Economics of Security Working Paper Series

economics-of-security.eu

Carlos Martí Sempere

The European Security Industry: A Research Agenda

February 2010

Economics of Security Working Paper 29

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: Martí Sempere, C. (2010). "The European Security Industry: A Research Agenda". Economics of Security Working Paper 29, Berlin: Economics of Security.

First published in 2010

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

The European Security Industry.

A Research Agenda[1]

Abstract

The security industry can be defined, in the first instance, as the industry that produces the goods and services required to protect citizens from insecurity. Yet, this industry, as opposed to defence, has not been an area of intense research. Their boundaries are unclear and the industry is not well characterised.

This paper analyses this knowledge gap and presents some ideas for a research agenda for this industry that could assist in unveiling the main features, the potential weaknesses and strengths, and the capability to solve the security needs of society in an efficient and effective way. The paper discusses a definition of this economic sector useful in setting its boundaries, and it briefly describes the main types of industries operating within the sector. It analyses methods for gathering information regarding the industry, customers, and other market agents. Finally, it outlines ways for assessing market performance in terms of the structure-conduct-performance paradigm.

Key words: security industry, security market, terrorism and organised crime countermeasures, competition, market performance.

BACKGROUND

[1] This research has been partly financed by the 7th European Research Framework Program in the field of Security.

Security is a fundamental *good* without which societies cannot prosper. Investment in security provides relevant benefits preventing or reducing damage to life and property and increasing resilience[2] to recover quickly from a security incident, whatever its nature. This investment may diminish the risk that the incident spills over into other activities, sectors and economies and ends up disrupting society's key functions due to the strong interdependencies of modern society. An adequate investment in this area may enhance what is known as *secure growth* where the confidence of citizens and the general welfare of the society blossom. Yet, benefits of security investments are not often easy to measure. For example one cannot accurately determine how many criminal or terrorist activities have been prevented due to improved security.

Security spending involves investment in human resources as well as on means required to support activities aimed at reducing threats and mitigating their potential damages e.g. large intelligence database systems or personal protective equipment for security personnel. These means, whilst unable *per se* to provide security, properly used, can improve it largely. Here the security industry is considered as the collection of economic agents that produces these means in terms of goods and services.

The capability to find and offer new technical solutions to security problems characterised by increased citizen confidence and low cost, is the most appropriate measure of success in this economic sector[3]. Whilst these expenditures may be considered as a sort of societal burden, they also provide other relevant benefits in terms of job creation, industrial capabilities, profits to shareholders, and innovations

[2] Resilience reduces large scale shocks and the intimidation of a huge citizen audience thereby frustrating the goals of terrorists.

[3] The use of finger biometry to protect laptops and personal digital assistants (PDAs) could be a good example.

applicable in other economic sectors. In short, this type of spending has positive effects on the general industrial and technological base of society, contributing to economic wealth in the long run[4].

However, few things are known about this economic sector. Information regarding economic figures, industrial capabilities, market conditions, structure of the industry, conduct of agents, and performance is not plentiful, and it may not be very accurate. Therefore, an agenda to generate knowledge is clearly required.

This paper presents a research agenda identifying areas and methods to improve knowledge of the security industry with particular emphasis on the European Union. Main themes addressed are: the boundaries of the sector, an overview of the main types of industries, methods to collect information, the analysis of suppliers, stakeholders and demand drivers, and the performance analysis. The rational that supports the agenda, the different approaches and the potential difficulties in implementing this agenda are detailed. The paper ends with a brief conclusion.

BOUNDARIES OF THE SECTOR

The first challenge to address should be the establishment of clear boundaries of the sector that identifies which undertakings should be included or excluded from the research. For such a purpose a definition of the sector would be helpful. An objective definition is not easy since subjective factors based on beliefs and preferences of the

[4] Investment in security always has an opportunity cost, raising the unresolved question regarding its application in other activities that could further increase society welfare and growth. For example, due to the high number of car accidents, investments could be made more effective in road or car safety.

author may be subtly slipped into the final wording. With this in mind, a pragmatic definition is presented, illustrated with brief comments surrounding the reasons behind such a definition.

The security industry is the industry that addresses all the products and services used specifically by the human being to prepare, prevent, protect, respond, reduce, palliate and deal with the threats and the 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 tries to address all the supporting activities, in terms of goods and services, needed to diminish risk. No explicit distinction is made on the beneficiary, because it is assumed that is society and their citizens. Since a security incident triggers a response aimed at mitigating their consequences an explicit reference is made to this term. However, long term activities and the associated means related to restoration and recovery of the situation to pre-event levels such as basic services restoration, repair and reconstruction, financial and economic recovery, etc. should be considered outside the scope of this industry, as long as their methods and activities do not differ essentially from the everyday routine activities of operation, repair or upgrade.

The most problematic part of the definition is the term "*undesired events*". These events can be distinguished because they create fear or insecurity in citizens. Whilst this feeling is to some extent subjective, it can be estimated based on interviews as shown in the next figure.

<figure 1>

Based on the above figure, five main sources of insecurity can be identified: armed conflicts, terrorism, organised crime, pandemics, and natural or man-made disasters. As can be seen, the two most relevant areas of insecurity are terrorism and organised crime. The industry related to these two sources of insecurity share large commonalities in terms of products and services. However, it has not been surveyed in depth, as opposed to the exhaustively explored defence industry. The former industry, despite of sharing some commonalities and similarities with the defence industry, also differs largely in terms of customer, products, and technologies.

Other major risks faced fundamentally with the support of the health industry are diseases and pandemics; however this industry is also related to terrorism and organised crime since similar measures are applied to defeat a chemical or biological attack.

The industry related to natural (floods, hurricanes, earthquakes, forest fires) or man-made disasters (technological or industrial accidents usually known as safety industry) addresses the response to hazards that cause damage without purposeful action. Whilst the same kind of equipment is shared for mitigating damages originated by terrorism and organised crime, the preventive means are of a very different nature (e.g. weather prediction systems). Principal customers of this industry are more closely related to health, civil protection and environmental protection agencies rather than law enforcement.

This paper will focus on the industries that address the risks associated with terrorism, organized crime, and natural or man-made disasters, with special emphasis on the first two, which are considered the most relevant sources of insecurity. This view is similar to the EU vision[5], the CEN BT/WG 161[6] and the Department of Homeland Security (Bush, 2002).

Measures may be split into two main activities. The first intends to prevent terror and criminal action, offering these groups opportunities and incentives to change their behaviour abandoning and replacing their criminal activities with legal ones[7]. The second intends to discourage these actions increasing the chance of being frustrated, the players apprehended and imprisoned, and penalties applied. In short, by raising their costs and reducing their benefits. The security industry focuses mainly on this second activity. This activity can be further broken down into active measures to abate the source of threat, targeting terrorist and crime organisations to reduce their operational capability; and protective or defensive measures aimed at strengthening the potential targets, increasing the difficulty to strike them with success. Once again, the security industry concentrates mainly in providing means for the second type of activity.

---

[5] See the introduction of the EU Commission (2009) document *Towards a more secure society and increased industrial competitiveness. Security Research Projects under the 7th Framework Program for Research*.

[6] The CEN BT/WG 161 on Protection and Security of the Citizen adopted the following definition in January 2005: "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.

[7] For example, soft measures addressing causes that may contribute to radicalisation, such as inequalities, social exclusion, poor social cohesion, sense of grievance and injustice, lack of opportunities, or discrimination. They can also challenge the ideologies (battle of ideas) that extremists believe can justify violence.

Active measures against terrorism and organised crime aim at disabling their infrastructure and networks, controlling their accesses to sensitive knowledge and material[8], discouraging people's involvement in these organisations and weakening their support and sponsors. These organisations operate nowadays in a highly efficient manner on trans-national networks (Europol, 2008, 2009). This is facilitated by the low cost of transport, transfer of money and communication which permits their operation in a mixed way, based on local players supported financially and logistically by their international counterparts. Therefore, the detection and disruption of the flow of persons, funds and illegal goods within these networks is one good method to reduce their capability, in particular when crossing borders.

These groups have fundamental advantages to act with a small level of risk due to the asymmetry of information they enjoy and the ease with which they can select opportunity targets. This behaviour, perceived from the outside as random, would force large and expensive investments to assure a sufficiently wide protection level. Since this approach is economically unaffordable, societies have to concentrate on the protection of key societal assets, networks, services and facilities, such as transport, health, energy, water, production of dangerous goods, information and communication, finance, food or government, usually known as critical infrastructures. A successful attack on any of them could create important disruptions to the entire society and generate large losses.

These groups may be wealthy enough to stand up to small armies, and their attacks can take a form similar to that of guerrilla or military action, using weapons such as mortars,

[8] For example access to weapons, explosive precursors, chemical or biological agents. Therefore, preventive measures are needed to safeguard these assets and avoid their steal.

RPG guns, MANPADS[9] or even CBRNE[10] devices against high pay off targets, that may result in mass casualties or widespread damage. Additionally, terrorists could act as proxy of certain states or may have foreign logistics bases. Countering these groups may require joint actions of law enforcement units and armed forces such as hostage recovery, maritime counter-terrorism, bomb disposal, renegade aircraft interception, and the prosecution of terrorists up to their havens in host countries. Moreover, security incidents with far reaching consequences may require the additional logistical capabilities of the Armed Forces. Therefore, areas exist where the separation of security and defence issues becomes complex, making the task of qualifying their suppliers challenging.

Public health may be a target of terrorism or organised crime as another means to achieve desired goals[11]. Chemical or biological agents can be dispersed in the air or water, infecting thousands of people, contaminating soils, buildings and transport assets, destroying agriculture, infecting animal and plant populations, and affecting food and feed at any stage in the supply chain. Safeguarding the society from this risk is a major challenge, where early detection systems and the pharmaceutical industry can provide some solutions.

Insurance companies play a relevant role in the security field. They facilitate the buying of insurance against potential damages, providing financial support for incident recovery. They estimate the risks and consequences of undesired events and define the payable amount (premium) to cover the economic losses of insecurity. They can

[9] Man Portable Air Defence System.
[10] Chemical, Biological, Radiological, Nuclear and Explosive.
[11] The chemical attack to Tokyo subway in 1996 and the anthrax attack in the USA after 9/11 raise concerns about this sort of actions.

stimulate security investment providing discounts to homeowners, businesses and other organisations who invest in cost-effective loss-mitigation measures. Therefore, they may have a considerable influence in standardising security procedures, solutions, and equipment[12]. However, since insurance companies are not true solution providers in reducing or eliminating risk, they should be considered a less relevant research area.

MAIN TYPES OF SECURITY INDUSTRIES

Due to the high diversity of threats, technologies and security solutions, this sector is composed of companies of a very varied nature, who sometimes only share as a unifying nexus the term *security*. Products and services generated include locks and safes, fire and burglar alarms, electronic access control systems, electronic surveillance equipment, armoured and protected vehicles, guard equipment and garments, security fencing, and security consulting. In some cases products have a very small supply chain, while in others they may require the integration of components from a large supply chain such as border and maritime surveillance systems. Sometimes production is very large and standardised such as in-motion detectors, whilst in others, it is more handcrafted and tailored to satisfy specific end customer demands such as a building intrusion detection systems. Sometimes products are sold directly to the customer, whilst in others, distributors, value added resellers and systems integration plays a key role in the supply chain. The technologies used in these products is varied and includes amongst others construction, automotive, aerospace, textiles and garments, ballistics, electronics, and information and communications systems. Usually these products and services are not only applicable to security, but also to other activities. For example,

[12] The European insurance companies still play in this area a low role. See page 155 of Wharton (2005).

identity cards may be used for police identification but also to exert the right to vote. Video cameras may be used for surveillance but also for leisure. Intermediate products tend to have this dual role that increases up the supply chain, where it might even occur that a company ignores the fact that its product is integrated and sold in the security market. This varied nature increases the difficulty of the analysis.

Measures and means to counter terrorism and organised crime are conditioned to a large extent by the behaviour and technological status of these groups. Their limited resources and the need to function undetected, dictates that they focus on inexpensive and easy to access technologies, in sharp contrast with the technologies that States can afford. Risks are only ever taken in limited cases for high pay off weapons. Yet these groups have shown competent capability in developing tactics and using technology in quite innovative ways to overcome deployed measures and achieve their goals. For example drug trafficking gangs have been able to use submarines to transport their illegal products, such as the one captured by the Mexican Police July 16, 2008 as reported by CBS News. The dynamic behaviour creates a competition between State measures and countermeasures of these groups that may bring about research and development of new security equipment and raise society expenditure, however not always with a clear outcome in terms of increased security.

Often the provision of security is based on non-material solutions or the development of redundancies to increase resilience, but in other cases, the security tasks or functions can be largely improved with the goods and services provided by the industry. In the next paragraph, the more relevant will be commented grouped around the main capabilities needed to fight terrorism and organised crime.

Preparedness

Preparedness addresses the tasks related to the planning, equipping, training, and rehearsing of resources and means needed to prevent, avoid or undergo security incidents such as the stockpiling of drugs, vaccines, or antidotes for facing a CBRN attack.

Preparedness requires special knowledge for analysing threats and vulnerabilities, assessing risk, developing contingency and resilience plans and procedures, assessing the required investments, performing feasibility studies of best methods to deal with insecurity or managing the acquisition of security solutions. These highly skilled activities are often outsourced to small consultancy companies and in other cases to departments of large companies specialised in this kind of technical assistance.

Preparedness also requires training and rehearsal systems, particularly for first responders and decision makers. This task is performed by companies specialised in training that may integrate software training tools. The computer industry may also develop systems to artificially simulate, in an inexpensive way, the incident scenario allowing stakeholders to rehearse the different responses, evaluate their outcome, and increase their capability to appropriately manage the situation. This seems to be a very promising market for the near future.

Early warning and awareness

Since terrorists and participants in organised crime conceal their activities, surveillance is necessary to detect, identify and recognise traces of suspicious activities in order to activate potential countermeasures able to frustrate any impending terrorist or criminal action. For example, the identification of organised crime bank accounts facilitates the detection of money laundering and may be used to block funds in support of illegal activities. Other examples are the discovery of illegal weapons hidden in baggage, the identification of a person claimed by justice on a border crossing, or the interception of phone and e-mail communications.

Early warning includes a plethora of surveillance equipments able to explore and record the full electromagnetic spectrum to identify precursor signals that can announce a security incident. This includes different types of sensors and components able to gather these signals extract meaningful information and transmit and depict it to the surveyor, reducing his or her workload. Sensors can be integrated into a network, increasing their reliability and facilitating the detection of anomalies that may announce a potential threat. The electronics, communications, computer and software industries are the main providers of equipment for early warning and surveillance.

Building and facilities protection

Surveillance equipment is used mainly in the protection of buildings and facilities. It is complemented with access control systems able to automatically identify and authorise access. CCTV is the most universal equipment for surveillance. Cameras usually operate in the visual spectrum, but image intensifiers or thermal cameras may be used under poor visual conditions. Most advanced cameras are able to process the images

being able to classify and distinguish the presence of people on the scene, monitor their behaviour, identify people based on their biometric features[13] and raise a warning if deemed suspicious. Many of the devices used to detect intrusion are able to sense sound, microwaves, ultrasounds, or vibrations. More simple detectors are able to notice doors or windows opening or breaking. Building protection may be complemented with fire detectors and automatic extinguishing systems.

Access control is based on credentials usually stored in magnetic or smart cards able to be read by computer. Most advanced systems use biometric features to verify that the card owner coincides with the identity information stored in the credential.

Borders systems

Border protection requires specific surveillance equipment to detect illegal entry in unregulated borders, as well as identification and verification of identity and access rights at entry points. Radars, day and night cameras and other long range sensors can be used to detect vehicles, persons and small boats attempting to illegally cross the border. Whilst sensors can be located at specific fixed locations, sometimes they have to be installed on mobile platforms such as vehicles, ships, airplanes or even satellites to assure a reasonable and affordable coverage of large border perimeters. The production of these complex systems requires platform builders and system integrators in addition to the sensor supplier.

[13] These equipments use the physiological characteristics of the face, hand geometry, fingerprint, eye retina, ear shape, or behaviour, such as voice or signature, using digital scanning and pattern recognition techniques for identification purposes.

Identification on borders (and other places) is based on personal identity cards, passports or visas. While this information was in the past stored on paper with adequate counterfeit protection –like specific paper and printing procedures such as holograms–, they are evolving today into new documents where the identity information, including biometric features, is encrypted and stored in the integrated circuit of a smart card able to be read and processed directly by a computer system, largely reducing the opportunity of identity fraud. Car-plate readers can be used for automatic vehicle identification.

Non-intrusive inspection systems are also needed to detect weapons, explosives and drugs under clothes and personal belongings. They are used in transportation hubs like airports or train stations, but more intensively on borders. They include metal detectors, X-ray systems or drug and explosive trace detectors.

Transport security

Finally control of merchandise is needed to avoid traffic of dangerous or forbidden material and smuggling of goods. Container seals and cargo manifest on paper are the traditional method in assuring the integrity of containers. These systems are today evolving into electronic seals and electronic cargo manifest documents that can be managed in a more agile way with the support of computers. Sensor equipment such as gamma ray and neutron detectors can be used to detect nuclear or radiological materiel, and high power X-ray and pulsed fast neutron can be used to obtain a radiography of the interior of the container helping to improve the customs inspection process.

The main challenge of inspection systems is an adequate level of efficiency, avoiding the entry of illegal material while maintaining a free (or nearly free) flow of legitimate travel and commerce with a reduced impact on trade, in terms of costs, delays or reduced flow. This is a relevant need in a globalised world where a considerable increase in personal and material flow is expected.

This requires a short timeframe, a low failure rate in terms of false positives and negatives, and a minimum amount of resources that today technology is not always able to provide. Therefore, this area is subject to intense research in the USA and the EU in order to find effective solutions that increase the number of inspections, since it is estimated that the contents of less than 2% of all containers are checked (Van der Voort, 2002). Electronic credentials and Radio Frequency Identification (RFID) combined with large databases and computer systems, seems to be a promising solution. However, progress in this area is being sluggish.

Intelligence systems

Data gathering and analysis regarding the activities of terrorism and organised crime is crucial in order to disable these groups before they can carry out their planned actions. The appropriate combination of disparate and initially unrelated evidence with historically recorded data may facilitate the generation of intelligence regarding members, networks, intentions and means of operation of these groups.

When an act of terrorism or some sort of criminal action is carried out, it is fundamental to investigate the scene where the event has occurred, to find and collect evidence. The

evidence can be analysed in forensic laboratories, using highly specialised instruments provided by the industry such as fingerprints or DNA to extract relevant information. This information may facilitate the reconstruction of the event and the identification of the perpetrators, helping to imprison and condemn criminals and prevent further attacks.

The investigation process can be improved through the use of large database computer systems where evidence can be compared with stored information regarding face, fingerprint, DNA, name, judicial records and other relevant data. Online access to this system from mobile terminals may be very useful when temporary spot controls are placed in streets, crossroads or stations where people have to cross to arrive to their destination. Industry can support this activity supplying high performance computers and specific algorithms such as pattern recognition, data mining and natural language processing to analyse information, validate hypothesis and derive knowledge.

Early warning of natural and man-made disasters

Natural and man-made disasters can be pre-warned, helping to respond quickly and avoid greater damages. Early warnings include weather forecasting systems, fire detection systems (in particular forest fires) and flooding detectors through the real-time measure of water levels in rivers and watersheds. Seismic sensors can detect earthquakes, however predictive methods to anticipate them is still an immature science.

The effectiveness of some of the solutions for early warning and intelligence are largely conditioned to the use of common standards (e.g., identity cards, containers seals, etc.) and the capability to interoperate and exchange or share information between the

different stakeholders responsible for security, in particular State agencies of Member States, in order to easily identify any kind of anomaly that may trigger the appropriate measure to curb the potential risk[14].

Protection / Response

The protection means includes different countermeasures to deter, deny, frustrate, or cope with mentioned threats. Countermeasures can be classified as passive or active. The main passive countermeasures include architectural barriers and building strengthening, personal or vehicle protection against light and non-conventional (CBRN) weapons, personal protection equipment for first responders, and other security measures integrated in the system design. Active countermeasures includes the use of weapons and vehicles to capture and prosecute outlaws, equipment to protect own communications to avoid interferences and espionage and to disrupt communications used by these groups (e.g., remote activation of explosives), and deactivation of improvised explosive devices.

Particularly relevant is the provision of guarding services, a very important part of the security industry that employs a large number of persons (higher than 1,700,000 according to CoESS (2008).

Protection in the cyberspace

[14] Such as the Schengen Information System (SIS) and the VISA information System (VIS), or EURODAC for asylum request control.

Cyber crime can be defined as *criminal acts committed using electronic communication networks and information systems or against such networks and services*[15]. This is one of the areas where illegal organisations can accrue important benefits if they access or modify key information; or block critical information systems using malicious software (malware) such as virus, spyware, worms or trojans. This problem could be particularly serious if they attack systems that support critical infrastructures, since such attacks can degrade or even disrupt the essential services they provide. The magnitude and losses of cyber attack is little known since many companies do not report security breaches on the basis of a potential loss of customer confidence. But a report in the Financial Times of May 5, 2006 estimated the cost in the UK to be around 10£ bn.

Identity theft is one of the ways to steal[16], modify or delete high value information, or to execute unauthorised operations such as the transfer of funds (financial fraud) in electronic commerce and banking systems. Techniques for obtaining passwords and credit card details include phishing where this sensitive information can be obtained by masquerading as a trustworthy person or web site.

Cybercrime tries to cause damage to electronic networks attacking their information systems, blocking their services, or hacking. It uses advanced techniques to decipher computer and communication codes to obtain passwords and to gain computer access in order to damage key system functions. The main purpose of these actions is usually extortion. Cybercrime may also include the publication of illegal content via electronic media such as sexual abuse of children or incitement to terrorism.

[15] Communication from the Commission "Towards a general policy in fight against cyber crime" COM (2007) 267 final.

[16] For example, digitalized films can be stolen and counterfeited and sold in piracy markets lowering the expected income of companies and causing large losses.

The computer software industry offers a wide range of solutions and services to assure the confidentiality, integrity and availability of data and systems such as: high assurance software development methodologies to avoid weak points, means of user identification and authentication including biometrics, strong encryption systems to assure secure information exchange, log systems and analysis tools for auditing purposes in order to detect intrusion and attacks, filters to avoid spam messages, programs to detect viruses, and redundant systems and back up tools to easily recover data and systems. Their ultimate objective is that the customer enjoys a *trusted* on-line environment. The growing internet market has massively stimulated the demand for these types of products and services. The Gartner company estimated the worldwide revenues of the security software market at 13.4 billion $ in 2008 of which 3.2 billion corresponded to Europe.

Consequence mitigation

Crisis management and emergency services require capabilities to cope with and mitigate the effects of a successful terrorist or criminal attack, or a natural or man made disaster, and avoid its propagation.

Means to cope with personal damages include first responders equipment such as search equipment for finding survivors between ruins, first aids, and evacuation means to secure areas or hospitals, sometimes using specialised vehicles such as ambulances. In the case of a large attack or disaster, additional means are needed for evacuating mass casualties and fatalities and administering relief to survivors providing energy, food,

medical care or water supply. Victims may also need psychological aid services to overcome the trauma caused by the incident.

Means to cope with material damages include fire-fighting equipment, emergency demolitions, deactivation of unexploded devices, and emergency repair of buildings or public works. It may also require surveillance of the disaster area to avoid looting, theft or vandalism.

A CBRN attack requires that first responders wear specialised equipment and vehicles are protected against these agents. The identification of the agent is essential in providing appropriate relief and reducing health damages. It may include the extensive use of medication and vaccination of the targeted population. Specialised equipment is also needed to decontaminate people, material, buildings, facilities or even geographic areas depending on the type of attack and the agent used.

Particularly relevant are the means needed to gather and share information about the overall situation, coordinate available resources (including volunteers), and evaluate how and with what effect these resources are being applied. These systems, popularly known as Command and Control systems, are based on a robust network of information and communications systems able to manage the situation. These systems require deployment capabilities in the area of the incident. The communications capabilities – that may include in some cases satellites– facilitate the sharing and distribution of timely and accurate information to the various response teams and the citizens, keeping them informed about the damage extent, continuing threats and actions to take. These capabilities may greatly speed up the response time and action to save life, limb and

property and curtail economic and environmental damage, reducing the magnitude of losses and avoiding propagation via indirect effects; in short, to improve the efficiency of the response. These system are including specialised software tools to improve situation awareness such as precise location of personnel and assets, information fusion, damage assessment, predictive tools of the evolving situation to anticipate impending threats, and decision support aids.

While the requirements of these systems are rather different than the defence industry, it is probably this industry, the more prepared to integrate the large number of sophisticated hardware, software and communication components that are needed to achieve such capability. Again, interoperability of communications, through appropriate use of standards, is an essential requirement to achieve a successful system when many organisations or countries are involved in the response.

DATA COLLECTION

A fundamental item of a research agenda should be the collection of enough quantitative and qualitative information to obtain a complete, accurate and reliable picture of this economic sector from which knowledge can be derived.

Here different problems appear. National security industry associations that can provide a wealth of information on the sector do not always exist. On the contrary, we find associations that only cover limited areas such as fire protection, ICT-Security or Security Services. Others name themselves as Security and Defence associations, but do not distinguish in which sector each company operates. In addition many industries and

conglomerates operate in more sectors than security, the latter not being its core business. Therefore, they may not classify themselves as security industry. All these problems complicate the data gathering process. The main identified information sources are:

- *Published texts*. There is a short list of publications regarding the European Security Industry and few papers exist in open literature that are directly related to this research. The EU research project STACATTO has carried out some studies from the supply chain and research and development point of view, but they are not a true economic analysis of the sector. ECORYS performed a competitive study of the sector in 2009 for DG Enterprise and Industry. IDC EMEA has also performed a study of the European network and information security market in the same year for DG Information Society and Media. Specialised consultancy companies, like Frost and Sullivan, publish written reports regarding this sector, but they are mainly focused on market opportunity analysis for assessing investors. These non-free reports, therefore, may be subject to (optimistic) biasing and should be read with caution.

  Specialised magazines, exhibition catalogues and directories in the field seem to be a good source of information on enterprises and products. However, these documents focus mainly on marketing issues and in supporting the search for partners, rather than providing a complete and objective profile. Independent technical reports on security technologies and products and official documents on public security programs and their budgets provide interesting insights into the sector. These raw sources of information, however, require considerable analysis.

- *Statistical information*. Eurostat can be a source of information for analysing this economic sector. The NACE[17] code of Statistical Classification of Economic Activities has reserved the code 80 for security and investigation activities, while the class 84.24 is reserved for Public order and Safety activities. With these codes some statistical information from the EU and Member States security sector related to expenditure, outputs, imports and exports could be obtained. However, security equipment is embedded in codes that also include other items. Nonetheless, the availability of this information is not always guaranteed.

- *General industrial European databases*. These databases can provide main economic values of security companies. Information could also be available on industrial and professional associations related to the different types of security industries. However, these reports are not always available or published on an annual basis.

- *Company information*. Another data source is the information disclosed by companies. The information contained on their websites provides accurate information relating to their products, marketing strategies and economic indicators. Yet only large companies publish a complete web page. Complementary information could be obtained through the analysis of the response to written questionnaires sent to companies; however this kind of approach tends to yield a very low and incomplete response level (in the range of 5%-30%), reducing the

[17] Nomenclature générale des Activités économiques dans les Communautés Européennes.

chance of obtaining a significant amount of useful information. Interviews can partially solve these problems. However, this requires considerable resources.

It is obvious that the depth and quality of any research depends greatly on the size, accuracy and reliability of the information collected. Therefore, the collection of the best available information is a critical issue. Besides, drawing conclusions will require the examination of the completeness and reliability of information collected. An initial list of information sources may be found at the end of the paper.

MAPPING THE EUROPEAN SECURITY INDUSTRY

The identification of industrial capabilities in the different market segments and the geographic distribution should be another relevant point of the agenda. Market segments can be derived from the different kind of security services and products, and their analysis could help to identify more precisely potential gaps. For example, the strong presence of foreign companies, such as USA subsidiaries, may indicate that the European security industry is not performing as well as expected.

The analysis should take into account capabilities in the areas of research, development, manufacturing and operational support. Special emphasis should be placed on technologies used, and the relevant role that information and communications technologies seems to play in this market.

The mapping process should be completed trying to obtain relevant data from the industry in order to ascertain a clearer image of the sector. Basic values to consider

include net sales, employees and profits. Other useful values could be: export sales, R&D expenditure, percentage of activity in the security field, market capitalisation or added value. Since the high number of companies in the sector might impede a comprehensive analysis, this activity should concentrate on major and leading stakeholders as their main features may provide a better clue of the principal patterns of the sector.

The analysis should also study the supply chain of security products, its current complexity, and the role that small and medium enterprises (SME) play. This analysis should be complemented assessing the degree of diversification in the industry and the role of security in their core business. This will aid in the identification of strong backward and forward links with other economic sectors of the economy.

One area to survey is the identification of companies with a large market share, since it may create dominant positions that could impact on market performance. Obtaining concentration ratios would be quite useful, yet it may not be easy to obtain enough quantitative information to measure this value. The reasons behind such market concentration such as large capital requirements and economies of scale of mass production should be evaluated as well.

The size of the sector in each EU Member State as well as the overall size, is relevant information to collect. Differences between countries that may appear, including those related to technological capabilities, should be considered. An attempt to compare sectors on each side of the Atlantic, should enough information be collected, could highlight remarkable similarities and differences. In figure 2 an initial distribution can

be seen, where it is possible to see that France, United Kingdom and Germany have the strongest security industry.

<figure 2>

Measuring the output of the sector in economic terms appears to be difficult. The OECD report estimated the worldwide security industry turnover to be between 100 and 120 billion $ in 2004. The values for the three main European economies given were: Germany 4 billion, UK 3 billion and France 3 billion. The Homeland Security Research Corporation estimated worldwide expenditures in security for 2004 at 157 billion $ of which 34.2 billion corresponded to Europe. Civitas group estimated worldwide expenditure at 55 billion $ for 2006 of which 13 billion corresponded to Europe. Unfortunately, the methodologies used to estimate these values are not described, but such large differences suggest that sector boundaries of each estimate are different, or methods are probably rather inaccurate. Efforts to improve accuracy, while not easy, are certainly needed. Aggregation of values could be carried out based on the turnover of the largest companies. However, since some industries are highly diversified conglomerates and their turnover on security is not always known (or is considered commercially confidential), this value could be very imprecise.

DEMAND ANALYSIS

A research agenda shall include an analysis of the demand. The different stakeholders that request security –namely Public Administration, corporations and individual consumers– should be analysed in detail to discover the main drivers that shape their purchasing behaviour. Main stakeholders are:

- *Individual consumers*. These consumers purchase security to protect their households and other main assets such as vehicles, and earnings (through bank accounts and deposits). Household protection is usually based on relatively inexpensive low technology products such as locks and safes. People with higher acquisition power install intrusion equipment systems wired to a small alarm centre that connects, through a communications line, to a central alarm system operated by a guarding company. These systems are based on widely available and competitively priced standard off-the-shelf products.

- *Private agents (organisations and companies)*. These agents buy security to protect their businesses and prevent any economic loss due to the disruption created by a security incident. They develop business continuity and security plans and purchase the means needed to implement them, mainly early warning systems, and access control systems. Security services demand includes protection of assets (e.g. transport of funds) and investigation services. Investment is more common in large corporations who usually have a Security Officer. Due to its nature, the banking sector and air transport have been the main investors in this field. Here security solutions are usually more tailored to user needs.

  Of particular relevance are the organisations that own or operate critical infrastructures. Since the disruption of their services can have severe social and economic consequences, these organizations invest more resources in security. Yet considerations of efficiency can make these organizations invest below what is

desirable from the social point of view and regulations could be needed to fix a minimum amount of security they have to provide.

- *The Public Administration*. The third relevant customer is the Public Administration. It has a true key role in safeguarding society from security threats and thus is the main consumer of security products and services. Yet, its role does not circumscribe to be a mere customer that sets the demand of many security products and services of government agencies involved in the direct protection the citizens, but also in the setting up of public policies, laws, regulations that specify legal security obligations of firms and individuals and features and performance of security goods and services (e.g. privacy rights). These regulations may have a significant impact on the economy in terms of required investments, trade frictional cost, or welfare losses. In addition, the Public Administration may stimulate security investment providing aids and subsidies, or act as a locomotive in the development of new solutions through the financing of research and large acquisitions. This role greatly influences demand and supply in this sector, as well as the behaviour of private agents. Main purchasers are law enforcement, civil protection and emergency organizations. They may operate at local, regional, national, European or even supranational level.

The analysis of the demand should identify the preferred goods and services of each type of customer and the reasons behind it, such as risk perception, loss expectation, risk aversion and the investment required to gain a feeling of confidence or peace of

mind[18] as well as other related factors with influence in the purchasing decision such as general economic growth, network economies and bounded rationality.

<Table 1>

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, courts of justice, and prisons. This value is 25% smaller when compared with the defence sector. Once again, we see that the four main consumers are the United Kingdom, Germany, France and Italy. The table shows a moderate growth rate similar to defence expenditures. However, these values could only be considered an estimate of demand size, because these numbers also reflect purchases of goods and services not related to this market (e.g. fuel). Furthermore, it does not consider the expenses of private agents as companies and individuals. Civitas Group estimated this value around 43% of government expenditures. An approximation to this value so far seems achievable only through indirect methods such as the one mentioned in Hobijn (2002).

To forecast the future of security demand is even more difficult, since it depends on many factors previously mentioned. These factors are difficult to measure accurately, and their true influence on demand is unclear. Yet a large security incident in the world or a general economic crisis may have a more direct impact on security investment. Growing rates have been given in some documents, but they seem a futile theoretical exercise. For example, the OECD (2004) report estimated a growing rate of 7-8%

[18] This value depends on the frequency and the type of incidents, the range of possible targets, the sophistication of the attack method and the countermeasure complexity. This perception is often based on cognitive experience of the past rather than estimates of probability of future events.

annually a truly healthy value that is coherent with the previous table, but only for 2004. The Homeland Security Research Corporation estimated a steeper trend for reaching an expenditure of around 178 billion $ in 2015, a value that means an approximate yearly growth rate of 15% for Europe. Frost and Sullivan (2005) estimates this value for Europe at 10% annually over the coming years. These values seem too high, when compared with the growth rate of the previous table, the latter values possibly suggesting a higher inertia to raise investment even in the presence of large attacks such as the Madrid (2004) and London (2005) bombings.

Therefore a more accurate measure of the demand and the driving force of investments in security are a relevant research issue. For example, globalisation is increasing the flow of persons due to immigration or tourism, and the flow of merchandise, or e-commerce on the internet. Such growth is increasing terrorism and organised crime opportunities and the threat level. These facts press on a large demand of products and services, in terms of quantity and better quality, to cope with this higher risk that partially explains the protracted growth of the market.

Another question to evaluate is the potential fragmentation of this market in Europe –as EOS(2009) states–, in particularly in the field of Public Procurement. Such a fragmented market may hinder the achievement of economies of scale and may impede an adequate allocation of research and procurement resources that may be suboptimal due to duplication of programmes, especially when their complexity recommends a more cooperative approach and the funding of a single project.

The demand for security in other areas of the world that may potentially be supplied by the European Security industry should be a relevant area of study. Customers such as China, India and Brazil, as they progress will increase their security spending, whilst they do not always have enough proficiency to indigenously produce the security equipment. An indicator could be the demerged information of the balance of payments in relation to security products and services sales. Available information from Eurostat could facilitate its measure. Yet, these sales might be merged within broader accounts such as electronic equipment. Conversely, imports of security and intermediate products should also be assessed in terms of higher competition and potential bottlenecks for manufacturing the final product.

PERFORMANCE ANALYSIS

Any research agenda should evaluate the performance of the market. This is a complex task due to the variety of industries in this economic sector and the availability of sufficient information to perform the analysis. Such analysis, even based on qualitative information, when quantitative data is not available, is required when searching for policies that may enhance this sector.

Performance analysis tries to evaluate if industry: is efficient at allocating resources; is able to exploit economies of scale, scope, and learning; and shows a dynamic trend to provide innovative high value security products and services at the lowest cost, while adequately remunerating their shareholders. Since competition stimulates a better allocation of resources one of the main areas of research in performance analysis is the analysis of market structure and conduct of the industry as long as they assure, over the

long run, a *workable competition* where efficient firms are rewarded and inefficient ones are punished. If this dynamic is present, the market will be driven to greater efficiency over time to the maximum benefit of customers. The analysis should be made jointly examining basic market conditions and government policies as both provide the general framework to the industry.

This *structure, conduct and performance* model for performing industrial analyses was pioneered by Bain (1956). The model has been further reviewed and refined by many authors such as Scherer and Ross (1990) or Martin (1993). This theoretical framework is still a rich source of guidance for industrial analyses of many economic sectors including defence (Hartley, 2007).

Basic conditions

Basic market conditions analyses questions related to demand, such as price elasticity, substitutes, market growth, demand cyclicality, and purchasing methods; as well as issues related to supply such as cost structures, inputs, technology, and information. These conditions have influence on the structure of the industry and the attractiveness of the sector to new investors.

Structure

The number and size distribution of buyers and sellers in the market, entry conditions, product differentiation, vertical integration, diversification, and imports are elements of the market structure with influence in the degree of competition in the market and the

strategic behaviour of the industry. For example, economies or large scale production or large investment means entry barriers that may result in few new entrants.

Conduct

Market conduct assesses the actual behaviour of firms with regards to pricing, product strategy, advertising, research and innovation, and other tactics to maximize profits. If market concentration is low, decisions are made more independently, but when concentration is high, competitors' behaviour will have a strong influence in company behaviour and industry will be more tempted to shape the market to its own benefit. In such cases, industry conduct may not be optimal from the societal point of view.

Performance

As has been noted, market performance is the ultimate arbiter on how well market forces are doing. The analysis should evaluate if market incentives are appropriate to reach a good performance and there are some restraints of current structure and conduct that degrade market efficiency to satisfy society needs in security. Of particular relevance is the dynamic performance that results in product and services with improved performance and lower cost. Performance can be assessed through some indicators like product quality, allocative and productive efficiency, equity value and profitability, etc.

Government policy

Finally, government policy has a strong influence on the sector. First, it fixes competition policy and assures a level playing field. Second, it is an important supporter of market performance providing subsidies and other incentives to finance research, development and innovation. Third, it is the largest purchaser of goods and services (e.g., e-passports) playing a key role in market growth. Fourth, it fixes minimum security requirements for private business through laws and regulations strongly influencing demand. Fifth, it also plays a key role in the development of standards and agreements in an economic sector were network effects are quite important.

CONCLUSION

This paper has presented a research agenda for improving what is known about the security sector in the European Union. It has drawn a first description of the sector, the main types of goods and services offered and some of the relevant technologies used. It has described methods for data collection, the mapping of industrial capabilities, demand analysis and performance analysis. The main hurdles that any agenda has to overcome in order to achieve the desired goal have also been highlighted. Poor and sparse information are noted as the main obstacle in reaching reliable conclusions.

The implementation of the agenda would provide relevant findings that will help to review initial assumptions and hypotheses about this industry, and reveal new research paths. It may depict a clearer image facilitating a better judgement to those attempting to define policies and plans aimed at improving this relevant economic sector for the security of Europe and its citizens.

SOME INFORMATION SOURCES IDENTIFIED

<table 2>

REFERENCES

Bain, Joseph S. (1956) Barriers to New Competition: their character and consequences in manufacturing industries. Cambridge, MA. Harvard University Press.

Bush, George W. (2002). The Department of Homeland Security.

Civitas Group (2006). The Homeland Security Market. Essential Dynamics and Trends.

CoESS (2008) Private Security. Fact and Figures 2008.

ECORYS Research and Consulting (2009). Study of the competitiveness of the EU security industry.

EOS - European Organisation for Security (2009). Priorities for a future European Security Framework.

European Union (2005). The European Union Counterterrorism Strategy.

European Union (2007). Green paper of biopreparedness.

European Union (2007). Towards a general policy on the fight against cyber crime. COM (2007) 267 Final.

Europol (2008). EU Organised Crime Threat Assessment.

Europol (2009). EU Terrorism Situation and Trend Report.

Frost and Sullivan (2005). European Homeland Security. A Market Opportunity Analysis.

Gartner (2009). Market trends: Security Market, Worldwide 2007-2013.

Hartley, K. (2007). The arms industry, procurement and industrial policies, in Handbook of defence economics II. Chapter 33. page 1139-1176. North Holland.

Hobijn, Bart (2002). What Will Homeland Security Cost? Economic Policy Review, Volume 8, Number 2.

Homeland Security Research Corporation (2005). Homeland Security and Homeland Defence. Global Market Outlook 2006-2015.

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.

Institute for Protection and Security of the Citizen (2005). Emerging technologies in the context of security. Joint Research Centre.

Martin, Stephen (1993). Advanced Industrial Economics. Blackwell Publishers. Cambrigde, Massachusetts. USA.

OECD (2004). The Security Economy.

OECD (2003). Emerging Risks in the 21st Century. An Agenda for Action

OECD (2008). Malicious Software (malware). A security threat to the Internet Economy.

Scherer, Frederic and Ross, David (1990). Industrial market structure and economic performance. Boston. Hougthon Mifflin.

Van de Voort, Maarten & O'Brien, Kevin (2003). Seacurity. Improving the Security of the Global Sea-Container Shipping System. Rand Europe.

Wharton Risk Management and Decision Process Centre (2005). TRIA and beyond. Terrorism risk financing in the US.

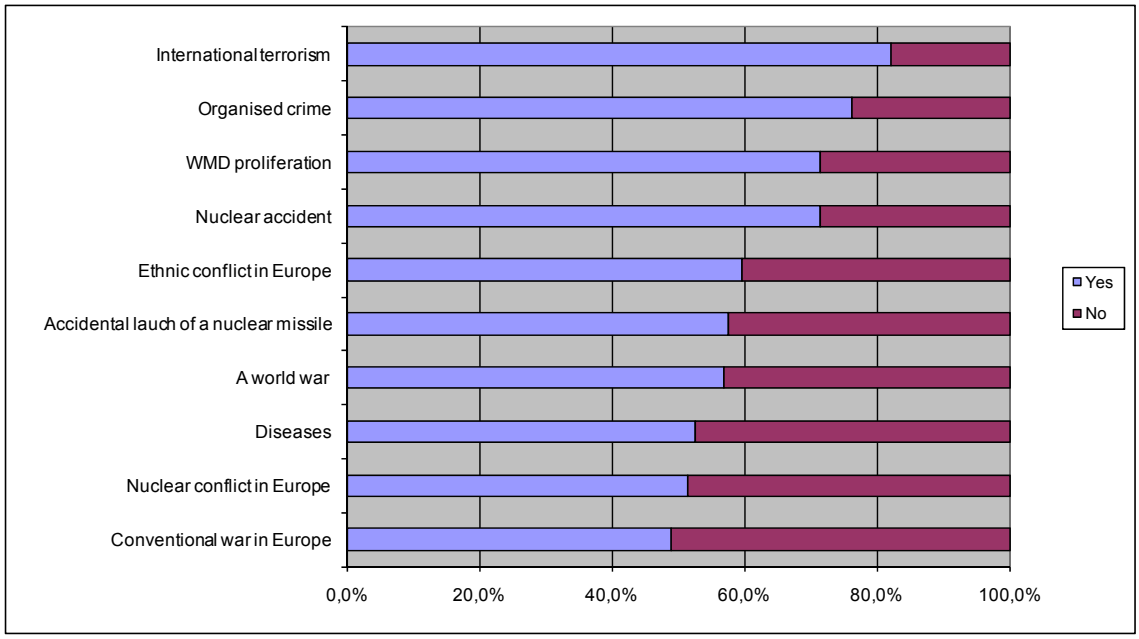

Figure 1. What do European Union citizens fear? Source: Eurobarometre, Sondage no. 58.1 Oct./Nov. 2002.

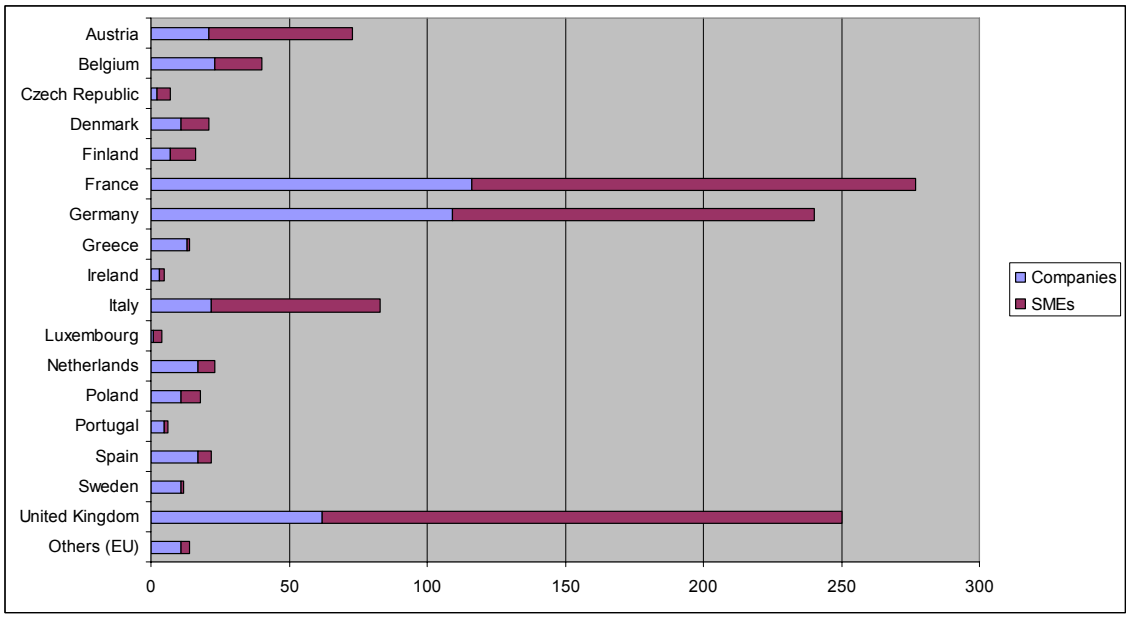

Figure 2. Number of European companies working in the security sector. Source: European Security Directory 2009

	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	-	845.4	983.0	1,064.7	1,428.6	1,653.8	1,960.0
Romania	-	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 in M€ (2003-2007)
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)

Name	Organisation	Web address	Information
DG ENTR	Directorate General Enterprise and Industry	ec.europa.eu/enterprise/security/index_en.htm	Security research
DG JLS	Directorate General Justice, Freedom and Security.	ec.europa.eu/dgs/justice_home/index_en.htm	Security action Plans.
ESRIF	European Security Research Information Forum	www.esrif.eu	Security research
EOS	European Organisation for Security	www.eos-eu.com	Security stakeholders.
ESD	European Security Directory	www.esd-partners.com	European Security industry.
EUROSTAT	European Statistical Agency	ec.europa.eu/eurostat	European and Member States statistics.
STACCATO	Stakeholders Platform for Supply chain Mapping, Market Condition Analysis and Technologies Opportunities	www.asd-europe.org/Content/Default.asp?PageID=34	Security supply chain, market conditions and Technology analysis.
	Europe infoway	www.security-europe.info	Security, safety and fire directory
COESS	Confederation of European Security Services	http://coess.org/about.htm	Providers of protection services (guards)
ECSA	European Corporate Security Association	http://www.ecsa-eu.org	Corporate Protection
EURALARM	Association of European	http://www.euralarm.org	Installer of fire

	manufacturers and installers of fire and security systems.		and security alarm systems mainly for private agents.
ENISA	European Network and Information Security Agency	http://www.enisa.europa.eu	Security of networks and information.
OECD	Organisation for Economic Co-operation and Development	www.oecd.org	World economic trends.
IMF	International Monetary Fund	www.imf.org	World economic Outlook.
World Bank	World Bank	www.worldbank.org	World economic information.
IPSC	Institute for the protection and the security of citizen	ipsc.jrc.ec.europa.eu	Research on citizen security.

Table 2. Sources of information identified.