produced tends to have a U-shaped form, where cost decrease – due to economies of scale, scope and learning– until it reaches the minimum efficiency scale or MES and then starts to grow since diseconomies of scale (e.g. management) begin to unfold. The question is to assess if companies are operating too short (or too far) from MES. Concentration may be desirable to reach a higher productive efficiency when competition is not significantly impeded. Even (natural) monopolies or duopolies may be preferred when economies of scale are so high that a market with more than one or two companies will be too inefficient such as for example the satellite market.

At first sight, the structure of the industry is often organised to meet this productive efficiency. This is the case of massive equipment suppliers as for example CCTV manufacturers like Panasonic or Sony; or security components suppliers such as Honeywell or Bosch which have a large size and market share. Small size companies, conversely, are more frequent when these economies are smaller and other factors have stronger influence on efficiency. The lower size and concentration of this industry in comparison with defence may be due probably to a considerable lower value of the minimum efficiency scale cause by a smaller cost of developing products.

The reduced demand of security equipment, however, set limits to productive efficiency, because the demand is too short to achieve the scale where production costs are minimised. This is the case of some market segments such as cargo and baggage inspection equipment.

A detailed assessment of the adequacy of industry size is an interesting exercise that should be made to identify if current market structure is negatively impacting on productive efficiency, as seems to be the case of small suppliers in the residential market. Yet, this is a complex task that requires a more in-depth analysis.

DYNAMIC EFFICIENCY OR RATE OF TECHNOLOGICAL PROGRESS

The third question to evaluate is dynamic efficiency, i.e. the capability of the industry to exploit new technologies, develop new products, or improve production processes that drive ahead quality, innovation and timeliness as well as drive down prices. Such efficiency strikes at the very foundation of profits and output, rather than their marginal improvement. A highly dynamic market is always desirable, and may be especially necessary to counter the innovative capability of terrorism and organised crime.

There is a wide debate on the literature about the efficiency of large and small firms in the invention and innovation process. Freeman (1986:137) argues that small firms may have some comparative advantage in the earlier stages of inventive work and the less expensive, but more radical innovations[210]. Small firms tend also to be more flexible to find and exploit research results and putting innovation into use. But large firms have an advantage in the later stages and in the improvement and scaling up of early breakthroughs.

According to Martin (1994:368) large firms may enjoy advantages due to economies of scale in the R&D processes, because the R&D output rises more than proportionately with size. In the end, this is a question about the production function for knowledge. Large firms can undertake costly and time consuming developments which are beyond the resources of a small firm[211]. They enjoy advantages where large numbers of different specialists are needed to solve a problem or expensive instrumentation and sophisticated equipment is essential. Large firms also have a comparative advantage where there are several possible alternative routes to success, with uncertainty attached to all of them, but benefit for the simultaneous pursuit of several (Freeman, 1986:138). In addition, large firms are best prepared to support inevitable R&D failures and delays until outcome becomes profitable. Firms with a large market share or large diversified firms will be more willing to invest in R&D because they will earn more profits due to large revenues or they will be more likely to apply a successful innovation in some of the markets in which they operate.

As a conclusion, it can be said that both kind of firms have advantages in the innovation race. The analysis made on the European security industry shows that many market innovations have been dealt by small companies as can be the development of IP cameras by Axis Communications. Successful innovative SMEs have been later on purchased by larger companies for subsequent innovation and market take over. Yet, large research projects (especially government financed) are geared by large companies either as a prime contractor or as a consortium leader.

Box 8. Company size and innovative efficiency

The role of incentives

The evaluation of dynamic efficiency shall consider if the market, by itself, provides adequate incentives. Product or process innovations in general result in better or cheaper products that will compete more successfully with rivals, increasing (or not losing) revenues, benefits and sometimes market share. Yet incentives will be mainly driven by the expected benefits that industry forecasts. This means that a short demand, large development complexity, large development time, and expensiveness of the innovation process will slow down technological progress. This is the case of the security market where uncertainties about the performance or the operational effectiveness of the new technology or product –especially when requirements are very strict as for example a low false alarm rate– combined with uncertainties related to the development and

[210] The search of drastic innovation of small firms and new entrants can be explained by the hope of these firms in acquiring a position on the top of the heap, whereas incumbents with a large market share may show excessive inertia trying to protect their past investments through marginal improvements in existing technology, when the threat of new products is not seen too high (Martin, 1994:366).

[211] The complexity of the innovation (measured in the absolute number of components of the system) is one factor which will limit the type of innovation which a small firm can afford (Hobday, 1998).

production costs will slow down dynamic efficiency, especially if demand is highly sensitive to price. This results in innovation barriers where returns are seen too risky or too remote in time for being financed internally. Even with a moderate level of uncertainty, the security market may not be enough attractive if demand is weak, due for example to a fragmented market, to assure a certain level of profit and the product has no application in other markets. Such restraints might explain the sluggishness of innovation in the security market in some areas.

When incentives are weak, it can be said that there exists a failure in the innovation market (Tirole, 1988 and Arrow, 1962) since it is unable to allocate the appropriate resources to innovation. State intervention can break this *impasse* providing adequate incentives to achieve social optimum through the financing of industry or government led R&D projects; and subsequent procurement can simply act by providing assurance of future demand for the embodied innovation. Large government contracts of equipment are able to underwrite private financing and create industrial leaders quickly (IPTS, 2005:63). Experimental government projects, therefore, drive the first phase of many new technologies, a case that is also true in the security field as for example biometrics for national identity cards and passports, or secure containers.

Distortive effects of State industrial support

However, State intervention is not costless. It will involve the outlay of R&D aids as well as administrative costs of their management. Furthermore, it will have a potential distorting effect on competition that may have undesired effects on the market. Since amount of aids are bounded, the whole industry cannot be helped. Only some companies will be granted with aids, whereas others will not receive such aids. The advantages provided by these aids to beneficiaries may crowd out the market of competitors. This may be especially true in large projects where the financing of more than one project is impeded due to the amount of aid required. In these cases, the likelihood of success of rivals will be significantly reduced or even disappear if research and development costs are too high to be privately financed. In this vein, excessive market concentration may be favoured.

When market segments are under development, the *learning curve* drives down costs as a function of experience. Suppliers which benefit from government contracts that involve innovation have a higher chance in bidding for future contracts and reduce their costs in advance of open market competition. Being the first producer, economies of learning by doing, will help to improve production processes and become efficient earlier that competitors preserving the initial advantage. The awarded company may take all the market, and obtain a monopolistic position, due to the advantages achieved during the early phases of a product life. Long-term contracts and sheer demand may perpetuate this monopolistic capture. Such competitive advantages may be exploited to sell later on products, based on the knowledge and capabilities acquired, in other countries or private markets.

A final remark is that this support may induce firms to maximize subsidies, rather than become more efficient. Methods to reduce these potential distorting effects on the market are commented in the next chapter.

One interesting way of creating incentives for investing in research and development

with no counterpart in Europe is the U.S. Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act. This act passed in 2002 lowers the liability risk of manufacturers that provide security products and services designated as 'Qualified Anti-terrorism Technologies'. The act aims to remove hesitant companies to market antiterrorism technologies because of two concerns: the cost of potentially devastating jury verdicts should the technologies fail, and the cost and scarcity of adequate liability insurance. Around 200 companies have obtained SAFETY Act certification. Certification criteria are based on the technical capability and efficacy of the technology, the economic effects of deployment versus non-deployment and the evaluation of insurance needs (Carafano, 2008).

The Act is incentive for industry because it opens the door to less pervasive tests to verify that security products have enough quality and value. Hence, it helps to speed up technological progress since the time to market may be considerably shortened. Yet, the Act seems to be controversial, because it may help to unfold low value products that do not really increase overall security.

Box 9. A U.S. method to promote market innovation

Standards and network effects

Standards, as has been seen at the end of chapter III, are essential to support innovation and technological progress. Network externalities in particular are only achievable through the development of interoperability standards. The lack of coordination of the supply side to produce standards may delay innovation and progress. Solving this market failure may require the intervention of the State. As we have seen European institutions are very active in the development of standards, yet as perceived by industry efforts seem to be insufficient.

Standardization facilitates dynamic performance in terms of improved innovation, reducing unnecessary diversity, and enlarges production due to the benefits associated to network externalities. –the higher the usage by the society, the more popular the product becomes. Yet, there is a risk that such benefits are only captured by a small number of firms capable of exercising enormous market power (Cave, 2005). Such market power might impair, as we have seen, on allocative efficiency.

The life cycle of technology

The evolution of technology has a relevant influence on market structure, as can be seen by the accelerating rise and decline of high technology industries of which the security industry is not an exception. For this kind of industry, it is more interesting to use models of the evolution of industrial structure over time, from entry of the first firms early in the industry life cycle to exit as the industry winds down, rather than steady-state models of market structure applicable to more traditional economic sectors. Abernathy and Utterback (1975), Freeman (1986: chapter 8), Keppler and Graddy (1990), or Cave (2005), provide a framework with some nuances that may be applied to assess the dynamic efficiency of the security industry. They distinguish three main stages or development phases.

Phase 1. This is the initial exploration phase where advanced science, new technology and invention, realised through imaginative entrepreneurship, are applied to satisfy in a

new way and with superior performance customers needs. During this gestation phase there is a widespread uncertainty on user needs, relevant technologies and attributes of the new product. Users tend to play a major role in suggesting the need and the ultimate form of the innovation. Production is inchoate, unstandardized and based on manual operations or operations that rely upon general purpose equipment. Early adopters tend to be experimental, relatively risk neutral and a have a relative high-income (public sector, large companies). These factors combine to produce inelastic demand and high-return of investment. The capital is scarce and under tight control (e.g. via exploratory procurement arrangements, or *business angels*) and there is a small number of pioneering firms, often of small size, in some cases spin-off of incumbent firms. Pioneering firms benefit of two positive effects: *learning by doing* and *reputation effects*. Learning by doing assures that the cumulative experience gained will be able to deliver solutions with higher functionality and performance and a better matching of user needs at lower average cost than subsequent entrants (if the delay to achieve such features is large, due for example to patents or difficulty to copy a technology, the industry could end up in a virtual monopoly). Reputation will be the result of a demonstrated track record and a large installed base.

Phase 2. Over time, the initial uncertainties abate as *dominant designs* emerge (this depending on product complexity and variety on buyers' preferences). The success of these designs will reward pioneering firms with exceptional sales growth and temporary monopoly profits displacing less efficient rivals (those with the highest costs and lowest quality). This will trigger a market growth phase during which a swarm of secondary innovators will attempt to enter attracted by the demand growth (this depending also on the easy of imitation). As a consequence demand will grow and become more stable and the customer base more diverse and larger. The practicalities of marketing, distribution, maintenance, advertising, etc. will favour the standardization of products. Availability of capital increases from mainstream venture capitalists, mergers, acquisitions, strategic alliances and so on[212]. The band wagon effect is a vivid metaphor of this stage and it relates to a rapid diffusion process which occurs when it becomes evident that the basic innovations can generate super-profits and may destroy outmoded products and industrial processes.

Phase 3. The last stage is the consolidation, maturation or shake-out phase during which market saturation, the approach of technical advances to limits (innovation slowing down and becoming more incremental), and the competitive effects of swarming and changing cost of inputs, may all tend to reduce product price and profitability, and with them the attraction of future investment. During this phase demand becomes more elastic and pressures shift to cost saving innovation in process technologies (i.e. the production tends to become elaborated and tightly integrated through automation and process control becoming industry more capital intensive) and to exploit economies of scale in order to raise productive efficiency. The production volume will rise and ultimately lead to business failures (companies able to accumulate more capacity able to charge a low price due to economies of scale and outplace rivals) and a concentration of the market to the mature phase where returns raise again. The process will continue until the number of companies levels off and market share stabilises[213]. During this

[212] Table 21 provides a confirmation in the case of digital video surveillance.

[213] Processes tend to be so well integrated that changes becomes very costly, because even a minor change may require changes in other elements of the process and in the product design. The benefits of high productivity are achieved only at the cost of decreased flexibility and innovative capacity

phase capital is more likely to be raised through equity markets, with successful firms launching Initial Public Stock Offering (IPO).

The life cycle of technology can be applied to understand the formation and evolution of some security market segments, understand problems in the different phases and eventually design measures to solve such problems. For example many home alarm and intrusion detections systems can be considered to be in the third stage with a stable and mature demand as well as firms in the market; fingerprint identification and access control as well as digital CCTV, inspection equipment, PMR are more in the second phase with some dominant design being successfully marketed and the market experiencing a considerable demand growth and a swarm of imitators; finally biological agent detection systems, face recognition or command and control systems seems to be more in the initial stage where still dominant designs do not emerge, markets are small demand comes from government, and considerable experimentation exists.

Concluding remark

An initial assessment on dynamic performance would suggest that innovation is reasonable good in the security market in many market segments where new products often appear as a response to competition and buyers demand. Furthermore, the price fall of security equipment (e.g. passenger baggage scanning equipment) observed in different documents shows that technology advances in terms of better quality and smaller prices are passed on to consumers. However, this assessment is too short of evidence and a more quantitative analysis is clearly needed.

Incentives for a good dynamic performance have been analysed. A short market demand, complex and risk research, IPR right not being well protected, government incentives improperly applied, and *tipping* effects –i.e. the tendency for the market demand to shift toward a product that has gained a small initial lead drying up the demand of losing competitors– may have an adverse effect on performance.

PERFORMANCE INDICATORS

A way to assess industry performance is to measure some indicators related to its health and competitiveness from the static and dynamic point of view. Candidate values can be market revenues (growth), firm value in the stock market[214], labour productivity (gross value added), profitability (return on sales or return on equity), export sales ratio (international success of EU security equipment), or import penetration (inability of the industry to provide competitively products and services). R&D expenditures as a fraction of revenues may indicate an industry committed to innovation, yet this value should be commensurated with the level of R&D success. Yet, not all these values are easy to collect.

(Abernathy and Utterback, 1975). Hence incumbents, in this phase, may be more interested in protecting these fixed capital investments and in delaying the introduction of new technologies.

[214] A growing value over standard index means an industry that is highly valued by investors due to its proven efficiency and promising future earnings. On the contrary, falling share prices, management and board changes, sales of unprofitable parts of the business and ultimately bankruptcy may suggests a poor performing market.

As we have seen during the study we have identified a growing market in many market segments. For example security and investigation activities had an average annual growth during the period 2003-2008 of 6.8% (Eurostat, 2010). Labour productivity for security services can be obtained from Eurostat *sbs_na_1a_se_r2* table. It was value at €23,000 in 2008. Labour productivity of the security equipment is not available, but a good proxy could be the general value for the European industry which is around €55,000 in 2008 (Eurostat, 2010). Eurostat *ebd_all* table shows that wage adjusted labour productivity in the machinery and equipment market, a market very close to security, productivity is around 140% in 2007 (129% in 2004). We have also seen that Europe is able to export its security equipment to many other countries, this indicating a competitive industry. However, we have also seen than Europe is also a net importer of security equipment, this indicating, in combination with a less technological advanced industry, that the European industry is not as competitive as market demands.

The EU Industrial R&D Investment Scoreboard database has been a good source to assess this industry in more detail. As can be seen in the 2008 database, many European industries involved in the security market are in the top 50 R&D investors as for example Robert Bosch, Siemens, EADS, ST Microelectronics, Infineon Technologies, Safran (Sagem), Thales. Other twelve companies involved in the security market are in the top 1000 list. Non-EU security companies are also large investors in security such as Panasonic, Sony, Cisco, Samsung, Motorola, General Electric, LG, or Honeywell. This may confirm the hypothesis of a market where R&D plays a large role.

Based on this table, we have also calculated the average operating profit of the 1000 industries and we have compared it with the average profit of the security industries. The values obtained, however, do not show a significant difference (6.4% against 5.1%). The slightly lower value of the security industry certainly is not an indicator of an efficient market, or a market where entry conditions may create some market power which could have a negative effect on market performance.

RESUME AND CONCLUSIONS

This chapter has made an initial analysis of the security market performance. As has been seen, this market shows a reasonable competition to assure a good performance forcing the industry to allocate efficiently its resources, search for productive efficiency and innovate in order to survive and prosper. Suppliers tend to be enough large to assure a good competition, whereas large size assures a good performance in the production of massive equipment. Yet, there are cases, were efficiency of the market can be compromised. This may be the case of public procurement where only a few number of companies are able to bid, or the case of manned guarding companies which exhibit a large concentration whilst innovation is rather low. Fragmentation is high in installers and small size guarding companies. Such fragmentation, however, may impair the productive efficiency.

The market incentive to increase dynamic efficiency in terms of better and innovative products is hampered by expected benefits. Small size markets and the complexity of innovation do limit the willingness of industry to strive for a good dynamic efficiency. Government intervention may help to solve this market failure, however not without cost and distortion. Standard able to achieve network economies may be also subject to market failure. In both cases, State intervention may be helpful. A model that explains

dynamic efficiency applicable to the security equipment market with examples has been also shown.

A short analysis has been made of performance indicators. However, this analysis is too preliminary and requires further work to derive more reliable conclusions and potential industrial policies.

IX. SUMMARY AND CONCLUSIONS

After having made a complete survey of the European security industry, this chapter tries to briefly sum up the main findings of the survey. It describes the main market features and examines the most relevant market trends. The different vision of security in the USA and the EU and its impact on the market is assessed with some detail. Some conclusions that can be derived from the collected information and the analyses already made are presented. As an afterthought, areas of potential policy are briefly evaluated. Finally, a proposal for future research on the security industry is drawn.

MARKET FEATURES

The industry that supplies goods and services to combat terrorism and organised crime exhibit some features that can be resumed in the next points.

A market composed of very different types of industries

The security market includes very different types of products and services that are supplied by very different stakeholders in terms of technology, cost structure, size, manufacturing methods, supply chain, revenues, customers, etc. Therefore patterns applicable to this economic sector are not many; and they only emerge in specific market segments. Electronics, information and communication technologies are probably the key and more pervasive technologies integrated in nearly any kind of security equipment. This is because many security solutions rely on screening and early warning where these technologies play a key role. The wide capabilities of these technologies seem often to promise security without burden nor cost.

A demand not only driven by the threat of terrorism and organisation crime and technology

The demand of security goods and services seems to be mainly driven by the threat of terrorism and organised crime as well as their capability to counter these threats in an effective way. Yet, the bounded rationality of human beings for performing complex cost-benefit analysis as well as interdependencies and externalities may compromise the chance of an optimal resource allocation to achieve security. However, when security practices become well accepted rules by society –where ethical issues can play its role– demand becomes more stable and more subject to overall society growth, as for example trade flow, travel flow, construction, etc.

Security product often applicable to other societal needs

Security equipments and services are often applicable to solve societal needs unrelated to security. For example, remote home surveillance services may be used also for healthcare and warning of home accidents. Personal identification cards used in borders may also be used to exert vote rights, request health services or manage bank funds. Technologies in this market also tend to show a higher duality than defence equipment. Equipment originally developed for civilian needs is also applicable to security needs like X-ray screening system. Adaptation seems also to be less complex than civilian technologies applicable to defence needs since products are often less complex and

operate in a less harsh environment. Therefore, technological spin-offs and spin-ons seem to be more likely in this market.

Equipment industry located in more industrialised EU member states

The EU equipment security industrial base is mainly located in the more industrialised member states, namely United Kingdom, Germany, France and Italy[215], whereas others states play a comparatively smaller role. Many of these industries operate with a European (and global) dimension. These companies have, apart from representation offices, production facilities (e.g. Siemens, Bosch) in other Member States as well as abroad.

Products and services that benefit of large economies of scale of development and production determine a market with a short number of large companies and European or World champions. Being economies of scale not so large medium size companies are more numerous. For example CEIA, one of the largest world suppliers of airport metal detectors, is not too much bigger in personnel than an SME. Distributors and installers of home and small business alarm systems tend to have a smaller size and sometimes a very small size.

Major suppliers division of large industrial conglomerates or business groups

Major security suppliers are divisions or business units of large diversified conglomerates that operate in more that one market as for example EADS Defence and Security, SAGEM Defence and Security, Thales Security Systems, Ericsson Security Systems, ELSAG Datamat (Finmeccanica), or Detica and Chubb (UTC) owned by BAE Systems. This industrial structure has sense since these companies operate in areas with similar technologies, such as electronics, information and communication technologies, where synergies can happen easily. Yet security is not frequently the principal business of these organisations.

A market of small size

The security market is of small size when compared with the whole size of the economy (0,48% of the European GDP in 2007) and other economic sectors (8,81 % of the total revenues of the ICT market). The growth rate in the last years has been good with a value higher that inflation, but the impact of general economic downturn is having a negative impact still unknown. In short, protection against terrorism and organised crime is a real concern, but it does not represent a large business opportunity for the industry.

The revenues in some market segments combined with the risks and costs of developing the demanded products and services creates few incentives for new entrants and innovators due to low expected profits in comparison with richer opportunities that other commercial markets present to many promising technologies today. This may result in slow-pace technological progress due to the limited availability of resources and expertise. For example, the development of integrated circuits are essential to miniaturize solutions and reduce equipment price, but it is less attractive than the design

[215] According to Eurostat, these member states accounted for the 62,66% of the European GDP in 2008.

of chips for mobile communications, gaming, or personal digital assistants that today are massively produced and sold.

Security services have the largest market share

Security manned services probably share the big part of the cake, close to one half. Electronic surveillance equipment based on CCTV is the most important part of the security equipment demand. Perimeter control, access control systems, and computer security are the other relevant market segments.

Research, technology and innovation is a key feature

A demand quite elastic to new products, whose quality and performance enhances security, promotes a market driven by innovation and technological progress. This means that research, development and technology play a relevant role in nearly all market segments, since user's needs often demand goods and services on the verge of the state of art and industrial proficiency. For example, some technologies such as sensors used in inspection and detection of CBRNE have a large maturing process due to the need of a low false alarm rate. While, in many cases, technology may be brought from other areas to be finally integrated into the security solution, in other cases tailored research is essential to improve product performance such as for example biometric e-passports. Radical or disruptive performance is the basis of competition in brand new markets, whilst incremental performance and process innovation drives more mature markets. The ownership of advanced proprietary technologies, whether related to the product design or the manufacturing process, often lays down the competitive position of companies. The presence of security related companies in the EU Industrial R&D Investment Scoreboard is an indicator that research, development and innovation play a key role in this market. Yet, the diversity of the industry may show large variations across market segments and company size.

A large supply chain

The supply chain for development or production of security equipment is usually large, especially in complex solutions. It may include public bodies, research centres, universities, laboratories, standardisation bodies, SMEs, system suppliers and prime contractors. This chain is becoming more international as a way to increase best value for money. Many components and intermediate products in the supply chain have additional use in other sectors and often the security market is not the main buyer (e.g. communication systems). Two forces shape this supply chain: technical specialization tends to deverticalize the market, whereas system complexity tends to increase the size of the supply chain. On the other hand, regarding the supply chain of manned guarding services, it seems to be rather simple.

A market where network economies play a relevant role

The security market is characterised by network economies and externalities. In such markets, competition rules may not be enough to achieve optimum allocation of resources to provide the goods and services that society demand. Coordination from the demand and the supply side may be suitable to achieve a better outcome. From the demand side, it may require coordination of security measures as for example

agreements on the provision of security services and the equipment to use. From the supply side, it may require the development of industrial standards that certifies equipment minimum performance or assures interoperability. In these cases, the development of voluntary governance mechanism (Williamson, 1985:chapter 1), state intervention or supranational agreement) is necessary. Since the outcome of State intervention may result in mandatory regulations with strong social or economic impact as for example transport, a careful analysis is required to assess the costs and benefits of such measures in order to maximize social welfare.

A market where the government plays a key role

The government plays in this market an essential role as entrepreneur, aid provider or sponsor of the industry through aids and the finance of research, purchaser of solutions that will increase society security, and regulator when the market mechanism does not assure automatically the desired security level, or deliverable products or services do not assure minimum quality standards. Anyhow, private security needs largely shape the demand in this market.

A market largely internationalised where the USA plays the leading role

The security market is largely internationalised, operating many industries on a world basis. In this market, the United States industry plays a leading role. Many U.S. companies operate in Europe (e.g. GE, Honeywell or L-3), but the opposite is also true, and some European companies like Siemens, Bosch, or Sagem successfully operate in the USA market despite potential barriers[216], playing also leading positions in the world market.

Whereas U.S. leading role can be explained by the general economic and industrial leadership of this country, it is also a consequence of the powerful investment in new security solutions supported by the Department of Homeland Security that provides powerful incentives to the industry for innovation. This provides competitive advantages to its industry over European and other world industry.

Far East security industry is becoming also very competitive in some market niches such as CCTV cameras, biometrics and computer security, for example NEC Argentina won the Bolivian voting cards, and Hyundai has supplied the Egypt AFIS system. Whereas competitiveness is mainly sustained by low price of electronic components due to labour cost advantages, in other areas competition is becoming more based on the product quality and performance.

MARKET TRENDS

Areas of future growth

Security is an evolving concept. Growth of the market depends on the threats that society perceives, the policies applied to increase the feeling of security, the adaptation of governance structures to effectively deal with these matters, but also on the evolution of technology to reduce these threats. The kind of terror attacks and the kind of illegal

[216] See ECORYS (2009:63).

activities of organized crime will have a deep impact on future market needs as dramatically showed 9/11 attacks. Hence changes in the market demand and the industry can be expected if security incidents become more frequent and dangerous as well as threats cannot be countered with current equipment due to changes in tactics and means of these groups. Being the case, novel products and services and new manufacturers are expected to appear in the market, other things being equal. As long as the technologies are available, products will appear easily. However, products with breakthrough performance and falling price, able to remove important vulnerabilities and deter from potential attacks, will require large investment in research, if their development cannot be nurtured by discoveries coming from other economic sectors.

Small and medium sized companies as well as the residential market will continue to spend resources in security, though their sensitivity to price will only trigger their demand when security goods and services are rather inexpensive. This demand will be mainly leaned to the protection against crime and theft.

Governments and large organizations managing or operating critical infrastructures will continue to be the main purchasers of security in the next years, stimulated by security concerns, which materialise in programmes like the EPCIP. Surveillance, physical protection, and access control will continue to be the major contributors to abate the risk of terrorism and organized crime. Inspection equipment for baggage and cargo will continue to grow as trade continues to expand. Progress on CBRN protection equipment seems to be uncertain as long as this threat does not clearly manifest.

New technologies that show a growing trend in the next years are digital video surveillance, smart cards, biometric systems, and RFID. Biometrics and smarts cards seem to be the future technology that will override the older type of identification cards based on a magnetic stripe. The new technology will help to expand the identity market, a basic enabler of many services that will not need face-to-face relation for their supply from access control to e-government and e-finance.

The expansion of these technologies depends on uncertain conditions like R&D progress, user acceptance, affordability, adequate standards, and regulations that being not met may hinder their growth. Moreover, progress in these areas may be more driven by other societal needs and goals and non-exclusively with the fight against terrorism and organized crime like the abovementioned e-government and e-finance.

New EU member states may be especially demanding of security equipment due to quicker economic growth, raising cost of labour-intensive security services and small installed base.

Security and defence companies

The new perception of security threats in the European Union devaluates those threats related to territorial defence and armed conflicts based on sophisticated and technologically advanced weapons, while rises threats generated far away of the European borders proceeding from State failure and disintegration and threats which may facilitate radicalisation and promote terrorism and organised crime (Pullinger, 2006).

This environment hence restrains the need of traditional defence in favour of security. Such a change has attracted the defence industry to offer its solutions to undergo the new threats posed by terrorism and crime. This is facilitated by the commonality of many technologies used for defence and security, the large experience of defence companies in managing large and complex programmes aimed at achieving new capabilities, and the good knowledge of the end customer.

This is seen by the defence industry as an opportunity to diversify their portfolio, gain a foothold in this market, and increase its share of the security business in the company turnover (Dowdall, 2005). The EU (2009) report on the security research programme shows clear evidence of the defence industry competence to become the main recipient of funds. Furthermore, many research organisations like the Swedish Defence Research Agency (FOI), VTT, SINTEF, Dutch Research Institute (TNO), CEA or Qinetiq traditionally working for defence are now turning their focus to security issues. This industry is mainly involved in programmes like border protection, maritime surveillance or CBRNE[217]. This trend probably will continue in the future and may even increase if defence budget shrinks and security budget grows faster.

The permanent need of research and development

Research, development and innovation will continue to play a relevant role since threats of terrorism and organised crime poses big challenges to the industry in terms of equipment performance, effectiveness and affordability. While this market could profit of overall technological progress, it will also need R&D activities to advance in specific areas and integrate new and more powerful technologies in future products. Some security solutions, such as explosive detection or chemical and biological agent detection, will need of fundamental advances in science and technology to solve current shortfalls and deficiencies. Moreover, since terrorists' behaviour will not be static in the face of enhanced security measures and will be inventive in developing new ways to circumvent them, a permanent R&D capability seems essential to continue defeating the new threats. Yet, incentives may not be enough for industry to achieve desirable advances if demand is too scarce.

CONCLUSIONS

This survey has shown that the security industry can provide goods and services that integrated with the adequate procedures can largely enhance the security of citizens and consequently the welfare of society. Yet, security equipment and security services have inherent limitations to remove insecurity and the root causes of terrorism and crime. Equipment may fail, be poorly integrated or be wrongly operated. And services may not follow best practices. Social engineering and human negligence may easily create breaches and put security at risk. It should not be forgotten that security solutions have a socio-technical nature mixing technical and non-technical design. Departures to attend

[217] This trend can be observed also in the United States. For example, the SBInet program, the surveillance system of the Secure Border Initiative was awarded in 2006 to Boeing Corporation. Northrop-Grumman is involved in the new Automatic Fingerprint Identification System for the United Kingdom. The top 25 Homeland Security contractors (http://www.govexec.com/features/0809-15/0809-15s10s1.htm) is led by companies like Boeing Co. (1), Lockheed Martin (2), General Dynamics Co. (5), L-3 Communications Holdings (8), and QinetiQ Ltd. (13), and BAE Systems (22).

the human, political, social, operational and organisational aspects of solutions will doom technology to failure and give easily pace to vulnerabilities.

The industrial impact of a different vision on security on each side of the Atlantic

The strategic outlook, the threat perception and the role of technology for improving security clearly differs between the USA and the EU when we compare the different approaches followed on each side of the Atlantic. The 9/11 attack boosted investments on security in the United States. The creation of the Department of Homeland Security and the Homeland Security Advanced Research Projects Agency (HSARPA)[218], an agency similar to DARPA but focused on security, demonstrate a clear pledge to reduce security shortfalls pushing technology ahead[219]. The DHS large budget has allowed the financing of many research and development programmes (e.g. protection of big cities against a WMD based on detector equipment installed in the main highways). This approach goes beyond European efforts to increase its security, this suggesting a more prudent, less ambitious, and probably more rational approach on this side of the Atlantic.

Industrial differences, consequently, are closely related to the different vision of security to both sides of the Atlantic, which translates into different demands and different industrial responses, rather than irreversible gaps in industrial capabilities. Namely, Europe has a strong position in many enabling sectors of security like aerospace, defence, telecommunications, software, biotechnology or pharmaceutical (Ecorys, 2009:x). However, the U.S. approach has an inherent adverse effect on the European security industrial base. The large DHS budget is pushing ahead technological solutions due to the generous financing of R&D and acquisition programmes that gives its industry advantages in terms of products with higher performance and lower cost[220]. This financing facilitates the quick development of products ready for the market and the creation of new champions. In such context, it can be expected that U.S. companies will attempt to achieve above normal profits marketing their products worldwide, having a good chance to compete with success with less developed European industries and to consolidate a solid export position. Moreover, the higher expertise of the U.S. industry is an asset when international standards are defined, because it may progressively impose (*de facto*) normative and operational standards worldwide that inevitably will favour the U.S. industry (See COM (2004) 700: page 21 and the e-seals for containers).

---

[218] This agency funds R&D of homeland security technologies to *support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities*.

[219] This may be less motivated by the outcome of an objective assessment of security investments and more by a wider strategy with emphasis on technological leadership that provides long-term competitive advantages in the world trade (Krugman, 1996:110). Such strategic behaviour (i.e. maintain a hedge towards Europe) could mean a limited chance of collaboration when sharing with Europe the positive externalities of a large R&D budget is not seen as a priority for doing business. The European Commission and the United States signed the 18th November 2010 an Implementing Arrangement for cooperative activities in the field of homeland/civil security research. The Arrangement does not create financial obligations.

[220] In a market where marginal costs fall as output increases, a large demand that increases the output of home firms is doubly beneficial: directly, because it lowers the cost of production, and indirectly, because it makes domestic firms more competitive on foreign markets (Martin, 1993:404).

In sum, whereas Europe receives positive externalities of the USA large investments in security, it can also be said that the European industry operates in a somehow adverse environment, because the chance to differentiate by means of large R&D investment may be small due to limited resources. This environment may impact negatively on the exporting capability of the European Union in foreign markets such as South America, Asia or Africa when American companies also bid. In such case, follow-up and defensive innovative strategies like better adapting early discoveries, i.e. cherry-picking the best bits and avoiding the mistakes already made, combined with other strategies, such as product differentiation or better manufacturing and commercialization infrastructure, may have a role in preserving the competitiveness of the European industry[221].

Benefits of consolidating the European security market

A market like security, where economies of scale and network economies are so relevant, will benefit of a true European dimension, since a larger number of customers will make easier the attainment of such economies and will provide a more stable (i.e. less cyclical) demand for many security solutions. Such a market will reinforce the European industrial base.

As we have seen, the security market in Europe cannot be considered fragmented by national borders, yet barriers exist that impede a stronger competition such as differences in national regulations and standards and the traditional preference of national suppliers in large public purchases. Probably, there is still room to improve a level playing field. A wider market will create incentives for industrial concentration to achieve a European dimension, a desirable feature since it is also recognised that the number of companies operating in the sector is often too high. Consumers will benefit of stronger competition and a more efficient industry in terms of better, innovative and less expensive goods and services.

The increasing competition across EU Member States will lead to the concentration of sales in the hands of the largest and more efficient firms (Martin, 1993:192). Such transformation could involve market restructuring. While long-term benefits will be positive, the restructuring process may create short-term imbalances in terms of plant closures and job losses of the less efficient firms.

Benefits of EU security research

R&D competition may be desirable for certain security equipment even if duplication or parallel research appears (Porter, 1990:636) when such uncoordinated innovation efforts are subsequently coordinated by markets (Metcalfe, 2002:2) which will in the end value the innovation. But this approach may be less justified for large and complex systems purchased by governments where national budgets are too strait to finance such research. In such cases, cooperation of member states in the field of research, development and innovation may have sense since it will facilitate the pooling of resources, the creation of more powerful research teams and the appearance of synergies and economies of scale, which will increase the likelihood of a better and less expensive

[221] This has been the strategy of Airbus 'be later but better' (Sutton, 2001:469).

solution. Examples of such kind of systems are border protection, maritime surveillance, patrol aircrafts, or satellite surveillance. A coordinated research will also help to cover potential research gaps and control duplication that may result in excessive resources waste when programmes are large[222].
Coordinated research, however, does not come without cost. Barriers and rigidities to collaboration from the demand and the supply side may be a source of suboptimal solutions with a true adverse impact on the market. For example, these developments call for the harmonisation of requirements from different end users, in order to simplify the complexity of the product, and may need previous agreements on best practices or standards. Such harmonization has a considerable cost in terms of time and resources. The formation of international consortia may also take time, and bargaining on the agreed distribution of work may predominate over the efficient criterion in the allocation of resources (Hartley, 1995:457). As a conclusion, it can be said that joint research may not be always the best solution. Furthermore adequate governance infrastructure is needed to achieve such coordination[223].

ESRIF (2009: 202) advocates strongly for '... *Field labs are needed for the validation (verifying whether it is fit for purpose), i.e. realistic environments for the demonstration, validation and optimisation of innovative systems for security tasks or meeting points where end-users, security authorities, industry and the research community can have access to the technological solutions relevant for their daily work*'. While not explicitly said, the text assumes field labs of European dimension. This kind of initiatives certainly will have a positive effect on quality and cost, yet it may face with reluctance of Member State that may still consider security, a concept closely tied to national sovereignty (Enders and Sandler, 2006:142).

Benefits of reusing defence and civilian expertise

The challenges of security require the amassing of expertise, know-how and resources to succeed in the development of solutions. For example, the large experience attained in the defence field in the area of intelligence, surveillance and reconnaissance as well as command and control can fertilise the development of many security solutions such as the already known as 'Network Enabled Capabilities'. Advances in many areas of the civilian sector may also be reused in the field of security. In particular advances of electronics, information and communication technologies financed by other sectors may push ahead the development of new and improved systems such as smart cards, RFID tags, mobile communications, etc.

Profiting of integrating security in civilian products and services

It is reasonable to believe that the EU has enough technological and industrial base to develop security systems and solutions, but without commercialization prospects, the development of these systems is very unlikely. Since pay-off of many protective measures, especially against terrorism, is hardly measurable, due to the difficulty to assess the threat and its consequences before and after the measure is implemented, the need to improve and spend in security may be lacking.

[222] Here the European Research Framework Program plays a very positive role.
[223] This raises the question whether a European Security Agency could be a good solution to correct failures to achieve the economic benefits from international collective action. Such action is requested by EOS (2009) industrial association.

To overcome such problem a likely successful strategy would be to focus explicitly on technologies that, in addition to counter terrorism and organised crime, have broader applications. Research with multiple uses like defence or the civilian market may have, therefore, sense and will bring higher and more tangible pay-offs.

This approach would help to reduce vulnerabilities and, at the same time, enhance reliability, productivity, quality of services, or the provision of new commercial capabilities as examples shown in chapter III. Such strategy needs a careful assessment of advantages of the research for security as well as to other economic fields. Introducing security requirements in the early stages of the design of a new system may help to reduce costs instead of introducing them later on (ESRIF, 2009:17). However, markets do not reward always such behaviour. Rather, markets reward first movers – that is, those companies who are first in bringing a new product to market. This means that it is more important to get into the market early rather than first investing in improving product security (Anderson, 2001a).

The complexity of properly allocating resources to security

Protecting society from terrorism and organised crime is hard to achieve. Measures are always expensive and resources limited. Determining how much to spend and in which areas is always difficult. Furthermore, asymmetry of information and the inability to protect everything, since hardening of every target is unrealistic for the economic point of view, give always advantages to terrorism and organised crime to find and hit a weak spot. The damages that a terrorist group may cause are in most cases considerably larger than the cost of organising and performing the attack, and sometimes disproportionately higher as the 9/11 has shown.

One of the ultimate objectives of terrorism is to impose economic hardship on the targeted country. This strategic rationality has been manifested in explicit statements by Osama bin Laden, among others. For example, he crowed about the positive exchange ratio between the cost of the September 11 attacks and the cost of its consequences to the United States (Davis, 2009:xxxiii).

A big challenge is that these threats claim a significant fraction of the discretionary resources that might otherwise be invested in ways that pay broader dividends over time. In such a case, the impact of those expenditures may be disproportional to the costs caused by the attack themselves. Security and preparedness measures shall be warily designed so that the resources devoted to them do not end up generating the very costs that a terrorist aims to impose. This argument brought by Jackson *et al.* (2007b) is analysed also by Sandler (2009) when he ponders the security spending of USA on the order of magnitude of tens of billions of dollars, compared with the money saved from reduced damages in the order of millions. Stewart and Mueller (2009) also raise this question when they evaluate USA homeland security spending and estimate cost per life saved (using the value of a statistical life) to determine the rationality of these expenditures and assess alternative investments to mitigate the risk of other hazards (e.g. vehicle and road safety, health programmes or flood protection) that could be more cost-effective (i.e. more lives saved).

The allocation of resources to security should be optimal and decisions should be based on a balanced analysis of benefits of mitigating the risk and its consequences against both the economic cost of developing and deploying some security solutions. Hence, tolerating some level of insecurity is economically rational when costs outweigh benefits. While no mathematical formula can reveal the appropriate balance and decisions are made in an environment of bounded rationality, principles of transparency, accountability, and informed judgement may help to avoid large imbalances and resources misallocation. This may require of adequate information to take into account the full range of costs and benefits combined with analytical methods and tools to evaluate program performance in order to support the final decision[224]. Rational decisions, rather than emotional based decisions based on alarmism and excessive weighting of worst case scenarios without assessing its likelihood (Sunstein, 2002), should rule decision making in security investment to avoid hyperbolic overreaction to improbable contingencies. As Mueller (2005) states 'If terrorist force us to redirect resources away from sensible programs and future growth, in order to pursue unachievable but politically popular levels of domestic security, then they have won an important victory that mortgages our future'.

The field of information security is being especially rich on research on how much to invest in computer security. Gordon and Loeb (2002) present an interesting paper to assess the optimal investing amount to protect a given set of information. Their analysis suggests that, under plausible assumptions, investment in information security may well be justified only for a midrange of information vulnerabilities. That is little or no information security is economically justified from extremely high, as well as extremely low, levels of vulnerability since the reduction of the expected loss will not justify the investment. It also suggests that to maximize the expected benefit from investment to protect information, a firm should spend only a small fraction of the expected loss due to a security breach. The argument seems still valid when applied *ceteris paribus* to general investment in security.

Box 10. How much is enough in security investment

Potential areas of industrial policy

The security market, as has been shown, is subject to inefficiencies and failures with an adverse impact on its performance in terms of expensive products with low performance, innovativeness, or international competitiveness. Reasons may be due to lack of coordination between agents, barriers to competition, industry strategic behaviour, low innovation incentives, excessive risks, low initial demand due to network effects, limited capital access, technological obsolescence, or high-tech skill dependence[225].

Governments may play an important role in changing market dynamics consistent with the public interest when failures and inefficiencies appear. Yet, government action should be grounded on sectoral studies to implement adequate solving measures and

[224] On a critique of DHS methods for evaluating program performance and effectiveness, see Thomson (2007) and GAO (2010).

[225] No general document on EU security industrial policy has been identified, as opposed to defence where some official documents exist. This suggests that little attention has been already paid to this industry.

should consider costs and benefits to ensure that intervention is both proportionate and appropriate.

Lack of information may be a main source of poor market performance such as for example reliable data about vulnerabilities and attacks. A policy option could be therefore the collection and publication of information to foster better investments, as for example CERT teams. As Tirole (1988:109) states when deciding whether to become informed, a consumer takes only the private cost and the private benefit into account, but he or she does not take into account the fact that, by being better informed, he induces (or allows) the firm to credibly offer the high quality. So it can be inferred that increasing the number of informed customers favours efficiency. Thus consumers' information should be encouraged beyond its privately optimal. However, as Spulber (1989:64) advices, the welfare gains from improved information flow to participants must be compared with the costs of government production of information. The need of policy action in markets with asymmetric information may thus depend on the trade-off between the costs of information production and the costs of inefficient transactions.

The *tipping* tendencies of economic competition, described in the previous chapter, like too few firms, excessive market dominance, slow or distorted technological development, high prices for hardware and software, possibilities for overt or tacit collusion among suppliers and integrators (Cave, 2005) may be also a source of poor performance in market segments where network effects play a critical role such as biometrics and RFID.

State R&D financing and public purchases may help to keep up with new security threats through the development of efficient and affordable countermeasures. Yet, this support is not easy to provide. As NRC (2002:351) states 'the facilitation of technology development will be a complicated task for governments. It is very difficult to define goals for such programmes, support the necessary scientific and engineering research, facilitate the maturation of technologies into robust products, and eventually ensure that these products are implemented by appropriate users'. The main challenge is to allocate resources to potential innovations that do match with market needs, whilst avoiding the *tipping* tendency that R&D financing may help to increase.

Providing this support, while keeping up a fair competitive environment, is not an easy task not being enough openness, transparency, objective awarding and rigorous monitoring of aids. Additional measures required include: (a) precompetitive R&D engagement, (b) multiple-sourcing arrangement something that may be inefficient in natural monopoly markets; (c) a careful design competition on major procurements; (d) technologically neutral requirements or based on open standards, (e) open and transparent supply chain management, and (f) the inclusion of some form of compulsory licensing of IPR option arrangements in procurement contracts based on fair, reasonable and non-discriminatory (FRAND) criteria (Cave, undated, 2005).

The motivation to provide aids mainly resides in the public interest of enhancing security when market mechanism fails. This would mean that decisions should be focused mainly on security projects with large impact and benefits to society, that otherwise would not take place. It would also mean that aid intensity should be tamed by the size of demand, commercialisation prospects in other economic sectors, or spin-offs with large impact on the economy. This probably explains that much research in

security today is oriented to dual technology markets such as ICT, robotics, biotechnology or aerospace, which are believed to the essential for the future competitiveness of the European industry in world markets (Tisdall & Hartley, 2008:177). It may well be that such believe may discretionarily outplace projects that could embed higher social gains.

Coordination may be especially required for setting (interoperability) standards and fixing minimum security requirements since they might be essential to boost market demand[226]. The support for their development may be important when private agents show too much inertia. Monitoring is also required to avoid strategic behaviour aimed at reducing opportunities of competitors during the development of standards. This may be the case when industry led standard consortia hide collusive practices; when a provider with large market share deliberately makes its equipment incompatible with rivals offering, or when the holder of a key patent effectively controls all those who use it. An RTD policy, where access to research results is open, could promote diversity; balance scale and scope economies with economic efficiency; restrain vertical foreclosure whilst encouraging appropriate integration; and inspire further product and process innovation (Cave, 2005).

THE NEED OF FURTHER ECONOMIC RESEARCH

This study shall be seen as another step to abate ignorance regarding the European security industry. It has shown the often elementary knowledge we have on this (complex) economic sector and the scant information that impedes a better characterisation and further progress in the understanding of this market. Datasets are not enough rich to discover evidences, make inferences and empirically confirm hypotheses. Many hypotheses have been only suggested, pending to be fully tested, and there are insufficient evidences to refute or sustain some interesting conjectures. In short, evidences found are often too anecdotal to be useful.

Consequently, efforts are needed to gather on a durable basis such information (in particular quantitative data), allowing that researchers exploit it to better understand the structure and behaviour of this industrial sector and, thereby, identifying more accurately potential performance troubles in the market. Compiling such information involves an important, but necessary, effort to progress in the research and to avoid skewed conclusions that may sustain inappropriate industrial policies.

Main information shortfalls are the accurate measure of market demand across market segments and customers, imports and exports, and government research and development financing. From the supply side a better characterization of the industry is needed in terms of turnover, employees, sales by relevant markets, suppliers, customers, R&D investment and other economic indicators. Only a rich information base may open the door to econometric studies that are badly needed in this area.

For the future, there is no shortage of research questions in the security market. For example better knowledge is needed on cost structure in development and production and the role of economies of scale, scope and learning on each market segment. More

[226] Failures to achieve standards have occurred in the past. For example a pan-European identification card has not been achieved, thus limiting e-government solutions on member states. It seems that there is room for improvements in this area.

progress is needed in unveiling differences between security, defence and civilian firms as well as assessing linkages and synergies between these firms, fruit of the exchange of knowledge and technology. Finally, more insight is needed in characterising government role and procurement policies and potential non-optimal decision making. A more precise characterization of the conduct of market agents is also needed. Finally, econometric studies on market performance using different indicators would help to determine more accurately the health of this industry.

ACRONYMS

ACE	Automated Commercial Environment
AFIS	Automatic Fingerprint Identification System
AIDS	Acquired Immune Deficiency Syndrome
AIS	Automatic Identification System
ASTM	American Society for Testing and Materials
ATM	Automatic Teller Machine / Air Traffic Management
BAA	British Airport Authority
BSL	Biosafety Level (1, 2, 3, 4)
CAD	Computer Aided Design
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CCTV	Close Circuit TeleVision
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEO	Chief Executive Officer
CFCA	Community Fisheries Control Agency
COTS	Commercial Off the Shelf
CT	Computer Tomography
DARPA	Defence Advanced Research Project Agency
DHS	Department of Homeland Security
DVR	Digital Video Recorder
EDA	European Defence Agency
EEA	European Environment Agency
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EPCIP	European Programme on Critical Infrastructures Protection
EPOSS	European Technology Platform on Smart Systems Integration
ERFP	European Research Framework Programme
ERP	Enterprise Resource Planning
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research Information Forum
ETSI	European Telecommunications Standard Institute
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
EUROSUR	European Surveillance System for Borders
EUSECON	European Security Economics
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Members States of the European Union.
GAO	Government Accounting Office
GDP	Gross Domestic Product
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HEPA	High Efficiency Particulate Arresting
HEU	High Enriched Uranium
IAEA	International Atomic Energy Agency
IATA	International Aviation Transport Agency
ICAO	International Civil Aviation Organisation
IC	Integrated Circuit

ICT	Information and Communication System
IED	Improvised Explosive Device
IMO	International Maritime Organisation
IPR	Intellectual Property Rights
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ISPS	International Ship and Port facility Security Code
IT	Information Technology
ISDEFE	Ingeniería de Sistemas de Defensa
JRC	Joint Research Centre
LAN	Local Area Network
LCD	Liquid Crystal Display
LRIT	Long Range Identification and Tracking
MANPADS	Man Portable Air Defence System
MES	Minimum Efficiency Scale
NACE	Statistical classification of economic activities in the European Community.
nec	Not elsewhere classified
NIJ	National Institute of Justice
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
PASR	Preparatory Action on Security Research
PC	Personal Computer
PDA	Personal Digital Assistant.
PMR	Professional Mobile Radio
PIRA	Provisional Irish Republic Army
POS	Point Of Sales
PPE	Personal Protective Equipment
PTZ	Pan, Tilt and Zoom
R&D	Research and Development
RF	Radio Frequency
RFID	Radio Frequency Identification
RPG	Rocket Propelled Gun
RTD	Research, Technology, Development
SCADA	Supervisory Control And Data Acquisition
SIS	Schengen Information System
SSL	Secure Socket Layer
SME	Small and Medium Enterprise
TCP / IP	Transmission Control Protocol / Internet Protocol
TETRA	Terrestrial Trunked Radio
TFEU	Treaty of the Functioning of the European Union
UAV	Unmanned Air Vehicle
UNO	United Nations Organisation
US-VISIT	U.S. Visitor and Immigration Status Indication Technology
VIP	Very Important Person
VIS	Visa Information System
WMD	Weapon of Mass Destruction
WP	Working Package

REFERENCES

Ackerman, Gary A. and Moran, Kevin S. (2006). Bioterrorism and Threat Assessment. Prepared for the Weapons of Mass Destruction Commission. Paper no. 22. Stockholm.

Acuity Market Intelligence (2009). The Future of Biometrics. Market Analysis, Segmentation and Forecasts. Insight into the Trends, Drivers and Opportunities that will shape the Industry through 2020. Available at http://www.acuity-mi.com.

AeroAssit (2008). RFID in Aviation: Airport Luggage Control. An AeroaAssist white paper.

Anderson, Ross and Moore Tyler (2008). Information Security Economics and Beyond. University of Cambridge Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK.

Anderson, Ross E. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons. New York.

Anderson, Ross E. (2001a). Why Information Security is Hard. An Economic Perspective. University of Cambridge Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK.

Anderson, Ross, Böhme, Rainer, Clayton Richard and Moore, Tyler (2007). Security Economics and the internal market. ENISA report.

Becker, Gary S. (1968). Crime and Punishment: An Economic Approach. The Journal of Political Economy. Vol. 76, No. 2 (Mar – Apr) pp. 169-217.

Brookson, Charles and Zumerle, Dionisio (2006) Security for ICT - the Work of ETSI ETSI White Paper No. 1. Sophia Antipolis Cedex, France.

Brown Chad (2006). Transcendental Terrorism and Dirty Bombs. Radiological Weapons Threat Revisited. Occasional Paper No. 54. Center For Strategy and Technology. Air University. Maxwell Air Froce Base, Alabama.

Don, Bruce W., Frelinger, David R., Gerwehr, Scott; Landree, Eric, Jackson, Brian A. (2007). Network technologies for networked terrorist. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations. Prepared for the Department of Homeland Security. RAND. Santa Monica (CA).

Brück Tilman, Karaisl Marie, Schneider Friedrich (2008). A survey of the Economics of Security. Economics of Security Working Paper 1. Deutsches Institut für Wirtschaftsforschung, Berlin.

Bush, George W. - President (2002). The Department of Homeland Security. Washington D.C. Available at www.dhs.gov/xlibrary/assets/book.pdf (03/05/2010).

Carafano, James Jay. (2008). Fighting Terrorism, Addressing Liability: A global Proposal. Published by the Heritage Foundation. No 2138. May 21, 2008. Washington D.C.

Cave, Jonathan (2005). Economic Aspects of Biometrics. Background paper for the Institute of Prospective Technological Studies. DG JRC, European Commission. Sevilla.

Cave, Jonathan (undated). Competition and procurement. Rand Europe. Cambridge (UK). Draft.

Chalk, Peter (2008). The Maritime Dimension of International Security. Terrorism, Piracy and Challenges to the United States. Rand. Santa Monica, CA.

Civitas Group (2006). The Homeland Security Market. Essential Dynamics and Trends. Available at www.civitasgroup.com.

Civitas Group (2007). The Nuclear and Radiological Security Market. Available at www.civitasgroup.com.

Coase, Ronald H. (1937). The Nature of the Firm. Economica, New Series, Vol. 4, No. 16 (Nov. 1937) pp. 386-405.

Coase, Ronald H. (1960). The problem of social cost. Journal of Law and Economics.

CoESS – Confederation of European Security Services (2008) Private Security. Fact and Figures 2008. Available at www.coess.org/pdf/CoESS_Facts_Figures_2008.pdf (03/05/2010).

Daly Sara, Parachini John and Rosenau William (2005). Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor. Implications of Three Case Studies for Combating Nuclear Terrorism. Rand Corporation. Santa Monica, CA.

David, Paul A. and Greenstein, Shane (1990). The economics of compatibility standards: and introduction to recent research. In: Economics on Innovation and New Technologies, Vol. 1, pp. 3-41, Harwood Academic Publishers. London.

Davies, Simon and Hosein, Gus (2007) Identity Policy: Risks & Rewards. The London School of Economics and Political Science. London.

Davis, Paul K. and Cragin, Kim, Editors (2009). Social Science for Counterterrorism. Putting the Pieces Together. RAND National Defence Research Institute. Santa Monica, CA.

De Waard, Jaap (1999). The private security industry in international perspective. In: European Journal on Criminal Policy and Research, Vol. 7, pp. 143-174.Kluwer Academic Publishers. Amsterdam.

Defence Science Board – DSB (2004) Task Force on preventing and defending against clandestine nuclear attack. Office of the Secretary of Defence. Washington D.C.

Department of Defence - DoD (2009). Technology Readiness Assessment Deskbook. Prepared by the Director, Research Directorate (DRD). Office of the Director, Defense Research and Engineering (DDR&E) Washington D.C.

Dowdall, P. and Braddon, D. (2005) Revolution in the Defence Electronics Market? An economic analysis in sector change. Defence Economics Research Unit. University of the West of England. Bristol.

ECORYS Research and Consulting (2009). Study of the competitiveness of the EU security industry. Directorate-General Enterprise & Industry. Brussels.

ECORYS Research and Consulting (2010). FWC Sector Competitiveness Studies. Study on the Impact of Emerging Defence Markets and Competitors on the Competitiveness of the European Defence Sector. Directorate-General Enterprise & Industry. Brussels.

EITO (2007). European Information Technology Observatory yearbook.

Elias, Bart (2008). Aviation Security: Background and Policy Options for Screening and Securing Air Cargo. Congressional Research Service (CRS) Report for Congress. Order Code RL 34390. Washington D.C.

Enders, Walter and Sandler, Todd (2006). The Political Economy of Terrorism. Cambridge University Press. New York.

EPOSS (2009). Strategic Research Agenda of the European Technology Platform on Smart System Integration. Version 2. EPoSS Office. Berlin.

ESRIF – European Security Research and Innovation Forum (2009). Final Report. Part 2. Brussels.

European Commission – DG Enterprise and Industry (2005). ICT Security, e-Invoicing and e-Payment Activities in European Enterprises. Special Report (September 2005). Brussels.

European Commission – DG Enterprise and Industry (2007). Study Analysing the Current Activities in the Field of UAV. ENTR/2007/0065. Brussels.

European Commission – DG Enterprise and Industry (2008). RFID Adoption and Implications. A sectoral e-Business Watch study by IDC / Global Retail Insights. Final Report. Version 4.0. Brussels.

European Commission (2004). Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research. Brussels.

European Commission (2006). Faster and more united?. The debate about Europe's crisis response capacity. External Relations Directorate General. Brussels.

European Commision (2007). On RFID: The next step to the internet of things. Lisbon, 15-16 November 2007.

European Commission (2009). Monitoring industrial Research. The 2009 EU R&D investment scoreboard. Joint Research Centre. Directorate General Research. Brussels.

European Organisation for Security – EOS (2009). Priorities for a future European Security Framework. Brussels.

European Parliament (2008). Working document on problem of profiling, notably on the basis of ethnicity and race, in counterterrorism, law enforcement, immigration, customs and border control. Committee on Civil Liberties, Justice and Home Affair. Rapporteur: Sarah Ludford.

Europol (2008). EU Organised Crime Threat Assessment. The Hague.

Europol (2009). EU Terrorism Situation and Trend Report. The Hague.

Eurostat (2009). Panorama of Transport. Luxemburg.

Eurostat (2010). Europe in figures – Eurostat Yearbook 2010. Luxemburg.

Fatah, Alim A. (2000). Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders. National Institute of Justice Guide 100-00. Washington D.C.

Fatah, Alim A. (2001). An Introduction to Biological Agent Detection Equipment for Emergency First Responders. National Institute of Justice Guide 101-00. Washington D.C.

FEMA (2003). Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks. Providing Protection to People and Buildings. Report 427.

Freeman, Christopher (1986). The Economics of Industrial Innovation. The MIT Press, Cambridge, Massachusetts.

Frost & Sullivan (2004). Country Industry Forecast – European Union. Security Industry. 4624-90. Frost & Sullivan Ltd. London.

Frost & Sullivan (2005). European Homeland Security. A Market Opportunity Analysis. B447-16. Frost & Sullivan Ltd. London.

Frost & Sullivan (2005a). World Video Surveillance Equipment Markets. A952-11. Frost & Sullivan Ltd. London.

Frost & Sullivan (2006). European Residential Security Markets. M050-19. Frost & Sullivan Ltd. London.

Frost & Sullivan (2006a). European Industrial and Commercial Security Products and Systems Markets. B818-19. Frost & Sullivan Ltd. London.
Frost & Sullivan (2006b). European Radio Frequency Identification Tags. M06B-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2007). European CCTV and Video Surveillance Equipment Markets. M052-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2007a). Container Security. N15C-16. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008). European Electronic Access Control. Security Markets Quarterly Market Intelligence Update. M320-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008a). Opportunities in the European Intrusion Detection Systems Market. Quarterly Market Intelligence Update. M321-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008b). European Manned Guarding Market. M213-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008c). World AFIS Markets. N38D-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008d). European Security Services Market. M2E0-11.. Frost & Sullivan Ltd. London.
Frost & Sullivan (2008e). North American Video Surveillance Cameras Market. N29A-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2009). Distribution Channel Analysis for European Security Systems. M37D-11. Frost & Sullivan Ltd. London.
Frost & Sullivan (2009a). Biometrics in Europe—Future Technologies and Applications. 9834-11. Frost & Sullivan Ltd. London.
Gansler, Jacques S. (1980). The defence industry. The MIT Press. Cambridge, Massachusetts.
GAO (1996). Terrorism and Drug trafficking. Technologies for Detecting Explosives and Narcotics. GAO/NSIAD/RCED-96-252. Washington D.C.
GAO (1999). Combating Terrorism. Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. GAO/NSIAD-99-163. Washington D.C.
GAO (2002). National Preparedness. Technologies for Secure Federal Buildings. GAO-02-687T. Washington D.C.
GAO (2008). Supply Chain Security. Challenges to Scanning 100 Percent of U.S.-bound Cargo Containers. GAO-08-533T. Washington D.C.
GAO (2010). Department of Homeland Security. Assessment of Selected Complex Acquisitions. GAO-10-588SP. Washington D.C.
GAO (2010a). Supply Chain Security. DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended. GAO-10-887. Washington D.C.
Gartner (2009). Market trends: Security Market, Worldwide 2007-2013. Available at www.gartner.com/DisplayDocument?id=1107215.
Gartner (2009a) Market Scope for Managed Security Services in Europe. G00171027.
Ghose, Anindya and Rajan, Uday (2006). The economic impact of regulatory information disclosure on information security investments, competition and social welfare. Submitted to Workshop on Economics and Information Security.
Gordon, Lawrence A. and Loeb, Martin P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and Systems Security, Vol. 5, No. 4, November 2002, pages 438-457.
Gras, Marianne L. (2004). The Legal Regulation of CCTV in Europe. Surveillance and Society. CCTV Special (eds. Norris, McCahill and Wood) 2 (2/3):216:229. Available at http://www.surveillance-and-society.org/cctv.htm.
Grottron, Frank (2009). Project Bioshield: Purposes and Authorities. Congressional Research Service (CRS) Report for Congress. Washington D.C.
Hartley, Keith and Sandler, Todd, editors (1995, 2007). Handbook of Defence Economics. Volume I & II. North Holland Publishing Company. Amsterdam.
Hartley, Keith and Lazaric, Nathalie (2008). Short Reference Guide on Tools and Methods for Industrial and Technological Analysis, in James, A., Hartley, K., et al, A Study on How to Measure the Strengths and weaknesses of the DTIB in Europe. EDA. Brussels.
Hayes, Ben (2009). NeoConOpticon. The EU Security-Industrial Complex. Transnational Institute in association with Statewatch.
Hempel, Leon and Töpfer, Eric (2002). Inception Report. Working paper No. 1. On the threshold to Urban Panopticon? Centre for Technology and Society. Technical University Berlin.
Hobday, Mike (1998). Product Complexity, Innovation and Industrial Organisation. Working Paper. CoPS Publication No. 52. Sussex Policy Research Unit. University of Sussex. Brighton.
Hobijn, Bart and Sager, Erick (2007). What has Homeland Security Cost? An assessment: 2001-2005. In: Current Issues in Economics and Finance, Vol. 13, No. 2. pp. 1-7. Federal Reverse Bank of New York.

Hobijn, Bart (2002). What Will Homeland Security Cost? In: Economic Policy Review, Vol. 8, No. 2, pp. 21-33. Federal Reserve Bank of New York.

Hoffmann, Bruce (1998). Inside Terrorism. Columbia University Press. New York.

Holmqvist, Caroline (2005). Private Security Companies. The Case of Regulation. SIPRI Policy Paper no. 9. Stockholm.

Huang, Hui and Whalley, John (2006). Baumol-Tobin and the Welfare Costs of National Security Border Delays. Working Paper 12296. National Bureau of Economics Research. Cambridge (MA).

IDC EMEA (2009). The European Network and Information Security Market. Scenario, Trend and Challenges. A Study for the European Commission, DG Information Society and Media. Brussels.

Industrial College of the Armed Forces – ICAF (2006). Final Report: Electronics Industry. National Defence University. Fort Mcnair, Washington D.C.

Institute for Prospective Technological Studies – IPTS (2003). Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. EUR 20823 European Commission. Directorate General. Joint Research Centre. Report available on http://www.jrc.es/home/publications/publication.cfm?pub=1118.

Institute for Prospective Technology Studies (2005). Biometrics at the frontiers: Assessing the impact on society for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). EUR 21585 EN. European Commission. Directorate General. Joint Research Centre. Report available on http://www.jrc.es.

Institute for the Protection and Security of the Citizen - IPSC (2005). Emerging Technologies in the Context of Security. Research Strategic Paper. Issued in the framework of Science and Technology Foresight. Ispra.

INHES and CoESS (2008). Private security and its role in European security. White Book.

Jackson, Brian A. (2001) Technology acquisition by terrorist groups: Threat assessment informed by lessons from private sector technology adoption. Rand Corporation. Santa Monica (CA).

Jackson, Brian A. and Frelinger, David R. (2009). Understanding Why Terrorist Operations Succeed or Fail. Rand Corporation. Santa Monica, CA.

Jackson, Brian A., Chalk, Peter, Kim Cragin, R., Newsome, Bruce, Parachini, John V., Rosenau, William, Simpson, Erin M., Sisson, Melanie, Temple, Donald (2007). Breaching the Fortress Wall. Understanding Terrorist Efforts to Overcome Defensive Technologies. Rand. Santa Monica (CA).

Jackson, Brian A., Dixon, Lloyd, Greenfield Victoria A. (2007b). Economically Targeted Terrorism. A Review of the Literature and Framework for Considering Defensive Approaches. Rand. Santa Monica (CA).

Jackson, Ian (2004). The future of the defence firm: the case of the UK aerospace industry. Defence and Peace Economics, Vol. 15(6), December, pp. 519-534.

James, Andrew D. Editor (2006) Science and Technology Policies for the Anti-terrorism era. NATO Science series. IOS Press. Amsterdam.

James, Andrew D. (2004). U.S. Defence R&D Spending: An Analysis of the Impacts. Rapporteur's report for the EURAB Working Group ERA Scope and Vision. PREST. University of Manchester.

Jenkings, Brian M. (2006). The new Age of Terrorism in The McGraw-Hill Homeland Security Handbook. New York.

Jenkins, Brian M. (1997). Protecting surface transportation systems and patrons from terrorist activities. Case studies of best security practices and a chronology of attacks. Mineta Transportation Institute. San José State University. San Jose, CA.

Katz, Michael L. and Shapiro, Carl (1994). System Competition and Network Effects. The Journal of Economic Perspectives, Vol. 8, Issue 2, pp. 93-115. Nashville.

Keppler, Steven and Graddy, Elisabeth (1990). The Evolution of New Industries and the Determinants of Market Structure. The RAND Journal of Economics, Vol. 21, No. 1. Pp. 27-44. RAND Corporation. Santa Monica (CA).

Knobler, Stacey L., Mahmoud, Adel A.F. and Pray, Leslie A. Editors (2002) Biological Threats and Terrorism. Assessing the Science and Response Capabilities. Workshop Summary.Based on a Workshop of the Forum on Emerging Infections. Board on Global Health. Institute of Medicine. National Academic Press. Washington, DC

Kowalski, W. J. (2003). Immune Building Systems Technologies. McGraw-Hill, New York.

Krantz, David H. and Kunreuther, Howard C. (2007). Goals and plans in decision making. Judgement and Decision Making, Vol. 2, No. 3, June 2007, pp. 137-168.

Krugman, Paul (1996) Pop Internationalism. The MIT Press. Cambridge (MA).

Kunreuther H. and Heal G. (2003). Interdependent Security. Journal of risk and uncertainty. 26:231-49.

Kunreuther H., Meyer, R. and Michel-Kerjan, E. (2007). Strategies for Better Protection against Catastrophic Risks. Invited Paper for the Conference on the Behavioural Foundations of Policy. Princeton University. October 19-20, 2007. Wharton School. University of Pennsylvania, PA.

Laffont, Jean Jacques and Tirole, Jean (1993). A theory of Incentives in Procurement and Regulation. The MIT Press. Cambridge (MA).

Markle Foundation (2002). Protecting America's Freedom in the Information Age. A report of the Markle Foundation Task Force.

Markowski, Stefan and Hall, Peter (1998). Challenges of Defence Procurement. Defence and Peace Economics, Vol. 9, pp. 3-37.

Markusen, Ann R. and Costigan, Sean S. (1999) Arming the Future: A Defense Industry for the 21st Century. Council of Foreign Relations Press, New York.

Marshall, A.W. and Meckling, W.H. (1962). Predictability of the Costs, Time and Success of Development. The RAND Corporation. Santa Monica (CA).

Marti, Carlos (2009). Study on the Level Playing Field for the European Defence Industry: The role of ownership and Public Aid Practices. European Defence Agency (EDA). Brussels.

Martin, Stephen (1993). Advanced Industrial Economics. Blackwell Publishers. Cambridge, Massachusetts.

Martin, Stephen (1994). Industrial Economics. Economic Analysis and Public Policy. Second Edition. Prentice Hall. Upper Saddle River, New Jersey.

Martonosi, Susan E., Ortiz, David S., and Willis, Henry H. (2005) Evaluating the viability of 100 per cent container inspection at America's ports. Rand Corporation. Santa Monica, CA.

Martonosi, Susan E. and Barnett, Arnold (2006). How Effective is Security Screening of Airline Passengers? Interfaces. Institute for Operations Research and the Management Sciences (INFORMS). Linthicum. Maryland.

Meade, Charles and Molander, Roger C. (2006). Considering the Effects of a Catastrophic Terrorist Attack. Rand Centre for Terrorist Risk Management Policy. Rand Corporation. Santa Monica, CA.

Metcalfe, J.S. (2002). Equilibrium and Evolutionary Foundations of Competition and Technology Policy: New Perspectives on the Division of Labour and the Innovation Process. ESRC Centre for Research on Innovation and Competition. University of Manchester.

Molander, Roger C. Mussington, David,B and Wilson Peter A. (1998) Cyberpayments and Money Laundering. Problems and Promise. Rand Corporation. Santa Monica, CA.

Mueller, John (2005). Reactions and Overreactions to Terrorism. Ohio State University. Mershon Center. Columbus, OH.

Mueller, John (2007). Reactions and Overreactions to Terrorism: The Atomic Obsession. Ohio State University. Mershon Center. Columbus, OH.

Mueller, John (2009). Establishing principles for evaluating measures designed to protect the homeland from terrorism. Department of Political Science. Ohio State University, Columbus, OH.

Munday, P., Pakenham, M., Nicoll, A,, Haine, J., Rinkineva, K, Jaarva, M., Johnson, J. and Waller, A. (2006). New European approaches to Counter Terrorism. ESSTRT Deliverable D6-1. Final Report.

Myers Peter, Wästerby, Pär, Strebl, Friederike nad Kieboom, Jasper (2010). Operational Testing Framework. Network of Testing Facilities for CBRNE Detection Equipment (CREATIF).

National Institute of Justice – NIJ (2000). Guide for the Selection of Drug Detectors for Law Enforcement Applications. NIJ Guide 601-00. Washington D.C.

National Institute of Justice – NIJ (2001). Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders. NIJ Guide 103-00. Washington D.C.

National Institute of Justice – NIJ (2006). Status and Needs of Forensic Science Service Providers: A Report to Congress.

National Institute of Justice - NIJ (2009). High-Priority Criminal Justice Technology needs. NCJ 225375. Report available at: http://www.ojp.usdoj.gov/nij.

National Research Council (1998). Panel on Technical Regulation of Explosives Detection Systems, Commission on Engineering and Technical Systems. Configuration Management and Performance Verification of Explosives-Detection Systems. National Academic Press. Washington D.C.

National Research Council (2002a). Cybersecurity today and tomorrow. Pay now or pay latter. National Academic Press. Washington D.C.

National Research Council (2002b) Assessment of the practicality of pulsed fast neutron analysis for aviation security. National Academic Press. Washington D.C.

National Research Council. Committee on Science and Technology for Countering Terrorism (2002). Making the Nation Safer. The role of Science and Technology in Countering Terrorism. National Academic Press. Washington D.C.

National Science and Technology Council - NTSC (2006). Biometric 'Foundation Documents'.

National Institute for Occupational Safety and Health - NIOSH (2003). Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks. Cincinnati, OH.

NISE East (1997). Perimeter Security Sensor Technologies Handbook for Defence Advanced Research Projects Agency (DARPA). Arlington (Virginia).

O'Hanlon M, Orszag P., Daalder, I., Destler, I., Gunter D., Lindsay, J., Litan, R. and Steinger, J. (2003). Protecting the American Homeland. One year on. The Brookings Institution Press. Washington D.C.

OECD (2003). Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris.

OECD (2003b). Emerging risks in the 21st Century. An Agenda for Action. Paris.

OECD (2003c). Security in Maritime Transport. Risk Factors and Economic Impact. Paris.

OECD (2004). The Security Economy. Paris.

OECD (2008). Malicious Software (malware). A security threat to the Internet Economy. Paris.

OHS – Office of Homeland Security (2002). National Strategy for Homeland Security. Washington D.C.

Policy Research Corporation (2009). The impact of 100% scanning of U.S.-bound containers on maritime transport. Final report. Commissioned by the European Commission. Directorate General Energy and Transport.

Porter, Michael E. (1985). Competitive Advantage. Creating and Sustaining Superior Performance. The Free Press. A Division of Macmillan, Inc. New York.

Porter, Michael E. (1990). The Competitive Advantage of Nations. The Macmillan Press Ltd. London and Basingstoke.

Pullinger, Stephen Editor (2006). EU Research and innovation policy and the future of the Common Foreign Security Policy. A Report Commissioned by the Science and Technology Foresight Unit of the DG Research, European Commission. Brussels.

Rao, Ramesh R. Eisenberg Jon and Schmitt, Ted Editors (2007) Improving disaster management: the role of IT in mitigation, preparedness, response and recovery. National Research Council. Committee on Using information Technology to Enhance Disaster Management. National Academic Press. Washington D.C.

Rapoport, David C. (1999). Terrorism and Weapons of the Apocalypse, National Security Studies Quarterly 5, no. 3 (summer 1999) pages 49-69.

Riley, K. Jack (2006). Border Control. Chapter 37 in David Kamien: The McGraw-Hill Homeland Security Handbook.

Rossof H. and Von Winterfeldt D. (2007). A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach. Risk Analysis, Vol. 27, No. 3. pp. 533-545.

Sandler, Todd (2009). The past and future of terrorism research. Revista de Economía Aplicada. Number 50 (vol. XVII), 2009, pp. 5 to 25.

Schelling, Thomas (1963). The Strategy of Conflict. Harvard University. Cambridge (MA).

Schelling, Thomas (1971) What Is the Business of Organized Crime? Journal of Public Law, Vol. 20, No. 1 pp. 71-84.

Scherer, F.M. (1980). Industrial Market Structure and Economic Performance. Rand McNally College Publishing Company. Chicago.

Scherer, F.M. (2000). The pharmaceutical industry in Handbook of Health Economics Volume I. Elsevier Science B.V.

SEESAC (2005) SALW and Private Security Companies in South Eastern Europe: A Cause or Effect of Insecurity? Second editon. Belgrade. Serbia and Montenegro.

Senger und Etterlin, Stefan von (2006). Security industries. Global context, European efforts and the potential in Berlin-Brandenburg. Potsdam.

Simon, Herbert A. (1978). Rational decision-making in business organizations. Nobel Memorial Lecture. Stockholm.

Spulber, Daniel F.(1989). Regulation and markets. The MIT Press, Cambridge, Massachusetts.

Stango, Victor (2004). The economics of standard wars. Review of Network Economics. Vol. 3, Issue 1 – March 2004. The Berkeley Electronic Press.

Sunstein, Cass R. (2002). Probability Neglect: Emotions, Worst Cases, and Law. The Yale Law Journal Vol.112:61.

Stewart, M.G. and Mueller, John (2009) Cost-Benefit Assessment of United States Homeland Security Spending. Centre for Infrastructure Performance and Reliability. Research report No. 273.01.2009. The University of Newcastle. New South Wales. Australia.

Sutton, John (2001). Technology and Market Structure. Massachusetts Institute of Technology. The MIT Press. Cambridge (MA).

Temple, Paul (2005). The empirical Economics of Standards. DTI Economics paper no. 12. UK Department of Trade and Industry. London.

Theisen, Lisa, Hannun, David W., Murray, Dale W. and Parmeter, John E. (2004). Survey of Commercially Available Explosives Detection Technologies and Equipment. Sandia National Laboratories. Albuquerque, NM.

Thomson, James A. (2007) DHS AWOL? Tough Questions About Homeland Security Have. Gone Missing. By James A. Thomson. Rand Review. Spring 2007. Vol. 31, No. 1. RAND. Santa Monica (CA).

Tirole, Jean (1988). The theory of industrial organization. MIT press, Cambridge, MA.

Tisdell, Clem and Hartley, Keith (2008) Microeconomic policy: a new perspective Cheltenham, UK; Northampton, MA: Edward Elgar.

Tversky, Amos and Kahneman, Daniel (1973) Availability: A heuristic for judging frequency and probability. Cognitive Psychology, Vol 5(2), Sep 1973, 207-232.

U.S. CBP (2006) Container Security Initiative. 2006-2011 Strategic Plan. Washington D.C.

U.S. Department of Homeland Security (2009). Budget in Brief. Fiscal year 2009. Washington D.C.

U.S. Department of State (2004). Patterns of Global Terrorism. Washington D.C.

Utterback, James M. and Abernathy, William J. (1975). A dynamic Model of Process and Product Innovation. The International Journal of Management Science, Vol. 3, No. 6. Pergamon Press. UK.

Van de Voort, Maarten and O'Brien, Kevin (2003). Seacurity. Improving the Security of the Global Sea-Container Shipping System. Rand. Santa Monica (CA).

Van Eeten, Michel J.G. and Bauer, Johannes M. (2008). Economics of Malware: Security Decisions, Incentives and Externalities. STI working Paper 2008/1 Information and Communications Technologies. OECD. Paris.

Van Steden, Ronald and Sarre, Rick (2007). The Growth of Private Security: Trends in the European Union. Security Journal, Vol. 20, pp. 222-235. Palgrave Macmillan Ltd, London.

Willis, Henry H. and Ortiz, David S. (2004). Evaluating the security of the global containerized supply chain. Rand Technical Report. Santa Monica (CA).

Williamson, Oliver E. (1971). The Vertical Integration of Production: Market Failure Considerations. American Economic Review. American Economic Association. Vol. 61(2), pages 112-23, May.

Williamson, Oliver E. (1979). Transaction-Cost Economics. The Governance of Contractual Relations. Journal of Law and Economics, Vol. 22, No. 2 (Oct., 1979), pp 233-261.

Williamson, Oliver E. (1985). The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting. The Free Press. A division of Macmillan, Inc. New York.

Zimmerman, Peter D. and Loeb, Cheryl (2004). Dirty bombs: The threat revisited. Defense Horizons. Number 38. A publication of the Center for Technology and National Security Police. National Defence University.