D.1.2

Taxonomy of Security Products, Systems and Services

Author(s): Thordis Sveinsdottir, Rachel Finn, Rowena Rodrigues, Kush Wadhwa (Trilateral Research & Consulting), Florian Fritz, Reinhard Kreissl, Roger von Laufenberg (IRKS Research) Paul de Hert, Alessia Tanas, Rosamunde van Braakel (Vrije Universiteit Brussel)

Dissemination level: Public

Deliverable type: Final

Version: 1

Submission date: 31 July 2014
Table of Contents

1 Introduction ........................................................................................................................................... 5
  1.1 Objectives and approach .............................................................................................................. 7
2 European Security Policy ..................................................................................................................... 8
  2.1 Disruption of international, serious and organised crime networks ........................................... 9
  2.2 Prevention of Terrorism and the addressing of radicalisation and recruitment ...................... 9
  2.3 Raising levels of security for citizens and businesses in cyberspace ...................................... 10
  2.4 Strengthening of security through border management ............................................................. 10
  2.5 Increase Europe's resilience to crises and disasters ................................................................. 11
3 Current categorisations of security sectors, products and systems ................................................. 13
  3.1 The European Commission ........................................................................................................... 13
  3.2 Ecorys studies on the EU security industry .................................................................................. 15
  3.3 European security and security certification projects ................................................................. 17
  3.4 Commercial taxonomies .............................................................................................................. 34
4 CRISP needs-based taxonomy of security products and systems ..................................................... 40
  4.1 Security application areas (Level 1) ............................................................................................ 40
    4.1.1 Border management .............................................................................................................. 40
    4.1.2 Critical Infrastructure ........................................................................................................ 40
    4.1.3 Households and individuals ............................................................................................... 41
    4.1.4 Public and semi-public venues ........................................................................................ 41
    4.1.5 Industrial and Retail .......................................................................................................... 42
    4.1.6 Emergency Preparedness Centres/Crisis Management .................................................. 42
    4.1.7 Transport .......................................................................................................................... 43
  4.2 Security demands (Level 2) ........................................................................................................... 44
    4.2.1 Access control .................................................................................................................... 44
    4.2.2 Asset/freight/cargo security ............................................................................................... 44
    4.2.3 Cyber security .................................................................................................................... 44
    4.2.4 Employee/visitor safety .................................................................................................... 45
    4.2.5 Loss prevention/shrinkage ................................................................................................. 45
    4.2.6 Perimeter/area/building security ....................................................................................... 45
    4.2.7 Point of transaction ........................................................................................................... 45
    4.2.8 Situation awareness ......................................................................................................... 46
  4.3 Security Needs/Functions (Level 3) ............................................................................................... 46
5 CRISP taxonomies of Security Products and Systems ........................................................................ 49
  5.1 Border Management Taxonomy ................................................................................................... 49
  5.2 Critical Infrastructure Taxonomy ................................................................................................ 51
5.3 Emergency Preparedness Centres/Crisis Management Taxonomy .................................53
5.4 Household and Individuals Taxonomy ........................................................................55
5.5 Industrial and Retail Taxonomy ..................................................................................56
5.6 Public and Semi-Public venues Taxonomy ..................................................................58
5.7 Transport Taxonomy ....................................................................................................60
5.8 Conclusion ....................................................................................................................62

6 Security Services: Criteria for Classification .....................................................................63
6.1 Towards a working definition of services ......................................................................63
6.2 General market framework for services .......................................................................64
6.3 Security: Public good or market commodity? ...............................................................65
6.4 Security as Profession and training requirements .........................................................66
6.5 Existing attempts at building categories of private security services ..............................72

7 CRISP Taxonomy of Security Services ...............................................................................75
7.1 Adaption of the categorisation of the Products and Systems Taxonomy for the Services .................................................................75
7.1.1 Security Services and Application Areas .................................................................75
7.1.2 Additional Functions ...............................................................................................77
7.2 Border Management Taxonomy ....................................................................................79
7.3 Critical Infrastructure Taxonomy ................................................................................81
7.4 Crisis Management Taxonomy ......................................................................................83
7.5 Household and Individuals Taxonomy ..........................................................................84
7.6 Industrial and Retail Taxonomy ....................................................................................86
7.7 Public and Semi-Public venues Taxonomy ....................................................................88
7.8 Transport Taxonomy ....................................................................................................90
7.9 Conclusion ....................................................................................................................92

8 Conclusion .......................................................................................................................93

9 References .......................................................................................................................96

Appendix A. List of reviewed Security Companies .................................................................100
Appendix B. List of Reviewed Security Services .................................................................102
Table of Figures

Figure 1: Matrix of the Staccato taxonomy ................................................................. 29

Table 1: EU security priority areas and relevant CRISP application areas ......................... 12
Table 2: Ecorys (2011) typology of security products and associated policy challenges ...... 17
Table 3: IRISS typology of surveillance technologies and use ........................................ 20
Table 4: IRISS typology of security technologies and use ............................................. 21
Table 5: IRISS typology of application areas and surveillance security products ............. 23
Table 6: The PACT categorization of security technology families and areas of use ........... 25
Table 7: SAPIENT categorisation of surveillance technologies according to technology “family”........................................................................................................................... 27
Table 8: SAPIENT categorisation of surveillance technologies according to surveillance function ................................................................................................................. 27
Table 9: Key ESEM issues per mission ........................................................................... 27
Table 10: Honeywell Markets & Solutions .................................................................... 32
Table 11: Honeywell categorisation for security needs .................................................... 35
Table 12: BOSCH categorisation of security areas ......................................................... 36
Table 13: BOSCH categorisation of security systems and products ................................ 37
Table 14: Tyco categorisation of security markets .......................................................... 38
Table 15: Tyco categorisation of security solutions, products and systems .................... 39
Table 16: CRISP security functions/needs ...................................................................... 48
Table 17: General Information and economic aspects of the European market in private security services ............................................................................................................. 64
Table 18: Drivers of public vs. private security, according to Smith and Brooks ............. 66
Table 19: Sample of academic study programmes preparing for security-related services (taken from FÖS 2014) ........................................................................................................................................ 68
Table 20: Training requirements security service providers need to fulfil according to EN 160782:2011 ......................................................................................................................... 72
Table 21: Security practices, as elaborated by Brooks (2009) ......................................... 72
Table 22: Security classification model developed by ASIS International ....................... 72
1 INTRODUCTION

In order to assist with the challenge of determining the needs for certification, this task examines the diversity of security products and systems and produces a useful, needs-based taxonomy in order to categorise these. The partners examined the security industry and current security solutions, along with reviewing EU security policy and related EU security, and security certification projects, in order to come up with a taxonomy that covers application areas currently active in the European security landscape.

In this taxonomy we lay particular stress on classification of products and systems through seven defined application areas. These were identified through a review of policy literature and commercially defined security sectors. The seven application areas are:

- **Border management**
- **Critical infrastructure** (e.g., electricity generation/transmission, gas and water systems, banking and finance systems)
- **Emergency preparedness centres/Crisis management**
- **Households and individuals**
- **Industrial and retail**
- **Public and semi-public venues**, including entertainment, government buildings, hospitals, campus, sport, culture, houses of worship, etc.
- **Transport**, including aviation, maritime and railway

This categorisation is important as any new proposal for evaluation and certification schemes for security products will need to work across these security sectors. What this chapter first and foremost highlights is the great diversity of security products and systems, but also the commonalities in their functions across application areas.

The taxonomy is grounded in the five EU Security priority areas and the following EC action points, which give an indication of which application areas and security needs remain a priority for Europe. These seven areas were chosen from synthesising areas identified in policy literature and from examining categorisations from large security suppliers, all of which categorise security equipment based on a perceived need of the customer.

Further to identifying application areas, this chapter also identifies key security demands by a review of commercial security company websites, and through a review of European policy literature and related security research projects. The demands that featured most prominently were synthesised into eight categories:

---


• Access control
• Asset/freight/cargo security
• Cyber security
• Employee/visitor/passenger safety
• Loss prevention/shrinkage
• Perimeter/area/building security
• Point of transaction security
• Situation awareness

Underpinning these demands are certain security needs, as identified in Deliverable 1.1 of the CRISP project, *Glossary of Security Products and Systems*. As these are covered there in great detail, only a short summary of each is included in this deliverable.

We are aware that application areas, security demands and needs do differ theoretically in their representation within contemporary society and culture, however as this task is a practically-oriented one, the key focus here is on physical products and systems which are amenable to certification and standardisation. We acknowledge also that there is a considerable overlap in needs and functions across the areas, and they are not mutually exclusive. Security is a complex political, social and cultural domain, and, as such, holds differing views, preconceptions, aims and needs.

It is, however, our aim to take a product and systems-oriented focus in the CRISP taxonomy, so that a large section of the security market may be covered. It should be stressed here that the taxonomy is a living document, to which new products and systems will be added as technology advances and application areas change.

Using the same system of classification as products and systems, security services are discussed in this deliverable with a view to highlighting major requirements for services standardisation and certification, building on training curricula of already existing services standards and terminology. Services operate in a very complex legal and regulatory environment. While partly the emergence of the “security professional” is discernable, there is also a tendency to develop very context-specific standards for services (such as those related to aviation or port/ maritime security). By using the same classification scheme (regarding application areas and demands for measures/solutions), the ground is laid for future analysis of the relationship between products and services, taking into account training requirements.

---

1.1 Objectives and Approach

The objectives of WP1, under which the taxonomy falls, are as follows:

- To provide a better understanding of security products and systems, concepts of operations, application areas and performance and develop a taxonomy for them;
- To provide a better understanding of security-related services;
- To set out criteria for comparing security products and systems to facilitate evaluation and certification through a harmonised approach.

In order to meet these aims, the CRISP taxonomy approach includes the review of a number of different taxonomies and categorisations of security sectors, demands, needs, products and systems, with the aim of delivering a clear and useful taxonomy for the purposes of standardising and certifying said products and systems. The taxonomy is based on desk research, including a review of European security strategy documents, European security and security certification research projects, as well as a review of security company websites in order to ascertain how the industry categorises security sectors, needs, products and systems.

The industry review was conducted by drawing on the CRISP partners’ database of security and surveillance companies, focusing firstly on large companies that provide a broad range of security products and systems and secondly on smaller companies who provide more specialised products. As is evident in this report, there are myriad ways in which security sectors, technologies, needs, products and systems can be categorised. For the purposes of building the CRISP taxonomy, these categorisations were synthesised to produce a products, systems and services-focused and needs-based taxonomy, with the aim of covering a broad range of equipment.

While categorisations of sectors/application areas differ between policies, projects and industries, there are also strong similarities, which were used to form the application areas that underpin the CRISP taxonomy. For the purposes of clarity and in keeping with the aims of this specific task, security application areas identified in other instances as separate were merged, as they were seen to be operationally similar, in that their security operations and consequent needs did not differ practically to a significant extent. An example of where categories were merged was in our application area transport, which includes aviation, maritime and railway. This is furthermore supported by the EC classification of the transport policy area, which covers air, road, rail, maritime, and inland waterways transport.

The next level of the taxonomy lists key security demands, identified and synthesised from a review of EU security policy, security research projects and end-user demands via a review of commercial websites. For the purposes of simplification and clarity, these demands are defined as practice-oriented; i.e., the focus is on a desired function of a product (e.g., access control) rather than or threat-oriented (e.g., fight against terrorism). This allows for a clearer categorisation of end products and systems as they are categorised on the basis of a specific

---

need, which form level three of the taxonomy through which security systems and products are further categorised.

The end of each branch of the taxonomy (level four) lists different security products systems and services, which were identified by a review of security industry websites and their commercial offerings. We note that each product listed has the potential to stand alone or become a part of a security system, many of which are tailor-made for specific customer needs. The same goes for the security services, which – although they can be – are seldom deployed without the usage of other security products and systems. Some of the services are the result of security systems, as for example alarm and CCTV monitoring. Many of the products and systems listed can furthermore be integrated with other commercial systems, such as logistics and stock management systems. The latter do not form part of the taxonomies, as the fall outside the scope of the project. Furthermore, products that fall clearly within the defence application area are excluded for the same reason.

The CRISP taxonomy was designed with function and need in mind. It will be a living document, which can change to incorporate new application areas, demands, needs and products. The branches are not mutually exclusive, and there is a level of repetition across taxonomies, as any security PSS may meet different needs and are thus placed on separate branches.

2 EUROPEAN SECURITY POLICY

In order to contextualise the CRISP taxonomy, partners first considered the five EU security priority areas presented in the EU Internal Security Strategy\(^4\) (ISS) and the five action points raised in order to reach the aims put forward by the EC. This is in line with conclusions regarding the state of the art in analysing and categorising the European security market, as e.g. evidenced by the Programming Mandate 487:

“At the same time, security solutions and services are not developed or deployed in a political vacuum, and efforts to support Europe’s security should be informed by the security objectives set by the EU and the Member States in the ESS, ISS and national security strategies.”\(^5\)

The EU ISS presents a shared agenda for the Member States, and the European Council, Commission and Parliament, as well as local authorities and the general public. The Strategy and action points were reviewed in order to identify and synthesise key areas, demands and needs for the purposes of building a taxonomy relevant for EU security policy. The five action points are as follows:

---


2.1 DISRUPTION OF INTERNATIONAL, SERIOUS AND ORGANISED CRIME NETWORKS

The first action point pertains to the disruption of serious and organised crime networks whose illegal activities include trafficking in human beings, drugs and firearms; money laundering; illegal shipment and dumping of waste inside and outside of Europe. Local manifestations can include burglary, car theft and sale of counterfeit and dangerous goods. In order to meet these aims, the document includes key action points, such as:

Actions proposed by the EC: A sustained collaborative effort from the EC and Member States to identify and dismantle criminal networks through understanding their operation methods and finance means. This will include diverse approaches (e.g., collection of passenger records, review and targeted use of the EU anti-money laundering legislation, strengthening of joint operations across EU between police, customs, border control and the judicial system). Furthermore, there needs to be an effort to combat corruption and ensure due process and use of administrative methods that help protect the economy against criminal infiltration. EU legal framework around the confiscation of criminal assets needs to be strengthened and mutual confiscation orders between Member States must be recognised. Criminal networks operate across borders, and information flow between agencies in Member States and outside of Europe is seen as key in this battle.

2.2 PREVENTION OF TERRORISM AND THE ADDRESSING OF RADICALISATION AND RECRUITMENT

Threat from terrorism is presented as ever present and constantly evolving, as terrorist organisations are seen to quickly adapt and innovate. The EC proposes the following actions: Empowerment of communities to prevent radicalisation and recruitment is seen as a vital part of diminishing this threat. In terms of security actions the proposal is to firstly work towards a framework for administrative measures regarding freezing assets to prevent terrorism and related activities. For this, the bilateral US and EU agreement and signature of the Terrorist Financing Tracking Programme remains important step towards the proposed EU policy for extraction and analysis of financial messaging data. Also, the prevention of access to explosives (2008) and CBRN substances (2009) is seen as priority legislative and non-legislative actions. EU should also aim to strengthen border control and export control systems within Europe and internationally. A high priority is to secure and protect transport, both aviation and maritime. Continuous strengthening of inspections and enforcements regimes is needed with regard to monitoring cargo operation and passenger movements. A

---

stronger focus on land transport security, especially passenger transport security, is needed to cover local and regional rail, as well as high speed rail and related infrastructure.

2.3 RAISING LEVELS OF SECURITY FOR CITIZENS AND BUSINESSES IN CYBERSPACE

Citizens, businesses, governments and critical infrastructures in Europe are increasingly targeted by cybercriminals due to increasingly advanced Internet infrastructure. Security of IT networks as essential for a well-functioning society, is recognised by the Digital Agenda for Europe\(^9\), which addresses cybersecurity, cybercrime, safer Internet and privacy as key components in building security for users.

The first step is seen to be capacity building in law enforcement and judiciary and works towards establishing The EU Cybercrime Centre (EC3) at Europol will allow for the building of operational and analytic capacity for investigations and cooperation with Member States and internationally. Member States are furthermore encouraged to develop their own cybercrime training, awareness and response and set up centres at a national level or in cooperation with other Member States. They should work with industry to empower and protect citizens and make reporting of cybercrime easy and straightforward, as well as guiding people in how to protect themselves and their assets online. The EC will furthermore tackle the handling of illegal Internet content and improve capability for dealing with cyber-attacks.

2.4 STRENGTHENING OF SECURITY THROUGH BORDER MANAGEMENT

With common external borders, smuggling and other cross-border illegal activity must be targeted at a European level, hence efficient control of EU’s external borders is crucial. In relation to movement of persons, the EU can treat migration management and the fight against crime as twin objectives of the integrated border management strategy.

The EU’s border management strategy is based on three strands\(^10\):

- An enhanced use of new technology for border checks
- An enhanced use of new technology for border surveillance
- An enhanced coordination of Member States through Frontex

Actions proposed from the EC: Firstly, to fully utilise EUROSUR\(^11\), which has an established mechanism for Member States to share information related to border surveillance and for cooperation with each other and with Frontex\(^12\) at tactical, operational and strategic level. EUROSUR utilises new technologies such as satellite imagery to detect and track targets at the maritime border, e.g., tracing fast vessels transporting drugs to the EU. Secondly, by enabling cooperation and information sharing between Member States and pan-European institutions such as Europol. Thirdly, to enable common risk management among member

---


\(^12\) Frontex, “Frontex”, no date http://frontex.europa.eu/
states. The Common Risk Management Framework (CRMF) entails continuous screening of electronic arrival/departure data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately.

### 2.5 Increase Europe's Resilience to Crises and Disasters

Following an increase in the frequency and scale of natural and man-made disasters a need for more coherent and better integrated European crisis and response capacity is needed. Actions proposed by the EC are to, firstly make full use of the Lisbon Treaty solidarity clause\(^ {13}\); secondly to develop an EU risk assessment and mapping guidelines for disaster management. The Commission will furthermore support efforts to establish a mutual understanding of various definitions of threat levels and to improve communication when levels are subject to change. Fourthly, the Strategy proposes that a strong link needs to be built in order of different situation awareness centres to communicate and pull together an accurate overview of the situation.\(^ {14}\)

From synthesising reviews on EU policy and projects, as well as markets identified in the commercial security sector, seven application areas were identified within which security efforts contribute towards action in the five EU Security Strategy priority areas:

<table>
<thead>
<tr>
<th>EU Security Priority Area</th>
<th>Application Area Involved</th>
</tr>
</thead>
</table>
| Disruption of international, serious and organised crime networks | Border management  
Households and individuals  
Industrial and retail  
Public and semi-public venues  
Emergency Preparedness Centres/Crisis Management  
Transport |
| Prevention of terrorism and addressing of radicalisation and recruitment | Border management  
Critical infrastructure  
Public and semi-public venues  
Emergency Preparedness Centres/Crisis Management  
Transport |
| Raising levels of security for citizens and businesses in Cyberspace | Border management  
Critical infrastructure  
Households and individuals  
Industrial and retail  
Public and semi-public venues  
Transport |


Strengthening of security through border management | Border management  
Industrial and retail  
Transport  
Emergency Preparedness Centres/Crisis Management  

Increase Europe’s resilience to crises and disasters | Border management  
Critical infrastructure  
Households and individuals  
Industrial and retail  
Public and semi-public venues  
Emergency Preparedness Centres/Crisis Management  
Transport  

Table 1: EU security priority areas and relevant CRISP application areas

The EU Internal Security Strategy serves as the foundation for the CRISP taxonomy, as it presents the five priority areas, where efforts will be concentrated, and consequently where relevant priority security products and systems will be identified and used. The priority areas are broad, and as such difficult to use as a first level of a taxonomy, which aims to categorise security products and systems. Hence, the concept of a somewhat narrower application area, where use is clearly defined, came about. We however, ensured that each of the seven CRISP application areas were relevant, to one or more, of the five priority areas, i.e., that security efforts within each application area contributed to assist the EU in their work to strengthen the internal security in Europe.
3 CURRENT CATEGORISATIONS OF SECURITY SECTORS, PRODUCTS AND SYSTEMS

In order to contextualise and inform the CRISP taxonomy, the partners reviewed categorisations and taxonomies of security, security sectors, needs, products and systems, from the EC and related security and security certification projects. This work demonstrates the multidimensional nature of the security sectors, product and system categorisations, which was then synthesised to build a taxonomy fit for purpose, i.e., to certify and standardise security products and systems. This review also serves to ensure that the CRISP taxonomy is relevant and useful for building a certification scheme for security products and systems in Europe.

3.1 THE EUROPEAN COMMISSION

The 2012 Action Plan for an innovative and competitive Security Industry\(^\text{15}\) states that there is currently no clear definition of the European security industry and a methodical classification of this industry is hindered by a number of factors, such as:

- The industry is not covered as such by the main statistical nomenclatures
- The production of security-related items is hidden under a wide range of headings and consequently statistics may be unreliable, as these do not distinguish between security and non-security activities.
- There is no statistical data source available at European level from the industry itself
- Procurers of security equipment and systems can be reluctant to provide information on security expenditures.

The Action Plan claims the security market is an extremely fragmented market, and that “divergent approaches have led to the creation of at least 27 different security markets, each of them being split into a large number of security sectors”\(^\text{16}\). The document argues that this market fragmentation has a negative impact on both supply-side and demand-side and leads to high barriers to market entry and makes economics of scale difficult. It leads to a lack of competition among suppliers and suboptimal use of public money.

The EC identifies three ways in which market fragmentation can be overcome, two of which are of interest to the CRISP project:

- **Standardisation.** Standards are seen to play a major role in defragmenting markets and are of utmost importance for interoperability of technologies. Standards are essential for ensuring uniform quality and are an important part of the move towards global competitiveness of the EU security industry. Overall there is a lack of


\(^{16}\) Ibid., p. 18.
standardisation within these industries but the EC identified major gaps within the following areas:

- CBRNE- minimum detection standards and sampling standards
- Border Security, as in common technical and interoperability standards for automated border control systems and biometric identifiers
- Crisis management and civil protection, especially standards for communication, command and control interoperability, as well as mass notification of populations.\(^\text{17,18}\)

- **Certification.** There are no EU-wide certification systems for security products and systems. National systems can vary extensively and thus further contribute to market fragmentation. The EC has identified two areas within which a certification systems could be started:
  - Airport screening equipment
  - Alarm systems

The EC Action Plan broadly divides the European security industry into the following sectors, under which it groups an overview of the technologies and systems that characterise the different segments:

- Aviation security
- Maritime security
- Border security
- Critical infrastructure protection
- Counter-terror intelligence (including cyber security and communication)
- Crisis management/civil protection
- Physical security protection
- Protective clothing

All of the above categories and areas are included to a varying degree in the CRISP taxonomy. While aviation and maritime security sectors have been combined under Transport, border management, critical infrastructures and crisis management (here as Emergency preparedness centres/crisis management) feature as a separate application areas.

\(^{17}\) In 2013 these three sectors were identified as priority sectors for the development of standardisation roadmaps in Mandate M/487 which was carried out in order to analyse existing security standardisation landscape in Europe, and select priority sectors and develop standardisation roadmaps for said sectors.


### 3.2 Ecorys Studies on the EU Security Industry

Ecorys Research and Consulting has performed two studies on the EU security industry on behalf of the European Commission. Firstly a *Study on the Competitiveness on the EU security industry*,\(^\text{19}\) and secondly a final report on *Security Regulation, Conformity Assessment & Certification*.\(^\text{20}\)

The first report categorises the security market according to the nature of security threats and priorities, and demand and supply-side characteristics. The two threat, and consequently security, categories Ecorys identifies are:

- **"Traditional" Security**, which corresponds to protection against "endogenous" threats such as "ordinary" criminal activity, fire protection, etc.
- **"New" Security**, which includes protection against exogenous threats such as terrorism, organised crime, cybercrime and protection from and response to major catastrophic events.\(^\text{21}\)

In categorising security sectors on the demand-side, four main institutional demand segments are listed based on distinctions between external and internal security dimensions; and between civil and private security responsibilities:

- Defence support for internal security (e.g., support in major crisis incidents)
- Civil security – public sector non-military administration (e.g., counter terrorism, law enforcement, civil order)
- Mixed public-private sector security (e.g., critical infrastructure, utilities etc.)
- Private sector security (this segment may be further segmented by degree of potential vulnerability to new security threats).

From a supply-side perspective, the report identifies three main segments of the security industry:

- **Traditional security industry**, supplying general security applications, which correspond mostly to protection against “traditional” security threats but can also be an integral part of overall responses to “new” security threats (e.g., physical access control, intrusion and fire detection, CCTV/video surveillance)
- **Security-orientated defence industry**, which is based on either the application of defence-related technologies in the area of security or where defence-orientated companies have acquired and/or adapted “civilian” technologies in order to address capability requirements within security markets. These technologies correspond primarily to protection against “new” security threats


New entrants, which include two groups: Suppliers from other civilian industry sectors, and start-up companies based on the development and commercialisation of new and innovative security technologies.

In combining the above elements, the first Ecorys report arrives at a three-part security market segmentation:

- **“Traditional” security market:** for which supply is broad-based and security technologies fairly standardised and transferable across sectors
- **Defence market:** which acknowledges the role of military support for internal security
- **Emerging “new” security market:** within which demand is often characterised by a limited number of customers, whose security requirements can be quite highly specified. In many cases these are governments and administrations, who define the shape and structure of demand through security policy and regulation (e.g., critical infrastructure protection, border management, etc.).

In 2011, the Ecorys report on *Security Regulation, Conformity Assessment & Certification* classifies security products into two main categories, depending on familiarity of operation and function, and identifies the key policy challenges associated with each type and suggests possible EU policy solutions for security products:

<table>
<thead>
<tr>
<th>Type of Security products</th>
<th>Policy Challenges</th>
<th>Possible EU level policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>General purpose security products (Type-1): address “familiar” security situations (security threats or functions) and can loosely be called “traditional” security equipment (e.g., intruder detection, CCTV, access control, security barriers)</td>
<td>Absence of common EU certification of products: Separate certification schemes in different EU states and little or no recognition of standards between countries. Presents huge administrative and cost burden on manufacturers/suppliers and for SMEs especially is a huge barrier to market entry.</td>
<td>Standards harmonisation Market recognition of European standards recognition Conformity assessment and certification (building on existing schemes)</td>
</tr>
</tbody>
</table>
| Priority and sensitive security products (Type-2) are technologies that address “unfamiliar” or new types of threats (terrorism, organised crime, cyber-crime, etc.) that often require the development or application of new technologies and approaches. Changes in organisation and implementation of security functions, e.g., automatisation | Wider range of policy challenges due to links with EU internal security. | Regulation:  
- Product (supply) based, which would require a classification of products, needs to address variation in needs between fields  
- Sector (demand based) would complement existing sector based regulatory frameworks |
can also fall under this category.

| Hybrid - Any standards should demonstrate conformity to recognised standards |

Table 2: Ecorys (2011) typology of security products and associated policy challenges

The Ecorys categorisations are useful, in that they differentiate between “new” security threats and solutions and “traditional” ones, how they are framed within current economic policy and what consequences this may have for certification and standardisation. In developing the CRISP taxonomy, partners took care to include technologies and systems from both groups in order to arrive at a taxonomy that encompasses a broad range of both “new” and “traditional” products and systems. It also supports the notion that taxonomies of security products and systems should be flexible and amenable to change, due to the fast moving developments within the market.

3.3 European Security and Security Certification Projects

The deliverables of the following EU-funded security and security certification projects were reviewed with the aim of examining current attempts at categorisations of security sectors/areas, products and systems in order to provide building blocks for the CRISP taxonomy, and also to gather information on available security technologies and the market needs that they help address. The projects approach security, security products and the security market in different ways depending on whether the frame is societal (ETTIS, IRIISS) economical/market oriented (Ecorys, 2009, 2011, STACCATO) or technological (SAPIENT, PACT). These projects were chosen with a view to examine the different ways in which security products can be categorised from these different angles, in order to provide context and building blocks for the CRISP taxonomy.

*European Security Trends and Threats in Society - ETTIS*\(^{22}\)

The ETTIS project draws our attention to the fact that security is a concern at many different levels in contemporary society.\(^{23}\) The project categorises security into seven dimensions (physical security, political security, socio-economic security, cultural security, environmental security, radical uncertainty security and cyber security). In addition to being a concern for IGOs, states and enforcement agencies, other groups such as local authorities, civil organisations, private companies, voluntary groups and citizens may also have complex security needs. Threats, to which security is aimed and oriented, have also grown more complex and are perceived from multiple user viewpoints, e.g., security from the point of view of national sovereignty, or security as human-centre, “where individuals and communities have primacy over the state.”\(^{24}\)

\(^{22}\) European security Trends and Threats (ETTIS) project, “ETTIS project”, 2012  [http://ettis-project.eu/](http://ettis-project.eu/)

\(^{23}\) Lagazio, Monica, *Report on Research Approaches and Results*, D2.2 ETTIS project, July 2012.

\(^{24}\) Ibid., p.17.
Regarding security needs ETTIS categorises needs depending on stakeholder group. At the IGO and state level needs tend to refer to technological developments, institutional and policy support, knowledge management tools, foresight and strategic decision-making capabilities. With regard to societal and individual needs, these centre on strengthening prevention and preparedness, and response and recovery capabilities. Company needs centre on strengthening organisational capacity in order to protect key assets from attacks and failures, which will require development and enhancement of current and new technologies as well as the implementation of new internal processes.

With regard to security solutions, which are the key focus of research in EU-funded projects, ETTIS lists them as follows:

- Technological Solutions
  - Information, intelligence, surveillance and monitoring
    - Tools for sharing and managing information
    - Early warning systems, threat detection
    - Comprehensive surveillance for monitoring of borders
    - Sensors and facial recognition
    - Event detection
  - Detection technologies
    - Robotic devices
    - Sensors (fast working sensors, ease of use and mobile sensors)
  - CBRN and crisis preparedness
    - Sensing and detecting CBRN substances
    - Software and hardware tools supporting decision making in crises
    - Reliable means of communication
    - Indoor site navigation systems
  - Environment and radical uncertainty (including health)
    - Climate change related security efforts
  - Information and cyberspace
    - Cryptographic techniques
    - Operating systems
    - Anomaly detection
  - Space
    - Weather monitoring
    - Surveillance satellites
Although ETTIS identifies security technologies and systems that correspond with needs of various actors, it also demonstrates that many of the needs are focused on non-tangible solutions, such as training, policy, the need for dialogue, standards and reaching common understandings regarding security and its role. Furthermore, the project identifies how perceptions of security, differ depending on the level of each stakeholder, e.g., individuals and governments. The ETTIS categorisation method was helpful in drawing our attention to how to select and construct application areas and security demands that help arrive at tangible security solutions, i.e., products and systems that can be certified. ETTIS also contributed the areas of space and weather monitoring and a focus on information and cyberspace, both of which were incorporated in the CRISP taxonomy.

*Increasing Resilience in Surveillance Societies - IRISS*  

The EU FP7 project IRISS aims to investigate the societal effects of different “surveillance practices” from both a social science and legal perspective. In particular, the project focuses on those surveillance practices which are aimed at law enforcement and the fight against terrorism.

IRISS does not explicitly provide a taxonomy as such, but it extensively analyses the factors supporting the implementation of surveillance solutions by both public authorities and private actors. Great emphasis is given to the social and economic costs of said surveillance as well as to protection or infringement of civil liberties, fundamental rights and ethical aspects. In this respect, IRISS also provides for a brief taxonomy of social and economic costs related to surveillance and discusses the relevance of such costs for investment decisions and overall societal well-being.

In the sections below, we report the types of surveillance technologies and techniques that IRISS describes according to their uses in preventing and combating crime and terrorism. Secondly, we concentrate on the surveillance tools which, according to the project, made the object of increased usage for policy strategies after 9/11. Thirdly we report the list of surveillance solutions offered by companies in various surveillance areas.

---

27 Ibid., p.7.
28 Worthy of note is that IRISS creates a framework for a taxonomy of social and economic costs of surveillance. In this respect, the project puts forth two recommendations. First, more research in methods of the analysis of social and economic aspects of surveillance is needed to improve the reliability and comparability of such assessments. Second, the complexity of the involved issues and the danger of domination by individual interests demand representation of different interests and perspectives in any decision-making process on surveillance.
a) Surveillance technologies and techniques used in preventing and detecting crime and terrorism

According to IRISS, surveillance technologies can be grouped based on their functionalities which are those of identifying, locating, tracking individuals, screening populations and flows (data, money, etc.). The project investigates the operational effectiveness of the different technologies by placing them in context. Below is an overview of such technologies and of the areas where they are used.

<table>
<thead>
<tr>
<th>Type of technology / technique</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Administration (applicant background checks, receipt of benefits and receipt of credentials such as passports, criminal record-keeping, criminal identification, crimes investigation, forensic bio-information, drug testing technology</td>
</tr>
<tr>
<td>CCTV</td>
<td>Operation of traffic lights, crowd monitoring (banks, shops, restaurants and transport terminals), deterring and solving crime, automated number plate recognition</td>
</tr>
<tr>
<td>Facial recognition through data matching</td>
<td>Criminal identification, biometric visas and passports</td>
</tr>
<tr>
<td>Behaviour recognition</td>
<td>Identification of individuals, identifying suspicious or risky activities</td>
</tr>
<tr>
<td>Electronic monitoring</td>
<td>Understanding, predicting and modifying human behavior</td>
</tr>
<tr>
<td>Communication interception</td>
<td>Crime prevention; crime investigation; cyber situational awareness; protection of victims; acquittal of the innocent in criminal proceedings; social media monitoring and analysis: crowd sourcing</td>
</tr>
<tr>
<td>DNA profiling</td>
<td>Criminal investigation; forensic analysis; early identification, arrest of serial offenders; crime deterrence; profiling for law enforcement purposes</td>
</tr>
<tr>
<td>Body scanning</td>
<td>Airport security routines</td>
</tr>
</tbody>
</table>

Table 3: IRISS typology of surveillance technologies and use

---

29 Ibid., p. 12.
b) Surveillance technologies and techniques used in preventing and detecting crime and terrorism based on increased usage after 9/11

IRISS describes the events of 11 September 2001 as milestones for the co-evolution of surveillance technologies and practices. The following table provides the lists of surveillance technologies and techniques which, according to the project, were increasingly deployed as a consequence of policy responses to 9/11.

<table>
<thead>
<tr>
<th>Type of technology / technique</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government databases</td>
<td>Criminal records; policing and intelligence gathering; development of surveillance technologies such as satellites or wireless bugging</td>
</tr>
<tr>
<td>Web-generated data</td>
<td>Cyber surveillance.</td>
</tr>
<tr>
<td>Radio frequency identification (RFID)</td>
<td>Identifying and locating</td>
</tr>
<tr>
<td>GPS, GSM and Wi-Fi based location determination</td>
<td>Locating</td>
</tr>
<tr>
<td>Communications surveillance</td>
<td>Wiretapping (telephone lines, Internet calls)</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Identification and verification, criminal investigation, tracking of suspects, detection of suspect behavior; crime deterrent</td>
</tr>
<tr>
<td>Data processing / data mining</td>
<td>Group/personalised profiling, possible social sorting through “virtual selves”</td>
</tr>
</tbody>
</table>

Table 4: IRISS typology of security technologies and use

---

30 Ibid., p. 52.
31 Ibid., p. 58.
c) Surveillance solutions offered by surveillance companies

Below is the IRISS wide-ranging list of company products and services *vis à vis* their application areas.

<table>
<thead>
<tr>
<th>Application area</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government and law enforcement solutions</td>
<td>Airborne surveillance and reconnaissance aircrafts</td>
</tr>
<tr>
<td></td>
<td>Audio surveillance systems</td>
</tr>
<tr>
<td></td>
<td>Automatic identification systems</td>
</tr>
<tr>
<td></td>
<td>Biometric technologies and devices (biometric fingerprint, face, iris and voice identification and object recognition)</td>
</tr>
<tr>
<td></td>
<td>Cellular and telecoms monitoring – e.g., GSM monitoring systems</td>
</tr>
<tr>
<td></td>
<td>Coastal surveillance systems</td>
</tr>
<tr>
<td></td>
<td>Command and control systems</td>
</tr>
<tr>
<td>Communications and intelligence systems</td>
<td>Cross-domain information sharing tools</td>
</tr>
<tr>
<td></td>
<td>Data compilation and management</td>
</tr>
<tr>
<td></td>
<td>e-ID</td>
</tr>
<tr>
<td></td>
<td>Electronic intelligence and surveillance systems</td>
</tr>
<tr>
<td></td>
<td>e-Passports</td>
</tr>
<tr>
<td></td>
<td>Face recognition systems</td>
</tr>
<tr>
<td></td>
<td>Fingerprint identification systems and technologies</td>
</tr>
<tr>
<td></td>
<td>Geolocation or position determination via GPS or mobile phone triangulation</td>
</tr>
<tr>
<td></td>
<td>Identity management and credentialing solutions</td>
</tr>
<tr>
<td></td>
<td>Information systems</td>
</tr>
<tr>
<td></td>
<td>Intelligence collection and fusion</td>
</tr>
<tr>
<td></td>
<td>Intelligence, surveillance and reconnaissance systems</td>
</tr>
<tr>
<td></td>
<td>Intelligent CCTV with behaviour analysis capabilities</td>
</tr>
<tr>
<td></td>
<td>IP data inspection systems</td>
</tr>
<tr>
<td></td>
<td>Manned and unmanned aerial systems</td>
</tr>
<tr>
<td></td>
<td>Mobile identification</td>
</tr>
<tr>
<td></td>
<td>Mobile identity checks</td>
</tr>
<tr>
<td></td>
<td>Multi-sensor surveillance systems</td>
</tr>
<tr>
<td></td>
<td>National identity systems</td>
</tr>
<tr>
<td></td>
<td>Network surveillance</td>
</tr>
<tr>
<td></td>
<td>Offender monitoring systems</td>
</tr>
<tr>
<td></td>
<td>Operatives based surveillance</td>
</tr>
<tr>
<td></td>
<td>Radar</td>
</tr>
<tr>
<td></td>
<td>Radio monitoring and signal analysis</td>
</tr>
<tr>
<td></td>
<td>Remotely operated robots</td>
</tr>
<tr>
<td></td>
<td>Sensor technologies (e.g., fixed and mobile sensing, line sensors, point sensors, infra-red and thermal sensors)</td>
</tr>
<tr>
<td></td>
<td>Space and intelligence systems (including satellites and satellite monitoring)</td>
</tr>
<tr>
<td></td>
<td>Unmanned ground systems</td>
</tr>
<tr>
<td></td>
<td>Visual-range cameras</td>
</tr>
<tr>
<td></td>
<td>Voice and fax logging and analysis</td>
</tr>
<tr>
<td></td>
<td>Web intelligence tools</td>
</tr>
<tr>
<td>Wireless solutions (high-end radio communication systems for defense and commercial applications)</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Commercial solutions</strong></td>
<td></td>
</tr>
<tr>
<td>Advanced IP solutions</td>
<td></td>
</tr>
<tr>
<td>Biometric technologies and devices (biometric fingerprint, face, iris and voice identification, object recognition and eye tracking)</td>
<td></td>
</tr>
<tr>
<td>Business video surveillance</td>
<td></td>
</tr>
<tr>
<td>CCTV</td>
<td></td>
</tr>
<tr>
<td>Consumer information databases</td>
<td></td>
</tr>
<tr>
<td>Counter-surveillance products (counter-surveillance receivers, integrated detectors, radio monitoring systems, phone tap detectors)</td>
<td></td>
</tr>
<tr>
<td>Customer intelligence services</td>
<td></td>
</tr>
<tr>
<td>Data analytics (content analytics, mobile analytics, conversion analytics, social analytics and advertising analytics)</td>
<td></td>
</tr>
<tr>
<td>Data records storage solution</td>
<td></td>
</tr>
<tr>
<td>Employee background screening</td>
<td></td>
</tr>
<tr>
<td>Enterprise risk management platform</td>
<td></td>
</tr>
<tr>
<td>Face recognition systems</td>
<td></td>
</tr>
<tr>
<td>Geolocation or position determination via GPS or mobile phone triangulation</td>
<td></td>
</tr>
<tr>
<td>Hand-held bar code scanners</td>
<td></td>
</tr>
<tr>
<td>Identity solutions</td>
<td></td>
</tr>
<tr>
<td>IP data inspection systems</td>
<td></td>
</tr>
<tr>
<td>Logical access control solutions</td>
<td></td>
</tr>
<tr>
<td>Operatives based surveillance</td>
<td></td>
</tr>
<tr>
<td>Physical access control solutions</td>
<td></td>
</tr>
<tr>
<td>Remote patient monitoring (tele health)</td>
<td></td>
</tr>
<tr>
<td>Smart cards, readers</td>
<td></td>
</tr>
<tr>
<td>Vehicular surveillance solutions</td>
<td></td>
</tr>
<tr>
<td>Verification systems</td>
<td></td>
</tr>
<tr>
<td>Video analytics</td>
<td></td>
</tr>
<tr>
<td>Wireless sensing</td>
<td></td>
</tr>
<tr>
<td><strong>Solutions for individuals</strong></td>
<td></td>
</tr>
<tr>
<td>Child ID solutions</td>
<td></td>
</tr>
<tr>
<td>Counter-surveillance products</td>
<td></td>
</tr>
<tr>
<td>Face recognitions systems and technologies</td>
<td></td>
</tr>
<tr>
<td>GPS and mobile phone tracking</td>
<td></td>
</tr>
<tr>
<td>Home security systems</td>
<td></td>
</tr>
<tr>
<td>Home video surveillance (CCTV)</td>
<td></td>
</tr>
<tr>
<td>Intrusion systems</td>
<td></td>
</tr>
<tr>
<td>Medical alert systems</td>
<td></td>
</tr>
<tr>
<td>Monitoring services</td>
<td></td>
</tr>
<tr>
<td>Operatives based surveillance</td>
<td></td>
</tr>
<tr>
<td>Patient monitoring</td>
<td></td>
</tr>
<tr>
<td>Remote home monitoring</td>
<td></td>
</tr>
<tr>
<td>Security alarm and video surveillance</td>
<td></td>
</tr>
<tr>
<td>Street surveillance</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: IRISS typology of application areas and surveillance security products
The IRISS project provides a detailed overview of surveillance products, many of which were incorporated into the CRISP taxonomy to demonstrate how systems and products can be categorised based on demand and need. IRISS also provides an insight into how technologies can be categorised on the basis of functionality and operational effectiveness (e.g., detect, verify etc.) and how they may be grouped within specific application areas. Much like the Ecorys reports, IRISS brings to our attention the rapid expansion of “new” security technologies, many of which may pose specific issues with regard to certification and standardisation.

Public Perspective of Security and Privacy - PACT

The PACT project explores the existing relationships between human privacy and security and provides for a taxonomy of technologies applied in the surveillance and security sectors. Similarly to the methodology used in the SAPIENT project, technologies sharing common characteristics are ascribed to broad categories named as “families”. Within these “families”, which are 7 in total, up to 41 specific technology groups are identified and described and privacy considerations are provided on basis of available published privacy impact assessments. The following table reports the categorisation feeding in the taxonomy.

<table>
<thead>
<tr>
<th>Families</th>
<th>Technologies for area of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual surveillance</td>
<td>Video safety systems / CCTV &amp; storage, body scanner and augmented body imaging, Air surveillance, satellite / earth surveillance, personal imaging.</td>
</tr>
<tr>
<td>Communications surveillance</td>
<td>Mobile and landlines bugging, wiretapping and call logging; e-mail surveillance; VoIP.</td>
</tr>
<tr>
<td>Biometrics and identification</td>
<td>Criminal biometrics, technologies for multi-biometric systems, technologies for judicial and police cooperation systems, technologies for electronic passport and eGates, other authentication, access control and identity technologies.</td>
</tr>
</tbody>
</table>

[Table continues on the next page]

---

32 Ecorys Research and Consulting, op. cit., 2009 and 2011
35 The project also classifies technology families according to well-known types of privacy and privacy targets according to European Data Protection rules.
Sensors

Proximity smart cards, artificial nose and sniffers / explosive / weapon / drugs / detection technologies / sensor networks, vehicle tracking technologies, person tracking systems, behavioural analysis, smart home technologies, airport / port screening technologies, technologies for land and maritime border control systems.

Location determination

Transmitter location, Geo – tagging, RFID, Wi-Fi / Bluetooth similar technologies

Emergent and futuristic technologies

Neural wave analysis, DNA, intention / abnormal behavior detection technologies, vehicle systems technologies.

Table 6: The PACT categorization of security technology families and areas of use

For each of the seven families PACT identifies: 36

- Common features shared by the technologies in order to justify their grouping.
- Security and surveillance applications, solutions and/or systems where technologies in the family are mostly applied.
- Common privacy threats/risks and concerns and an explanation of range of privacy impacts, especially on groups under surveillance.

For each of the 41 technology groups covered by the families, PACT provides descriptions covering: 37

- How technology works, users and or parties promoting its development and degree of maturity.
- Who are the possible targets of the surveillance using the technology?
- Privacy threats and possible negative impacts considering applications/solutions/systems in which the technology is likely to be used.

The study finds out that the ever-increasing level of sophistication of surveillance technologies in areas of the professional, private and public lives of individuals opens up the scenario for privacy threats and concerns in particular the dilution of personal privacy and control by individuals (or even legal entities and public bodies) over personal data. 38

The project calls for a long-term vision and international framework of cooperation governing the application of technologies and applications for decision-makers and investors. It also notices that the security sector industry may in the future become more inclined to provide solutions in this direction but the support of the European Commission and national

---

36 García, et al., op. cit., 2012, p.15
37 Ibid., p.16.
38 Ibid., p. 217.
authorities is crucial to bring about progress towards systems embedding privacy and trustworthiness into technologies and systems.

Like the IRIISS project, PACT provides an extensive overview of security products and systems, which were used to populate the last level of the CRISP taxonomy. It also raises the issue of application of technology and how the context within which it is used may give rise to different impacts and issues. We used the notion of “context of use” in our building of the CRISP taxonomy, especially when categorizing the application areas and key security demands, each of which provides a specific context when underpinned by a security need.

Supporting fundamental rights, privacy and ethics and surveillance technologies - SAPIENT

The SAPIENT project provides for a review of the “state of the art” of surveillance studies, emerging “smart” surveillance technologies, and the adequacy of the existing legal framework in the surveillance sector.

The project aims at helping policy makers, technology developers and stakeholders to understand when “smart surveillance” should be used and how to apply criteria to assure that such systems respect the privacy of the citizens.

The project ranks surveillance technologies in wide-ranging categories named “families” and sets out a taxonomy of surveillance technologies by their different functions, in which factors such as “intrusiveness”, “comfort” and “speed” are examined. The tables below offer an overview of these two types of categorization.

<table>
<thead>
<tr>
<th>Technology “family”</th>
<th>Surveillance technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual surveillance</td>
<td>Photography (cameras, mobile phones, mobile video), CCTV, Unmanned aerial vehicles (UAVs), imaging scanners, and satellite.</td>
</tr>
<tr>
<td>Dataveillance</td>
<td>Data mining and profiling, Databases, data retention, Data integration: data warehouses, data marts and data federation; Cyber surveillance;</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Fingerprints; DNA matching; Facial recognition; Iris recognition systems; Behavioural biometrics.</td>
</tr>
<tr>
<td>Communication surveillance</td>
<td>Wiretapping (electronic eavesdropping); Telephone lines; Mobile phones; “Voice over Internet Protocol” (VoIP); Call logging; Monitoring text-based communication.</td>
</tr>
<tr>
<td>Sensors</td>
<td>Explosive and drug “sniffers”; Metal detectors; Audio sensors; Heat sensors; Multimodal</td>
</tr>
</tbody>
</table>

---

39 Ibid., p. 218.  
41 It is worthy of note that one of the project’s numerous findings was that some technologies are perceived as intrusive in some contexts and relatively “un-intrusive” in others. For example, the project reads that “the use of data mining to detect credit card fraud has been supported by individuals; however, there was an outcry over the proposed use of data mining techniques to monitor citizens’ behavior and build terrorist profiles” (Ibid., p.66)
behavioural sensing;

<table>
<thead>
<tr>
<th>Functions</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Biometric technology, RFID, CCTV.</td>
</tr>
<tr>
<td>Verify, authenticate and authorise</td>
<td>Biometric technology, RFID.</td>
</tr>
<tr>
<td>Detect/monitor</td>
<td>CCTV, unmanned aircraft systems (UASs), electronic monitoring</td>
</tr>
<tr>
<td></td>
<td>Device, data mining technologies; wiretapping;</td>
</tr>
<tr>
<td></td>
<td>monitoring of communications.</td>
</tr>
<tr>
<td>Locate/track</td>
<td>Satellite surveillance; mobile phone tracking; RFID; unmanned aircraft systems.</td>
</tr>
<tr>
<td>Collect information</td>
<td>Dataveillance technologies and applications, including data mining, data matching and data aggregation technologies; communication surveillance such as call logging, email monitoring and internet intercepts.</td>
</tr>
<tr>
<td>Link information (profiling)</td>
<td>Data mining; data matching; data aggregation.</td>
</tr>
</tbody>
</table>

Table 7: SAPIENT categorisation of surveillance technologies according to technology “family” 42

Table 8: SAPIENT categorisation of surveillance technologies according to surveillance function 43

In addition to focusing on “smart” surveillance technologies and how these are perceived within society, the SAPIENT project, provides an extensive and detailed overview of security technologies available, also concentrates on the function of a technology as means of categorizing it. Also, of relevance to the CRISP project, especially when it comes to certification and standardisation of products and systems is the project’s effort to provide guidance to stakeholders of when “smart surveillance” should be used and how to ensure that privacy of citizens is respected.

42 Ibid., p. 23 – 53.
43 Ibid., p. 53 – 61.
Stakeholders Platform for Supply Chain Mapping, Market Condition Analysis and Technologies Opportunities - STACCATO

The STACCATO project explores ways to develop a common Security Equipment Market (ESEM) in the EU. A multi-sector stakeholder platform composed of users, industry, SMEs, academia and think tanks has largely contributed to this aim\(^{44}\). The project focuses on the existing environment for security applications and notices that the European security market is currently very fragmented\(^{45}\). It therefore proposes methods for the development of a structured supply chain across Europe. The project also investigates on how to effectively integrate the potential of SMEs into the European security and technological industrial base and puts great emphasis on the role of standardisation to enhance interoperability in the security market for equipment and products.

STACCATO develops a taxonomy for security technology which builds upon a pre-existing taxonomy developed by SeNTRE (Security Network for Technological Research in Europe). The SeNTRE taxonomy has been taken into consideration in two ways:\(^{46}\)

1. Technology codification
2. Product/service codification

The five research levels of the SeNTRE taxonomy have been re-elaborated in STACCATO with the aim of developing a “user and supply” oriented taxonomy. The STACCATO taxonomy is structured along seven sections which are:

(I) Technologies and Components  
(II) Equipment and Sub Systems  
(IIIA) Systems-Services Functions  
(IIIB) Design-Manufacturing  
(IV) Integrated Platforms and Systems and Human Factors  
(VA) Missions Capabilities  
(VB) Policy and Support

The STACCATO taxonomy is a dual-use one for both the domains of security and defense.

---

\(^{45}\) Ibid., p. 4.  
\(^{46}\) Ibid., p.33.
STACCATO identifies nine “security missions/areas” - both demand-driven and supply-chain driven - which correspond to an equal number of technological areas. The missions/areas identified are the following:

- Critical infrastructure and network protection/cyber security
- CBRNE, including decontamination
- Crisis Management
- Wide area surveillance
- Movement of people
- Movement of Goods

And the 3 transversal missions:

- Interoperability
- Human Factors
- Standardization

---

47 Ibid., p. 34.
48 Ibid., p.42.
The project also presents the technology gaps/ bottlenecks common to most of the missions. These are:

- More user friendly systems.
- Gaps on communication systems (e.g., security of communications, cryptography, etc.)
- Interoperability of systems
- Mobility and transportability of systems
- Man-machine systems and their interfaces
- Cost of technology
- Data fusion
- Data mining
- Need for more system concept orientated solutions

An extensive and well-detailed classification of key technology issues (technology gaps/bottlenecks, emerging technologies and priority research areas) for each STACCATO mission is also provided.

As mentioned above, one of the prominent objectives pursued by STACCATO is that of enhancing the potential for the creation of a common security equipment market in Europe (ESEM). In this respect it is worth noting that the project offers a synthesis of key market issues that are to be overcome for each of the nine mission areas.

<table>
<thead>
<tr>
<th>Mission area</th>
<th>Key market issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical infrastructures and networks protection/</td>
<td>The Security market for critical infrastructure needs a lot of facilitation as normally the way from basic research to the final product is rather long, but the end-user cannot be kept within RTD-projects for the whole development-time. Apart from the fact that the stakeholders of critical infrastructure protection are highly sensible on the issue due to heterogeneous legal constraints, a diverse understanding of security missions, a diverse history and due to the fact, that this is not core business. By encouraging the building of peer-groups, the exchange of experience can be promoted, generating a pressure on technology.</td>
</tr>
<tr>
<td>cybersecurity</td>
<td></td>
</tr>
</tbody>
</table>

[Table continues on the next page]

---

49 Ibid, p.43.
50 The detailed representation of these issues can be found in the STACCATO Report Chapter, “Stakeholders Platform for Supply Chain Mapping, Market Condition Analysis and Technologies Opportunities”, p. 43 - 50.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CBRNE (including decontamination)</strong></td>
<td>There is currently a limited market for bio-detection products and the defense related market is minimal. The best way forward is to design bio-detection system for dual use (e.g., defense and diagnostic/food safety industries). Making the standards compatible for both could be important but it could be difficult because the threshold of detection may be different. Difficulty to find the good balance between security aspects and constraints for people (example of airports have been highlighted).</td>
</tr>
<tr>
<td><strong>Crisis management (focus on information and communication issues)</strong></td>
<td>From the market perspective, crisis management is abstract and not preventative, when compared to non-crisis fields.</td>
</tr>
</tbody>
</table>
| **Wide area surveillance**                                              | To develop a common market, standardisation, regulations and networks/agencies play a major role:  
  **Standardisation**: this seems to be a dominant point of attention.  
  Standardisation is a priority for the systems themselves and for interoperability among them.  
  **Regulations**: Wide area surveillance involves several entities. In such multi-stakeholder field, regulations will foster an environment in which technology development as well as operations and cooperation will be more effective. Networks/agencies: networks and agencies seem to form a key element in wide area surveillance. They represent many users involved in the topic and they can be in a 'neutral position' in order to facilitate the dialogue between the supply and demand sides. They, of course, could help in structuring funding programmes and foster cooperation among various stakeholders.  
  Attention is needed to long-term decision making as well as to the reinforcement of information sharing with other related actors (usually under data sharing legislation: MOU etc…). The situation can only be improved by putting the efforts of several stakeholders together.|
| **Movement of people**                                                  | Lack of a coordinated pan-European border control equipment policy.                                                                                                                                                                                                                                                                    |
| **Movement of goods**                                                   | For GNSS what is needed to speed implementation is governmental support through for example quick customs procedures/ e-Customs etc…                                                                                                                                                                                                                                                                 |

[Table continues on the next page]
Interoperability

The market within the EU for security equipment is fragmented. Fragmented on the demand side and on the supply side, with many industries ranging from big defense industries to SMEs of different types. The fragmentation leads to less security for the EU citizens for a given amount of allocated resources. The fragmentation could e.g. lead to
- Lack of interoperability
- An underinvestment in technical systems
- Inefficient acquisitions

Human factors

Human factors should be a market but it seems not to be realised yet. Any product or market where human decisions or actions occur is a prospective market for human factors.

Standardisation

Security market factors that are leading and/or stimulating the standardisation activities (taking into account the economic and technological impact) should be identified.51

Table 9: Key ESEM issues per mission52

As far as CRISP is concerned, the STACCATO research outcomes on the “standardization” mission are particularly relevant. In this respect, the project recognises that standards and related standardisation activities are of great importance to enhance the security market for equipment and products as they address a wide range of different purposes,53 such as:

- The rapid establishment of markets and acceleration of technologies take-up;
- The opening and/or enlarging of markets;
- The enhancement of competition by differentiating products and servicing;
- The enhancement of industrial efficiency by embodying best (or de facto) practices.

The project discovers that to support the emergence of a European Security Equipment Market, standards and standardisation activities should in priority address the following:

- Create an environment to elaborate a method for the analyses of the existing standards landscape related to security;
- Identify the security market factors that are leading and/or stimulating the standardisation activities (taking into account the economic and technological impact);
- Define a method for the prioritisation of the areas of actions in this sector. This could be undertaken within the ESRIF activities.

---

51 Ibid, p. 66.
52 STACCATO Project, op. cit., 2008.
According to the project, the European security market needs to be consolidated and developed at the EU level with regulation and funding mechanisms – conditioned upon the integration and development of a minimum level of standardisation and interoperability (for equipment, systems and services, between end users and between different countries)\textsuperscript{54}. This should be done by taking into account the specific features of security technologies and market and each security area/sector.

This consolidation should include emerging sectors as well as new developments such as the liberalisation of markets and the developments within the EU in sectors like energy, communications, and environment. However, the ESEM should especially include competitiveness as underlying principle, with adequate measures regarding the international competition: international cooperation and international norms taking into account European interests regarding the access to market in two levels: intra-European and access to third countries.

The review of EU-funded security projects revealed the multidimensionality of the security/security product field of study. There are myriad ways in which security areas, markets, products and systems can be categorised depending on the technology itself and the context within which it is used. Technologies can also be categorised and understood as responses to particular threats, or in relation to concerns, e.g., privacy, that they create within contemporary societies. Last but not least, security products can be classified in terms of their arrival in the market place, as in “traditional” and established, or “new” and unknown. All these factors are important to keep in mind as security products and systems are categorised and certified. CRISP focuses specifically on “security need” in its taxonomy and places security application areas as the starting point from which products and systems are then categorised.

For the purposes of categorising products and systems on the basis of need/function within the broad security sector, the projects provided inadequate starting points. These were most instances either too broad (e.g., “commercial solutions”) or intangible (e.g., “movement of people”) to provide a practical level 1, under which demands, and needs could be ascribed. The projects however did assist with clarifying the focus on function and areas/contexts of applications how these could be used to build a taxonomy of security products and systems. The review of these projects, as well as the review of commercial taxonomies (see next chapter) helped arrive at clearly defined application areas, from which the taxonomy could be started.

\textsuperscript{54} Ibid., p. 66.
3.4 Commercial Taxonomies

For the review of commercial taxonomies we used a database of security companies, which includes 350 companies, of varying sizes, with varying specialities and located all over the world. The database holds information on each company, for example location, status (global or national), size (staff numbers and turnover) where this information is publically available, and a short description of operational field. For the purposes of building the CRISP taxonomy we focused on reviewing twenty commercial websites of companies from the list which fulfilled the following criteria:

- The company should provide a broad selection of security products
- The company should provide for various different application areas

Furthermore, we also ensured that there was a mix between companies that provide products that can be classified as “new” and “traditional.”\(^{55}\) We also ensured that the companies were located in different countries in Europe and internationally for the purpose of making the CRISP taxonomy applicable for the security industry across Europe.\(^{56}\) The rationale for the criteria was to view ways in which security needs were catered for by the security industry and in what ways these are categorised.

The commercial taxonomies are customer-focused and aim firstly to situate a potential customer within a specific operational field, in order to assist with the realisation of security needs. What is interesting is that, irrespective of field, the needs overlap and consequently the security equipment and systems. Most of the companies also sell security services, ranging from initial risk assessment to consulting on complex product integration systems. Some companies furthermore, provide more wide ranging services on logistics and stock management, which are then further integrated with security (e.g., integrated stock intelligence and loss prevention systems).

Honeywell\(^{57}\)

Honeywell is a multinational conglomerate company whose security services are but one of their commercial endeavour. Consequently the company’s security products and systems are often sold of more extensive commercial management systems whereby security and logistics for example are integrated to suit a specific customer need.

Honeywell identifies sixteen different market segments to which the company tailors their products, systems and services. Once the needs and products available for each market segment are reviewed, extensive overlaps occur.

---

\(^{55}\) Ecorys Research and Consulting, op. cit., 2009 and 2011
\(^{56}\) The sample list of security companies can be found in Appendix A
<table>
<thead>
<tr>
<th>Markets &amp; Solutions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Airport</td>
<td>House of worship</td>
</tr>
<tr>
<td>Banking</td>
<td>Industrial</td>
</tr>
<tr>
<td>Campus/University</td>
<td>Life Sciences</td>
</tr>
<tr>
<td>Commercial office</td>
<td>Military</td>
</tr>
<tr>
<td>Finance</td>
<td>Residential</td>
</tr>
<tr>
<td>Gaming</td>
<td>Retail</td>
</tr>
<tr>
<td>Government</td>
<td>Seaport</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Utilities</td>
</tr>
</tbody>
</table>

Table 10: Honeywell Markets & Solutions

To each of the categorised markets, Honeywell presents the following needs for which they tailor and provide security solutions. These needs are commercially presented, and many overlap between markets. Other needs are presented as combinations of systems and equipment for complex security tasks. The needs in the table below are therefore a further synthesis and simplification of Honeywell’s needs categories. The needs are also categorised according to security focus, into four categories: protection of assets, compliance with standards and legislation, protection of people and places. We have made a distinction here between assets and places on the basis of scale, e.g., buildings are here categorised as places, whilst assets are a category under which smaller items fall.
<table>
<thead>
<tr>
<th>Assets</th>
<th>Compliance</th>
<th>People</th>
<th>Places</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investment protection</td>
<td>Government Compliance</td>
<td>Biometric verification</td>
<td>Perimeter intrusion detection</td>
</tr>
<tr>
<td>Video surveillance</td>
<td>HSPD-12 Compliance</td>
<td>Situational awareness/analysis</td>
<td>Situational awareness/analysis</td>
</tr>
<tr>
<td>ATM Security</td>
<td>JACO/HIPAA compliance</td>
<td>Employee/visitor safety</td>
<td>Building safety</td>
</tr>
<tr>
<td>Temperature/flooding/monitoring</td>
<td>FDA regulations compliance</td>
<td>Video surveillance</td>
<td>Video surveillance</td>
</tr>
<tr>
<td>Asset management, protection and tracking</td>
<td>International seaport legislation compliance</td>
<td>Identification</td>
<td>Opening/closing</td>
</tr>
<tr>
<td>Alarm communications</td>
<td>Transportation Work Identification Credential (TWIC)</td>
<td>Alarm communications</td>
<td>Building security</td>
</tr>
<tr>
<td>Point of transaction</td>
<td>Preventing downtime</td>
<td>24/7 building monitoring</td>
<td>24/7 building monitoring</td>
</tr>
<tr>
<td>Situational awareness/analysis</td>
<td></td>
<td>Food and beverage</td>
<td>Alarm communications</td>
</tr>
<tr>
<td>Shrinkage/loss prevention</td>
<td></td>
<td>Prevention of violence</td>
<td>Situational analysis</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>Sullivan awareness/analysis</td>
<td>Preventing downtime</td>
<td></td>
</tr>
<tr>
<td>Theft and burglary protection</td>
<td></td>
<td>Life safety</td>
<td>First response</td>
</tr>
<tr>
<td>First response</td>
<td></td>
<td>First response</td>
<td></td>
</tr>
</tbody>
</table>

Table 11: Honeywell categorisation for security needs

As Honeywell is a large scale supplier of security products and systems, its taxonomy provides a useful system of organising a great variety of equipment based on user group, security demands and needs. It provides clear categories of security markets, which provided a starting point for thinking about how CRISP application areas might be realised.
BOSCH

The BOSCH Group is another global supplier in the areas of automotive and industrial technology, consumer goods and building technology. BOSCH Security provides a broad range of security products including video surveillance systems with IP-solutions, access control systems, intrusion detection systems, fire detection and evacuation systems, security management systems and public address systems. BOSCH provides solutions for the following security areas:

<table>
<thead>
<tr>
<th>Security Areas</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Airport</td>
<td>Railway</td>
<td>Stadium and convention</td>
<td>Energy and utility</td>
<td>Other industry solutions</td>
<td></td>
</tr>
</tbody>
</table>

Table 12: BOSCH categorisation of security areas

BOSCH categorises security systems and products according to the six categories below, all of which were used for informing the building of the CRISP taxonomy. Access control featured in many of the corporate taxonomies either as a system or product like in the BOSCH taxonomy, or as a security demand, under which products and systems were placed like in the Tyco taxonomy presented below.

<table>
<thead>
<tr>
<th>Security systems and products</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Surveillance Systems</td>
<td>Access Control Systems</td>
<td>Intrusion alarm systems</td>
<td>Public address and voice evacuation systems</td>
<td>Fire alarm systems</td>
<td>Building management systems</td>
</tr>
<tr>
<td>CCTV cameras</td>
<td>Readers Biometric solutions Video surveillance Alarm systems</td>
<td>Intrusion detectors CCTV cameras Intelligent video analysis Alarm systems</td>
<td>Digital public address and emergency sound system</td>
<td>Modular fire panels Detectors Sprinklers Ventilation system</td>
<td>Integration system for: Alarm systems Evacuation system Access control CCTV +other automation systems</td>
</tr>
</tbody>
</table>

Table 13: BOSCH categorisation of security systems and products

Tyco

---

58 BOSCH Group, “BOSCH Security (UK page)”, no date. : http://www.boschsecurity.com
Much like Honeywell and BOSCH Group, Tyco is a market leader in security products and especially fire protection, which proved useful for the building of the taxonomy. Tyco is a supplier for the oil and gas industry, an application area which was merged under the heading Critical infrastructure for the CRISP taxonomy. Tyco presents nine “markets” and nine “solutions” groups under which security needs and products are further categorised:

<table>
<thead>
<tr>
<th>Markets</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; finance</td>
<td>Fire detection</td>
</tr>
<tr>
<td>Commercial and industrial</td>
<td>Fire suppression</td>
</tr>
<tr>
<td>Government</td>
<td>Personal protective equipment</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Transportation</td>
<td>Intrusion detection</td>
</tr>
</tbody>
</table>

**Table 14: Tyco categorisation of security markets**

<table>
<thead>
<tr>
<th>Markets</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; finance</td>
<td>Fire detection</td>
</tr>
<tr>
<td>Commercial and industrial</td>
<td>Fire suppression</td>
</tr>
<tr>
<td>Government</td>
<td>Personal protective equipment</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Transportation</td>
<td>Intrusion detection</td>
</tr>
</tbody>
</table>

The commercial taxonomies proved very useful in building the CRISP taxonomy as they provide a clear way of grouping users, demands and needs which is helpful for a market as fragmented as security provision. As is evident by the three commercial taxonomies presented here, they have strong similarities in that they are presented under the headings of perceived security markets or areas. We have selected the above three taxonomies on the basis of scale, as they present very well firstly how a fragmented user base, with varying and complex needs can be categorised, and secondly how a broad range of products can be organised according to function/need.

Building on this, we decided to make the application area the starting point of the CRISP taxonomy, which, however, features amended areas as some markets are grouped together due to similarities in demands presented by security companies. The second level of the CRISP taxonomy draws on the demands that feature most prominently in the commercial taxonomies, Access control being a security demand that featured in different ways (both cyber and physical) on all the company websites. A full list of company websites reviewed can be found in Appendix A.

<table>
<thead>
<tr>
<th>Glass break detection</th>
<th>Video surveillance cameras</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panic buttons</td>
<td>IP/networked video</td>
</tr>
<tr>
<td>Intercom &amp; door entry systems</td>
<td>Video alarm verification</td>
</tr>
<tr>
<td></td>
<td>Video analytics</td>
</tr>
<tr>
<td></td>
<td>Video storage systems</td>
</tr>
<tr>
<td></td>
<td>Integrated video solutions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Video surveillance integration</th>
<th>Access control integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network IP video integration</td>
<td>Alarm monitoring integration</td>
</tr>
<tr>
<td>Fire detection integration</td>
<td>Fire suppression integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access control readers &amp; cards</th>
<th>Visitor management systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity management systems</td>
<td>Door entry systems</td>
</tr>
<tr>
<td>Smart card and biometrics</td>
<td></td>
</tr>
<tr>
<td>Integrated access control systems</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retail solutions</th>
<th>Safety and security solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Loss prevention</td>
</tr>
<tr>
<td></td>
<td>Inventory intelligence</td>
</tr>
<tr>
<td></td>
<td>Store traffic intelligence</td>
</tr>
</tbody>
</table>

*Table 15: Tyco categorisation of security solutions, products and systems*
4 CRISP NEEDS-BASED TAXONOMY OF SECURITY PRODUCTS AND SYSTEMS

The five EU security policy priorities are the starting point of the taxonomy as an attempt was made to identify application areas where security measures contributing to the security involved in the priorities areas takes place, in order to start categorising security equipment and systems in use at each application area. The CRISP taxonomy takes a first step towards defragmentation, by focusing on broad application areas, and categorising equipment and systems based on demands and needs identified within these areas. This should allow for a practical approach towards standardisations and certification of security products and systems.

4.1 SECURITY APPLICATION AREAS (LEVEL 1)

4.1.1 Border management

Border management is one of the EU’s security policy priority areas, which is also recognised within commercial taxonomies as a separate security market with specific and high-end needs. While the EU’s overall aim is to ensure that EU citizens, non-European residents and visitors to the EU are allowed to freely and safely travel within the its borders, border management is also about strengthening external borders to ensure security and safety from outside threats. Border management requires the cooperation and collaborating of Member States and enhanced and large scale information sharing on visas, traveller data, suspected criminals/terrorist data, missing persons and stolen or lost property. Travel documents and the verification of these and their holders are also important for achieving the EU’s security aims, hence the documents have been equipped with advanced security features and biometrics, to establish a reliable link between the documents and their holder.

The CRISP taxonomy covers border management as firstly a process (i.e., verification and authorisation of persons and goods, including different actions, products and systems. Secondly, the taxonomy covers security functions within specific locations (e.g., border and immigration control areas) and the security of these facilities, their employees and staff.

4.1.2 Critical Infrastructure

The security application area of Critical infrastructure (CI) includes structures which are vital to the day-to-day running of contemporary society such as power plants, communication systems, water, oil and gas distribution systems. Damage to or loss of CI functions have the potential to cause a range of disruptions, resulting in contained and small scale effects, or potentially cross-border major disruptions to societal and economic functions. Due to the importance of CI, it is seen as a primary target for terrorism and criminal activity and infrastructure protection is a significant feature of the EC’s security policies.

The EU defines critical infrastructure is 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” 

Critical infrastructure protection as the objective of “ensuring that services vital to the society continue to function” is highly relevant to the fifth objective of Europe’s Internal Security Strategy, “increase Europe's resilience to crisis and disasters”. The Strategy also highlights that the threats to critical infrastructure calls for improvements to long-standing crisis and disaster management practices. Hence, there is some overlap between CI and the application area of Emergency preparedness centres/Crisis management.

4.1.3 Households and individuals

The application area of household security covers private residences of persons residing within the Member States and the security needs of individuals. The EU recognises that security challenges are both growing in scale and sophistication, and that European citizens want more in terms of security. Household and individual security products and systems, play an important role in the fight against organised crime, as theft from private households (e.g., assets and personal information for the purposes of committing fraud) fuel growth and sustenance of organised crime activities.

In reviewing in the commercial taxonomies, we found that households and individuals have somewhat simpler security demands, as these are mostly aimed at single, small scale, location and a low number of persons is involved at each location. Security products and systems are mainly aimed at building security, to include theft and burglary protection as well as protecting individuals (e.g., personal alarm buttons) living at each household. In recent years, the advancement of smartphones and networking capabilities now offers households more sophisticated surveillance capabilities.

4.1.4 Public and semi-public venues

The CRISP application area of public and semi-public venues involves a synthesis of commercially identified sectors, whose needs are similar in that they pertain to protection of the public which frequent said location, as well as closed off areas intended for employees and other authorised persons. This application area covers a range of physical locations, which include government buildings, hospitals, houses of worship, sports and entertainment...

---


venues and educational facilities (e.g., schools and university campuses) among others. This application area overlaps to a significant degree with the area of Transport due to the public nature of the location. However, we separate the two areas on the basis of the specific security needs that are present and the functions that are performed at locations within the Transport category due to high levels of human and goods traffic through these application areas. The venues within this area vary greatly in their security measures, with government buildings having high levels of security whilst entertainment venues and houses of worship may have a lower levels of security depending on their role and the context in which they operate.

4.1.5 Industrial and Retail

The application area of industrial and retail security incorporates similar security demands and needs as public and semi-public venues, but its key focus is on security of logistics, commercial activities, loss prevention, shrinkage and safety of visitors and staff. Again, the physical locations within this category vary greatly in size, location and endeavour, from a single CCTV camera in a small retail location to vast shopping centres and industrial complexes, which require access control for large number of persons, vast networks of logistics and complex stock management systems.

4.1.6 Emergency Preparedness Centres/Crisis Management

As outlined above, the fifth EU internal security objective is to enhance Europe’s resilience to crises and disasters, which relies on cooperation and collaboration between Member States and joint European systems to prevent, prepare, communicate and respond to disasters and crises arising from natural or man-made causes. EU has numerous response systems in place to coordinate efforts within and across Member States.

The Emergency Response Coordination Centre (ERCC) was set up in 2013 to collect and analyse real-time information on disasters, monitors hazards, prepare plans for the deployment of experts, teams and equipment, work with Member States to map available assets and coordinate the EU’s disaster response efforts. The ERCC is staffed and equipped with enhanced monitoring and analytical capacity, technologies for satellite images, early warning systems and state of the art crisis management tools. The ERCC acts as a one-stop shop for European emergency response by monitoring and assessing disasters, and coordinating response. Both mechanisms rely on information systems around the world, in the form of monitoring and civil protection systems. Monitoring systems include e.g.,

---

weather, space, volcano, flooding, earthquakes and critical infrastructure (e.g., nuclear power plants).

This application area covers security systems and products used for the purpose of emergency preparedness, i.e., situation awareness and crisis management in European and local member state run centres. The key functions identified within this CRISP application area are focused on disaster detection, data gathering and sharing, as well as communication around a network of centres around Europe.

### 4.1.7 Transport

The CRISP Transport application area combines different modes of transport and is derived from a review of EU transport policy whose foundation is the recognition of transport as fundamental to the EU’s economy and society.\(^{69}\) Freedom of movement is seen as vital for the Europe’s internal market, for citizen’s quality of life, economic growth and job creation. The EC’s transport policy, and consequently the CRISP application area, covers air, road, rail, maritime and inland waterways modes of transport.\(^{70}\)

Transport security remains a key focus for the EU, and the EU transport strategy\(^{71}\) recognises that the EU’s comprehensive approach, consisting of policy, legislation and monitoring of air and maritime transport security, needs further consolidation and more extensive cooperation with major international partners to increase effectiveness. The EU’s key transport objective is to “create a genuine Single European Transport Area by eliminating all residual barriers between modes and national systems, easing the process of integration and facilitating the emergence of multinational and multimodal operators”.\(^{72}\) An integral part of this strategy is a higher degree of convergence and standard enforcement (for safety, security, environmental rules and minimum service) across member states, which is essential for avoiding tensions and distortions. Enhanced and uninterrupted information flow between member states and systems is also deemed necessary to enhance transport safety and security.

The key security concerns identified for transport security are passenger and staff security, cargo security, and infrastructure security, and main physical locations, where security tasks are performed are airports, harbours, train stations, other transport hubs, as well as rail, road and waterway networks. These, in addition to needs and demands identified in the commercial sector are used for organising and building the CRISP Taxonomy for Transport. We note that CRISP transport application area overlaps to varying degrees with the other application areas in security product and system demands and needs; this is especially evident with border management and public and semi-public venues.

---


\(^{71}\) European Commission, White paper EC Roadmap to a Single European Transport Area, op. cit., 2011, p. 11..

\(^{72}\) Ibid., p.3.
4.2 **SECURITY DEMANDS (LEVEL 2)**

The security demands listed here are based on a review and synthesis of security product taxonomies from security company websites. The categories are not mutually exclusive and present considerable overlap due to how holistic security systems design can be, as it aims to meet a multiple security needs. All the categories cover a broad range of products and systems, as well as different scales of operation, e.g., small scale household need for surveillance of one location to extensive security systems used to ensure multi-location industrial security for systems, cargo, persons and vehicles. These categories were selected with the aim of covering a broad range of products and systems and to present a clear taxonomy based on security demands and needs.

4.2.1 **Access control**

Access control is a consistent security demand, presented on all of the security company websites. Access control covers a broad category of products and systems, which differ in scale from a key lock on one door, to complex systems which manage the access of thousands of employees to a company intranet. Access control can be automated, e.g., surveillance equipment detecting a presence of a moving objects and then requests verification before authorising/denying entry, or is supplied by manned entry points. Access control here refers to limiting access to a site to identified and verified persons or vehicles only, which can access certain physical or network spaces by password, key card, or biometrics.

4.2.2 **Asset/freight/cargo security**

This demand category covers a broad range of security needs, products and systems. It refers to the practice of guarding against theft and or manipulation of assets by using a system of labelling and tracking. This category may also include sensors, surveillance and stock management/logistic systems for larger operations. In order to ensure asset/freight/cargo security, other demands need to be met. These may include, but are not limited to access control, cybersecurity and point of transaction security. Asset/freight/cargo security systems differ in scale, e.g., from an individual household labelling items of value to extensive freight and cargo security management systems which track movement across the globe.

4.2.3 **Cyber security**

The EU recognises the Internet and digital technologies as the “backbone of our society and economy’ and ‘key enablers of prosperity and freedom.”73 As such, protecting businesses and citizens online is one of the objectives of the EU Internal Security Strategy, as mentioned above. This category covers a broad range of products, systems and technologies aimed at protecting networks, data and digital information from criminals, hackers, terrorist organisations and others who seek to capitalise from systems infiltration and data theft.

---

Cybersecurity measures vary greatly in scale, from a firewall on a single home computer to vast systems of firewalls, data encryption software and complex access systems. Products that fall under this category are to a large extent software based, e.g., virus scanning, firewalls, access control software, attack detection, data encryption etc.

4.2.4 Employee/visitor safety

Employee/visitor safety is a broad security demand, which covers a variety of technologies, products and systems. It broadly refers to ensuring the safety of all persons within a given location by using systems of surveillance, access control, perimeter security and situation awareness. This category covers broad range of scale, from one CCTV camera to networked systems covering extensive areas or multiple locations. This category overlaps with perimeter/area/building security to a great extent, but the needs and products which fall under this one are person focused, whilst the products in the latter are more building, perimeter and vehicle focused.

4.2.5 Loss prevention/shrinkage

This security demand features strongly within the industrial and retail application areas, where security focus is on loss prevention from theft or fraud. Depending on scale, loss prevention can range from a single CCTV camera within a small retail space, to complex systems of security surveillance, access control and perimeter security solutions. Freight and cargo labelling and tracking systems also fall under this category along with logistics and stock management systems which allow for close monitoring of assets and commercial products.

4.2.6 Perimeter/area/building security

This demand category is centred on security products and systems which monitor and ensure secure physical locations, be they buildings or geographical areas. This is a broad demand which utilises surveillance, sensor, detection and communication products and systems. As with the other demand categories, different scales of perimeter/area/building safety exist ranging from a CCTV system for a household to extensive perimeter intrusion and building security systems at airport or at power plants. This category overlaps significantly with the areas of access control and employee/visitor safety as the former is an integral part of building security and the latter may apply to the same application area.

4.2.7 Point of transaction

Point of transaction refers to monitoring an encounter where a transaction takes place. This can include a monetary transaction within a retail space, where surveillance cameras record all pay points, border management where scanning of travel documents takes place, delivery of goods where a signature is required and monetary transfers between financial institutions. Needs for identification, verification and authorisation feature strongly within this demand category.
4.2.8 Situation awareness

The CRISP D1.1 Glossary of Security Products and Systems\textsuperscript{74} defines situation awareness in its simplest terms as creating a “picture” of a given situation. Situation awareness is here used to cover large scale monitoring systems, information flow, communication networks which are involved in early warning and crisis centres such as the EU Emergency Response Coordination Centre (ERCC) and equivalent centres in member states. These systems may include flood, weather, volcano and earthquake monitoring, as well as monitoring for infectious disease or terrorist attacks. The system relies on extensive sensor, monitoring and communication systems for rapid and appropriate response.

4.3 Security Needs/Functions (Level 3)

Eleven out of the twelve security needs used for the CRISP taxonomy are derived from the identified and defined security functions from the CRISP Deliverable D1.1 Glossary of Security Products and Systems, and presented here in summary. The need/function “communicate” was added to the taxonomy to help categorise equipment such as alarm systems, which monitor and detect, but also communicate by way of signals, visuals or sounds.

<table>
<thead>
<tr>
<th>Security functions/needs</th>
<th>Short Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess</td>
<td>Assessing a situation is a widespread function to which systems, products and services across the application areas contribute. A key part of assessment is to make a judgement about someone/something. Assessing can encompass risk or threat assessments, but also targeted assessments of behaviour through specific profiling methods. The assessment process requires information, which has been gathered, merged and displayed (see different functions) in a previous phase.</td>
</tr>
<tr>
<td>Authorise</td>
<td>Authorising can be defined as serving the purpose of lending rights and status to individuals or groups. Being authorised or not determines whether access is granted or not, and whether certain information is shared or not. Authorising revolves around the granting, restricting and managing of rights.</td>
</tr>
<tr>
<td>Communicate</td>
<td>The communication function relates to the other functions as a step change in each security process either initiated by communication e.g. motion sensor switches on surveillance camera, or communicating breech through alarm systems. Merriam-Webster Online Dictionary\textsuperscript{75} has three definitions for the verb communicate which are useful here: “to convey</td>
</tr>
</tbody>
</table>

\textsuperscript{74} Fritz, et al., op. cit., 2014.
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>The control function within security is very broad and can be found in a large number of different areas and also relates to other functions, like “identify” “verify” and “authorise”. Control can mean to supervise the running of, limiting the level, intensity or numbers of, or regulating a specific security process.</td>
</tr>
<tr>
<td>Create situational awareness</td>
<td>Situational awareness “relates to cognitive processes as well as outcomes. It centres on and implies a decision-making instance relying on information gathered from a vast array of sources. Such information, in turn, relates to aspects of the world to create a ‘picture’ of a given situation.”</td>
</tr>
<tr>
<td>Detain</td>
<td>Detention is a security function which is applied in the general framework of criminal law but also in other fields such as, for instance forms part of the main priorities of the EU internal security strategy: border management and prevention of terrorism.</td>
</tr>
<tr>
<td>Identify</td>
<td>“Identification almost always relies upon the presence of a database to perform one-to-many matching, especially if this one-to-many matching is digitised and speed is a priority.” Three forms of security identification can be further defined: 1) identifying an object/person against a database; 2) identifying a substance, using chemical analysis; or 3) identifying an anomaly, by spotting an object/person in an inadequate space/context. In the specific context of crisis management, the function identify furthermore covers the type of damage/harm resulting from a threat, e.g. types of injuries, pathogens.</td>
</tr>
<tr>
<td>Information collection, storage and management to produce intelligence</td>
<td>These functions are a crucial part of contemporary security practices as without data a lot of the other functions would be limited to a large extent. Data collection can be found within most of the application areas, the most high profile being Border Management and Transport where information gathering, storage and sharing is deemed a priority in Europe’s security (see. EU Internal Security Strategy)</td>
</tr>
</tbody>
</table>

---

76 Ibid., p. 29.
78 Bellanova, et. al., op. cit., 2012, p.53
### Locate
To discover the exact place of a person or entity. In security products and systems the locating function often combined with the functions of detection as well as tracking. A more specific, security related definition of “to locate” can be found in the PACT project,\(^{79}\) where the function is already closely linked to the location determination technology itself, which “enable[s] the collection of geospatial data regarding a specific individual, object or area.”\(^{80}\)

### Prevent/protect
Prevention, like many of the other security functions means many different things to many different people and is highly dependent on the context and the goal. Concerning the EU’s internal security strategy crime prevention is a priority in the following domains: the prevention of serious and organised crime, the prevention of terrorism and radicalisation and the prevention of cybercrime.\(^{81}\)

### Track
Tracking could be framed as to monitoring a physical location of person or entity, which can be expanded to include tracking. Tracking can also be used for determining “who was in a geographic area [...] at a particular time,”\(^{82}\) linking this security function closely to surveillance tasks.

### Verify
The verifying function is closely related to the identifying function. SAPIENT provides a good differentiation between the verification and the identification function related to persons since “identification involves one-to-many matching,” while “verification (…) involve[s] the database system retrieving the features of a single person and performing a one-to-one comparison.”\(^{83}\)

| Locate | To discover the exact place of a person or entity. In security products and systems the locating function often combined with the functions of detection as well as tracking. A more specific, security related definition of “to locate” can be found in the PACT project,\(^{79}\) where the function is already closely linked to the location determination technology itself, which “enable[s] the collection of geospatial data regarding a specific individual, object or area.”\(^{80}\) |
| Prevent/protect | Prevention, like many of the other security functions means many different things to many different people and is highly dependent on the context and the goal. Concerning the EU’s internal security strategy crime prevention is a priority in the following domains: the prevention of serious and organised crime, the prevention of terrorism and radicalisation and the prevention of cybercrime.\(^{81}\) |
| Track | Tracking could be framed as to monitoring a physical location of person or entity, which can be expanded to include tracking. Tracking can also be used for determining “who was in a geographic area [...] at a particular time,”\(^{82}\) linking this security function closely to surveillance tasks. |
| Verify | The verifying function is closely related to the identifying function. SAPIENT provides a good differentiation between the verification and the identification function related to persons since “identification involves one-to-many matching,” while “verification (…) involve[s] the database system retrieving the features of a single person and performing a one-to-one comparison.”\(^{83}\) |

Table 16: CRISP security functions/needs

---

80 Ibid.
82 García, et al., op. cit., 2012, p. 25.
83 Bellanova, et. al., op. cit., 2012, p.55
5 CRISP TAXONOMIES OF SECURITY PRODUCTS AND SYSTEMS

In this chapter we present the CRISP taxonomies for security products and systems for each of the seven application areas, using the defined security demands and needs presented in sub-chapters 4.2 and 4.3 to further categorise equipment. For a better readability, most of the taxonomies have been divided on two pages.

5.1 BORDER MANAGEMENT TAXONOMY
5.2 **Critical Infrastructure Taxonomy**

```
Critical Infrastructure

Access control
- Detect: Video analytics
  - Video surveillance cameras/systems
- Identify: Sensors
  - Integrated video access control, intrusion and alarm systems
  - Database of persons/vehicle/vehicles
- Verify: Card reader
  - Biometric face/fingerprint/hand/iris, reader
- Authorise: Employee visitor management system
  - Visitor log/badge systems

Asset security
- Track: GPS/IOS location systems
- Identity: Video surveillance cameras/systems
- Prevent/protect: Wireless asset protection
  - RFID
- Malware detection
  - Intrusion/cyber attack detection
  - E-Document scanning
  - Virus scanning

Cybersecurity
- Information collection, storage and management
  - Encryption software
  - Data storage
  - Protected data transfer
  - Access control
    - Digital signature
    - Authentication/User administration
    - Firewalls and secure VPN
    - Domain/IP blocking
    - Patch management
    - Automated disconnect
  - CT scanner personnel
    - Liquid explosive detection
  - Detect: Rule based detection software
    - Millimetre wave body scanning
    - CBRN detection
  - Identify: Video surveillance cameras/systems
    - Biometric face/fingerprint/hand/iris, reader
    - Card reader
  - Database of persons/vehicle/vehicles
  - Employee visitor management system
  - Verify: Ultraviolet document viewers
    - Checkpoint forgery detection systems
    - Infrared document inspection
  - Authorise: Person barriers/gates
```
5.3 **Emergency Preparedness Centres/Crisis Management Taxonomy**
5.4 **HOUSEHOLD AND INDIVIDUALS TAXONOMY**
5.5 **Industrial and Retail Taxonomy**
D1.2: Taxonomy of Security Products, Systems and Services

CRISP project
5.6 Public and Semi-Public Venues Taxonomy

Public and semi-public spaces

Cybersecurity

- Access control
  - Digital signature
  - Authentication/authorization administration
  - Automated discovery
  - Patch management
  - Domain/VPN blocking
  - Firewalls and secure VPN
- Detect
  - CT scanner, pression/traffic
  - Liquid explosive detection
  - Role-based detection software
  - Millimeter wave body scanning
- Identity
  - Biometric face/fingerprint/handprint reader
  - Card/RFID reader
- Verify
  - Video surveillance cameras/systems
  - Database of persons/vehicles
- Authorize
  - Person barriers/turnstiles

Access control

- Detect
  - Video analytics
- Identity
  - Sensors
  - Integrated video, access control, intrusion, and alarm systems
  - Database of persons/vehicles
- Verify
  - Card/RFID reader
- Authorize
  - Visitor badge systems

Asset security

- Detect
  - Microwave detection
  - e-Document scanning
  - Intrusion/cyber attack detection
- Identity
  - Video surveillance cameras/systems
- Verify
  - RFID
- Authorize
  - Visitor badge systems

Employee/visitor security

- Detect
  - Surveillance cameras/systems
- Identity
  - Sensors
- Verify
  - Card/RFID reader
- Authorize
  - Visitor badge systems

Public and semi-public venues

Encryption software
- Data storage
- Protected data transfer

CRISP project

Page 58 of 106
5.7 Transport Taxonomy
1.2: Taxonomy of Security Products, Systems and Services

CRISP project

Transport

Perimeter/area/building security

Detect
- Sensors
- Glass break detector
- Fire/smoke detector
- CT scanner item
- Metal detectors
- Video analytics
- Rule-based detection software
- Motion detectors
- CBIR detection
- Video surveillance camera/system
- Video smart search capabilities

Identify
- General surveillance systems
- Radar

Verify
- Ultraviolet document viewers
- Document authentication
- Forged detection systems
- Infrared document inspection
- Fingerprint/iris reader
- Card/fob reader
- Database of persons/fire/route vehicles
- Keyed access

Authorise
- Visitor log/badge systems
- Employee/visitor management system
- Alarm systems
- Two-way communication systems
- Public address systems
- Information displays
- Emergency notifications (phone, email, SMS)
- Radio systems
- Secure entrance solutions (turnstiles, barriers, security lanes)
- Anti-tampering/anti-counterfeiting technology
- Flexible vehicle protection
- Vehicle security systems and barriers
- Perimeter fencing

Prevent/protect
- Blast protection
- Perimeter intrusion detection systems
- Blast resistant doors
- Fire doors
- Personnel/vehicle barriers
- Emergency light systems

Point of transaction

Detect
- CT scanner item
- Video analytics
- Video smart search

Identify
- Video surveillance camera/systems
- Signature/RF cryptos

Verify
- Ultraviolet document viewers
- Document authentication
- Forged detection systems
- Infrared document inspection
- Fingerprint/iris reader
- Bimodal face/fingerprint/iris/fret

Authorise
- Visitor log/badge systems
- Employee/visitor management system
- Alarm systems
- Two-way communication systems
- Public address systems
- Information displays
- Emergency notifications (phone, email, SMS)
- Radio systems
- Secure entrance solutions (turnstiles, barriers, security lanes)
- Anti-tampering/anti-counterfeiting technology
- Flexible vehicle protection
- Vehicle security systems and barriers
- Perimeter fencing

Prevent/protect
- Blast protection
- Perimeter intrusion detection systems
- Blast resistant doors
- Fire doors
- Personnel/vehicle barriers
- Emergency light systems
5.8 CONCLUSION

The purpose of this chapter was to produce a useful and needs-based taxonomy for security products and systems on the market in order to categorise them. Particular stress was placed on classification through application areas, seven of which were identified through a review of European policy and research project literature, as well as commercial websites of security product and system vendors. It is important that application areas provide a starting point for the taxonomy as any evaluation and certification scheme of products and systems will need to work across security sectors. The CRISP taxonomy contributes to this task in providing a clear way of categorising products according to application area > demand > need/function > security product/system.

As we explain throughout there is considerable overlap between application areas (e.g., border management and transport) demands (e.g., access control and area/building/perimeter security), and needs/functions as many products cater to more than demand or need, and products can be integrated to build a multi-functional security system. The branches are not mutually exclusive and the taxonomy, as a living document, can be amended to fit new application areas, demands, needs and products.
6 SECURITY SERVICES: CRITERIA FOR CLASSIFICATION

6.1 TOWARDS A WORKING DEFINITION OF SERVICES

ISO 9000 refers to services as a result of an activity or an interaction between suppliers and demanders. Also, the term refers to something intangible, involving provision of e.g. transportation or advice/consultancy or the delivery of security functions as set out in D1.1. ISO 9000 also refers to services coupled with products, such as repair services or delivery services. This adds to the general notion of a service as an intangible good or commodity.

With a view to developing a taxonomy of security-relevant services, several classification approaches seem promising. Among potential criteria that could be drawn upon, training most likely ranks highest. The amount of training hours the service provider requires in order to be entitled to work in a given profession not only allows for clues whether the respective security service is located more at a strategic level of security governance (such as a certified business continuity manager) or at the operational level (such as a security guard or cash in transit service providers). However, the equations little training = operational level and high training intensity = strategic level, cannot be generalised, as for example a network defence information security specialist can be as closely involved in detecting a threat or vulnerability in a perimeter as a security guard on patrol.

Fragmentation is probably the main challenge the EU security market faces. This is true not only for products and systems, but also for service provision. EU law lists four main characteristics of services: activities of an industrial character, activities of a commercial character, activities of craftsmen, activities of the professions. 84 While the freedom to provide services is one of the central pillars of EU-law, 85 the EU’s internal market in services in general is far from being accomplished. 86 Even with the adoption of the EU Service Directive, 87 no approach to tackling fragmentation in providing security services throughout the EU came in sight, as Art. 2(2)(k) of the Services Directive explicitly excludes private security services.

---

85 Art. 26 TFEU provides that „The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured [...]“
6.2 **General Market Framework for Services**

Differing from security products and systems, security services are typically certified with the private market in mind (i.e. not necessarily applicable to police, border guards, etc.). This means that standards for state-employed police and security personnel are arrived through different procedures than for private security providers. This could also be seen as a contributing factor to the above-mentioned market fragmentation, as there are national jurisdictions that strongly influence how national police and other security forces are to be trained and what exactly their competences might be.

Standards regulating the implementation of private security services and the training of staff do exist, however: examples for this are the standard on Aviation Security (EN 16082:2011) or on Maritime Security services, which is currently in the phase of public review (Draft EN 16747).

At the same time, this market for private security services has been growing. This growth is projected to continue in the foreseeable future. Evidence for this can be seen in a general shift in ratio between the number of police force and the number of private security personnel deployed. The Confederation of European Security Services (COESS), representing the interests of private security companies, in a 2011 report provides numbers reflecting the current status of this market segment:

<table>
<thead>
<tr>
<th>Economic Aspects of the European market in private security services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average EU-wide ratio security force per 10.000 inhabitants</td>
</tr>
<tr>
<td>Average EU-wide ration police force per 10.000 inhabitants</td>
</tr>
<tr>
<td>Total yearly turnover of the private security industry</td>
</tr>
<tr>
<td>Average market growth of the private security industry (based on yearly turnover) 2005-2010</td>
</tr>
<tr>
<td>Average combined market share, at national level, of the top three private security companies (market concentration)</td>
</tr>
<tr>
<td>Average balance of yearly turnover of general guarding services versus other industry segments</td>
</tr>
<tr>
<td>Average number of armoured cars in use for Cash-In-Transit (CIT) operations</td>
</tr>
</tbody>
</table>

Table 17: General Information and economic aspects of the European market in private security services

---


89 „Security Force“ to include a list of around 25 deployment theatres for such personnel. A detailed list to be found in Appendix B.

90 COESS, op. cit., 2011, p.143.
6.3 Security: Public Good or Market Commodity?

The provision of providing security as a public good pursues significantly different objectives than the provision of private security services as a market commodity. Conceptualising security as a public good, the major criterion would be whether no one can be excluded from enjoying the benefits the provision of such services bring about. Typically, therefore, security, such as national security from armed aggression, but also citizen security from terrorism or organised crime, is provided by the state, paid by taxes and no citizen can be excluded from benefiting. Such an understanding of security obviously sees its provision as a prerogative of the state.

With the provision of private security services, it is likely to be very different: typically, not the general public, the citizen, is the addressee of the measure taken, but rather specific clients (which obviously does not preclude cases private service provision addressing all citizens, such as airport screenings).

What is being deplored on many occasions as the “fragmentation of the EU’s security market” is the consequence of each member state’s applying different rules (national legislation), hampering cross-border provision of services, but also economies of scale. With the emergence of private markets in security products and services, this “monopoly” of provision decreases, yet fragmentation has not gone away, as the development of standards harmonising security service provision throughout the EU’s internal market is still underway.

Smith and Brooks provided an analysis of the main ramifications that result from providing security as a public good as opposed to a commodity on a market:

<table>
<thead>
<tr>
<th>Private Security</th>
<th>Function(^{91})</th>
<th>Public Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Input</td>
<td>Citizen</td>
</tr>
<tr>
<td>Selective</td>
<td>Service</td>
<td>Equal</td>
</tr>
<tr>
<td>Profit-driven</td>
<td>Delivery Resourcing</td>
<td>Tax-funded</td>
</tr>
<tr>
<td>Undetermined</td>
<td>Finance</td>
<td>Predetermined</td>
</tr>
<tr>
<td>Fragmented</td>
<td>Structure</td>
<td>Centralised</td>
</tr>
<tr>
<td>Citizen</td>
<td>Power</td>
<td>Legislated</td>
</tr>
<tr>
<td>Limited</td>
<td>Training</td>
<td>Intensive</td>
</tr>
<tr>
<td>Loss prevention</td>
<td>Role</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Protection</td>
<td>Orientation</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Specific</td>
<td>Target</td>
<td>General</td>
</tr>
<tr>
<td>Private</td>
<td>Space</td>
<td>Public</td>
</tr>
<tr>
<td>Restricted</td>
<td>Regulated</td>
<td>Heavily</td>
</tr>
</tbody>
</table>

\(^{91}\) “Function” is not to be confused with the way we use security functions in CRISP. Rather, this refers to dimensions of comparison between the private and the public aspects of security „marketing”.
### Security as Profession and Training Requirements

Analysis of already existing standards in the domain of private security services has shown that emphasis of training, education and refresher measures (vocational training) is a key element in ensuring quality of the services provided. EN 16802:2011, for example, stresses that any personnel employed by private security providers has to be specifically trained for every single task this person provides. This is seen as an important element of quality assurance.

A preliminary classification of security services can be made according to whether they are “blue collar” or “white collar” services, i.e. whether they involve manpower (guarding, cash in transit services) or complex and theoretical know-how, such as security consulting, data protection and management services or analytical services requiring extensive education and training. According to these criteria, certification schemes for security professionals would have to take into account different types of training and education.

Security services can be classified according to the extent of training that personnel have to undergo. This comprises the

- a) Duration of training (measured e.g. in hours, ECTS etc.),
- b) Level of achieved qualification (secondary, tertiary, ...)

Accordingly, security services are also subject of university study programmes: A cursory scan, taking higher education in Germany as an example, has yielded several study programs of relevance for or directly geared at security service professionals. This includes both Master and Bachelor programs (see Table 19). A comprehensive survey for Germany has been conducted by the Forschungsforum Öffentliche Sicherheit / FÖS (Research Forum on Public Safety and Security)\(^\text{94}\). The following table provides an overview of typical study programmes for security services.

---

93 European Credit Transfer System
| **Emergency Practitioner** | • Envisaged security area: emergency services, civil protection;  
• Target competencies of graduates: Management tasks, leadership development in civil protection and emergency services; skills development in education and training;  
• Prerequisite completed education: emergency paramedic. |
| **Security Management** | • Security Management in organisations or local communities / constituencies  
• Target competencies of graduates: identifying, assessing and handling risk situations;  
• Security areas: corporate and plant security, compliance management, facility management, consulting, leadership and investigative tasks (violent crime, economic crime), risk management, emergency management; organising simulations,  
• Entry prerequisite: general eligibility for higher education study programmes, OR completed education as naval officer |
| **Business Administration and Security Management** | • Leadership tasks in risk management and prevention (possible specialisation on emergency management)  
• Target skills: combination of business administration and disaster management, risk analysis and – management, disaster communication and analysis of the genesis of a disaster;  
• Obligatory entry exam |
| **Security and Risk prevention** | • Geared to fire-fighting services, civil protection organisations, policing services (investigate origins of a fire), industrial and facility security management, experts offering expertise to insurance companies (mainly risk assessments)  
• Objective: improve competencies in these fields |
| **International emergency and disaster relief** | • Disaster Management skills development  
• Graduates should be able to  
  o apply standards in international humanitarian relief  
  o work in an intercultural environment  
  o be knowledgeable international structures of cooperation in disaster relief  
  o carry our risk analyses and risk assessments  
  o plan and implement relief projects  
  o analyse logistical and medical processes with regard to disaster management |

[Table continues on the next page]
Target capabilities include:
- Optimise existing security management systems (e.g. in the fields of corporate and information security, as well as internal revisions/investigations)
- Business continuity management

Vocational training for journalists, corporate security professionals, private investigators;
Services taught include criminal tactics, IT-forensics, forensic psychology, business culture

Target capabilities and services include:
- Planning and implementation of risk management systems
- Consulting, auditing and support for companies with regard to risk management issues
- Conduct trainings in risk management
- Develop comprehensive security concepts for corporate security

### Table 19: Sample of academic study programmes preparing for security-related services (taken from FÖS 2014)

The information presented in the table above is distilled from existing security-related higher education curricula. Standards specifying aspects of private security provision typically do not specifically refer to training (or, for that matter, education) in a university-environment. Norms regulating competence criteria for security services, obviously, address personnel, but also the organisational framework of the service provider. While in the EU, there seems to be not so much coherent thinking about private security provision as a fully-fledged profession\(^\text{95}\), literature suggests that in Australia, for example, attempts at establishing the distinct category of a security professional are much more advanced:

“Security Professionals are practitioners who provide security services in government, the private sector, academia and the NGO sector in areas such as security policy, security management and the range of security consulting. Indeed, the profession provides services critical to the public interest and is recognised as representing a distinct managerial and technical discipline with its own body of knowledge and expertise.”\(^\text{96}\)

While the concept of a “security professional” might lead to a more coherent approach to the development of standards and certification of competencies of security staff and thus help reduce the market fragmentation, it also faces the challenge that the services provided by private security staff are of some degree of diversity and require different levels of qualification.

Certification schemes might reach the conclusion that the security professional could be seen as a profession uniting a bundle of services. Current training requirements as foreseen by the

---

\(^{95}\) EN 15602:2008 on Security Services Terminology specifies them as “services provided by security companies aimed at protection of people, property and assets”

relevant standards do conceive of more than one stage of training for service providers, starting with “basic training” which is to be refreshed at regular intervals. On top of this, “specialised” training is foreseen that allows for more detailed differentiation of skills. Such training allows the person to perform more complex tasks or heightens their ability to move from one service provision area to another (increased job mobility).

In sum, it should also be noted that the concept of security is constantly in flux and more often than not it also matters who is being asked. It could be argued that with this multidimensionality and diversity of what is or is not being framed as security-relevant,

“there exists a need for research into developing a consensus and functional unity among the various branches of the security profession, and to identify emergent issues that affect security as a profession, such as ethical considerations of transnational security practices. There is little agreement on definitions, but there is also little argument against the fact that the dramatic change in social structure and perceptions post-9/11 has changed security forever, and that change appears to be pushing security inexorably towards becoming a new profession.”

The European Standard EN 15602:2008 on terminology of Security Service Providers sketches out some features not of the “security professional” but of the “security officer” or “security guard” (and is thus more restricted in semantic scope). This person, properly trained and screened is to be characterised by the following functions he or she performs:

- Access Control functions, such as
  - Prevention or detection of intrusion, unauthorized entry or activity, vandalism or trespass on public or private property;
- Financial and capital-related crime
  - Prevention or detection of theft, loss, embezzlement, misappropriation or concealment of merchandise, money, bonds, stocks, notes or valuable documents or papers;
- Protection of individuals from bodily harm;
- Environmental protection and management in rural and maritime domains;
- Compliance aspects, such as
  - Enforcement of established company rules, regulations, policies and practices related to crime reduction;
- Reporting and apprehension of violators as defined by national law.

---

97 Griffiths, Mel, David Brooks, Jeffrey Corkill, „Defining the security professional: definition through a body of knowledge“, proceedings of the 3rd Australian security and intelligence conference, Edith Cowan University, Perth, 30th November 2010.

98 As in Table 18, “function” is not congruent with the CRISP approach outlined in D1.1. It is however, noteworthy to see an approach was chosen that characterises a security profession by the functions that have to be performed (and this is very similar to the CRISP-approach).
Regardless whether we should speak of “the security professional” or rather should focus on the kind of service that is being delivered, standards to enhance competency through training have emerged. EN 15602:2008\(^99\) contains several specifications relevant for the training of security personnel delivering security services. These are:

- “Basic Training”: allows a person who wishes to enter and work in the field of private security to gain minimum levels of skill (beginner’s level);
- “Refresher Training”: generally aimed at practicing, maintaining and updating previously acquired skills;
- “Additional Training”: to develop already learned skills, but also to acquire new ones
- “Specialised Training”: Offered to allow security personnel to acquire supplementary skills

How such approaches to training measures and requirement play out in a practical context, it is useful to look more closely at an example from the European Standard EN 16082:2011\(^{100}\) on Airport and aviation security services, where the concept of training is operationalised and adapted to aviation and airport requirements:

<table>
<thead>
<tr>
<th>Basic Training</th>
<th>Security Awareness</th>
<th>Communication skills &amp; terminology of airport/aviation security</th>
<th>Customer service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e.g. definitions common to aviation; understanding aviation security; aviation terminology; organisational principles of an airport; location of security-relevant and critical areas; other relevant parties (e.g. police, fire guards, airport authorities, other service providers); relevant workflows; security communication at an airport; risk and emergency management; dangerous objects; continuity planning</td>
<td>Basic English for aviation security; common international terminology; basic IT-terminology; abbreviations/acronyms</td>
<td>Interpersonal skills; conflict management; lost passengers; support for passengers; handling stress-situations</td>
</tr>
</tbody>
</table>

| Table continues on the next page |

\(^{100}\) CEN, EN 16082:2011 Airport and aviation security services.
<table>
<thead>
<tr>
<th>Specialised Training (examples)</th>
<th>Screening of passengers, personnel/crew and objects</th>
<th>Organisation and structure of security checkpoints; interviewing persons about objects they carry; knowledge of “blacklisted” persons and objects; personality profiles of passengers;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Key elements of an effective person-screening; using technology vs. screening with the hand; sensitive aspects of screening with the hand (e.g. sex, culture, disabilities)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key elements for effectively screening objects and hand luggage</td>
</tr>
<tr>
<td>Luggage Screening</td>
<td>Organising the workflow and procedures;</td>
<td>Organising the workflow and procedures;</td>
</tr>
<tr>
<td></td>
<td>Key elements of effective luggage screening;</td>
<td>Key elements of effective luggage screening;</td>
</tr>
<tr>
<td></td>
<td>Basic security measures</td>
<td>Basic security measures</td>
</tr>
<tr>
<td>Security of cargo and mail</td>
<td>Organising and facilitating cargo processing structures</td>
<td>Organising and facilitating cargo processing structures</td>
</tr>
<tr>
<td>Training on x-ray equipment and other detection devices</td>
<td>Organising an x-ray screening point; Understanding the workflow; Aspects of radiation safety; Knowledge about threat image projection (visualising dangerous goods);</td>
<td>Organising an x-ray screening point; Understanding the workflow; Aspects of radiation safety; Knowledge about threat image projection (visualising dangerous goods);</td>
</tr>
<tr>
<td>Screening vehicles</td>
<td>Organising the checkpoint and key elements of effective screening; Approach to randomly selecting vehicles and determining the screening rate</td>
<td>Organising the checkpoint and key elements of effective screening; Approach to randomly selecting vehicles and determining the screening rate</td>
</tr>
<tr>
<td>Protection and screening of airplanes</td>
<td>Key elements of the workflow</td>
<td>Key elements of the workflow</td>
</tr>
<tr>
<td>Other training elements</td>
<td>General introduction to airports, aviation and passenger-related affairs</td>
<td>General introduction to airports, aviation and passenger-related affairs</td>
</tr>
<tr>
<td></td>
<td>Risk analysis</td>
<td>Risk analysis</td>
</tr>
<tr>
<td></td>
<td>Theoretical and practical skills (as required by a specific task)</td>
<td>Theoretical and practical skills (as required by a specific task)</td>
</tr>
<tr>
<td></td>
<td>Workflows</td>
<td>Workflows</td>
</tr>
</tbody>
</table>
|                                | Testing of the training through practical and theoretical exams, | Testing of the training through practical and theoretical exams,
6.5 EXISTING ATTEMPTS AT BUILDING CATEGORIES OF PRIVATE SECURITY SERVICES

David Brooks built a model\(^\text{101}\) of practical security fields coupled with levels of governance, in an attempt to capture the multidimensionality and diversity of the field. The main purpose of this was the categorisation of the field through body-of-knowledge analysis. Brooks’ model focuses strongly on capabilities and the resources required to deliver them at different levels of governance. CRISP moves beyond this model by taking application areas and security functions into the analytical framework as well. However, this model provides a good glance at the market from the perspective “What is it that needs to be certified?” in terms of services a “security professional” should (be able to) deliver.

<table>
<thead>
<tr>
<th>Level of Governance</th>
<th>Strategic Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Operational</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>IT &amp; Computing</td>
</tr>
<tr>
<td></td>
<td>Physical Technology</td>
</tr>
<tr>
<td></td>
<td>Investigation</td>
</tr>
<tr>
<td></td>
<td>Personnel</td>
</tr>
<tr>
<td></td>
<td>Industrial</td>
</tr>
<tr>
<td></td>
<td>Level 1</td>
</tr>
<tr>
<td></td>
<td>Business Continuity</td>
</tr>
<tr>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Law</td>
</tr>
<tr>
<td></td>
<td>Criminology</td>
</tr>
<tr>
<td></td>
<td>Facility Management</td>
</tr>
<tr>
<td></td>
<td>Fire &amp; Life Safety</td>
</tr>
<tr>
<td></td>
<td>Safety</td>
</tr>
<tr>
<td></td>
<td>Level 2</td>
</tr>
</tbody>
</table>

Another classification, also in attempt to better penetrate the field and contribute to the emergence of the profession of the “security professional” by elaborating a shared body of knowledge, was developed by ASIS International in 2009.\(^\text{102}\) Their delimitation differs, and has a much stronger focus on security functionality as we understand it (cf. CRISP D1.1) and also takes application areas (as used in this deliverable) more into account:

<table>
<thead>
<tr>
<th>Physical security</th>
<th>Personnel security</th>
<th>Information security systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations</td>
<td>Loss prevention</td>
<td>Risk management</td>
</tr>
<tr>
<td>Legal aspects</td>
<td>Emergency / continuity planning</td>
<td>Fire protection</td>
</tr>
<tr>
<td>Crisis management</td>
<td>Disaster management</td>
<td>Counterterrorism</td>
</tr>
<tr>
<td>Competitive Intelligence</td>
<td>Executive Protection</td>
<td>Violence in the workplace</td>
</tr>
<tr>
<td>Crime prevention</td>
<td>Crime prevention through environmental design</td>
<td>Security Architecture &amp; engineering</td>
</tr>
</tbody>
</table>

---


Another attempt at building categories, was undertaken by Carlos Martí Sempere as part of the EUSECON project\textsuperscript{103}. This approach directly and exclusively addressing the European security market is more similar to the CRISP approach, as it merges security functions (as we understand them) with application areas and roughly looks like this:

- **Preparedness**
  - Consultancy
  - Training and Rehearsal

- **Intelligence and Surveillance**
  - CCTV
  - Intrusion detection and perimeter protection
  - Border protection
    - maritime surveillance
    - air surveillance
  - identification and access control
    - Mechanical locks, entryphones, key pads
    - card systems
    - biometric systems
    - land vehicles surveillance
  - screening of personnel and their belongings
  - goods and merchandise
    - tagging systems
  - Systems to support intelligence operations
  - CBRN detection / early warning equipment
    - chemical agents
    - biological agents
    - radiological agents
    - nuclear agents
  - other awareness products

- **Protection**
  - Building protection
  - Vehicle protection
  - personal protection
  - manned guarding services
  - network and information security (NIS)

- **Interdiction / crisis management**
  - Personal equipment

---

• Vehicles („For certain operations land vehicles, helicopters or maritime craft are needed to interdict criminal actions and prosecute malefactors. “)

• **Response and Recovery**
  • Firefighting
  • First response healthcare
  • Logistic support
  • Coordination and management (whole range of command & control infrastructures)

• **Forensics**
  • Equipment
  • Investigation Services.
7 CRISP TAXONOMY OF SECURITY SERVICES

The service-taxonomy builds on the same categories developed for products and systems. This could help future research work in this field better align development for these two areas (i.e. what kind of products are required to carry out what kinds of services?). Focus was laid on literatures and already existing standards on security service provision operationalising service “roles” or typologies. One example would be the security guard. While in the strict sense, this does not denote a specific service, but rather a kind of profession, it should also be viewed as a bundle of competencies and potential services (such as screening, searching, interrogating, etc.). It is also the added value of the taxonomy to highlight that one security profession is capable to perform more than one security functions.

7.1 ADAPTION OF THE CATEGORISATION OF THE PRODUCTS AND SYSTEMS TAXONOMY FOR THE SERVICES

The categorisations used for the security products and systems taxonomy thus are also used for the service taxonomy, but needs in some cases a few adaptions. Moreover for the better readability and comprehensibility of the security service taxonomy, a description of the use cases of security services in the application areas is provided.

7.1.1 Security Services and Application Areas

What the Taxonomy on security services shows is that the specific services can often be deployed in several of the application areas, but the individual application areas still have some unique features, which has an influence on the demand, function and usage of the security services. In connection with border management for example security staff is engaged in the most relevant security-functions such as detection, identification or authorisation. According to descriptions of service providers and the professional roles they outline, these roles (e.g. security guard, beat patrol, canine services) can be attributed to more than one function. Services regarding critical infrastructures are therefore not consistently dealt with. While some classification attempts know of “critical infrastructure protection” as a distinct service category, other schemes treat this application area implicitly with regard to general guarding or monitoring tasks, some however can be very specific when it comes to certifying e.g. cyber-related critical infrastructure protection. Again it can be seen that security guards, beat patrol services or canine services can perform a broad range of security-functions.

Households and security services are for example a very sensitive topic, since most of the time it implies the granting of one’s personal security through another – unknown – person and thus makes it necessary to trade-off some of one’s privacy. This leads to several security services that are, due to their intrusive nature, not or only partly applicable to households, as

---

104 Coess, op. cit., 2011.
for example with security guards. In the taxonomy, we thus have applied the idea broadly to include services ranging from community/neighbourhood watching and monitoring services to more targeted cases such as key holding (which in itself can be segmented according to the number of different functions served) or guarding services as for example deployed in the context of “gated communities.” Much depends also on national legislation which regulates service implementation parameters such as the wearing of uniforms or carrying weapons (firearms).

Compared to the households, security services applicable to public and semi-public places are completely opposite. On the one hand they have a strong component of access control functionality. On the other hand they also need to be able to control and oversee large groups of visitors or citizens, making the same security guard that can be used for the security of “gated communities” cover much more demands and functions. Beyond this, it should be noted that detention is one of the functions outlined in CRISP D1.1 which is strongly dependent on (national) legislation frameworks: not only in the context of public and semi-public places (but probably of high relevance here), regulation plays a strong role in setting the context. Security service providers in Finland, for example, have the right to hold up and detain a person under specified circumstances.\footnote{Finnish Ministry of the Interior, \textit{Private Security Services Act}, 2003, Online at: \url{http://www.finlex.fi/en/laki/kaannokset/2002/en20020282.pdf}.} It is interesting to note in this regard that this Act defines security services as the management of security on the basis of contractual relations.\footnote{Ibid., chapter 1.} Also, as far as the concept of the “security officer” is concerned, there is a certain tautology involved: the security officer is understood as a person in service of a private security service supplier and requiring security certification. In this instance, as well as future standardisation approaches, functionality should play a much stronger role.

Most of the security services that can be identified for the public and semi-public spaces can also be applied to security-related services in the domain of industry and retail, spanning the entire scope of applicable services, covering services that require basic training up to services which require intensive training. Furthermore the industry sector will also probably be similarly susceptible to threats than critical infrastructures are.

In line with the EU’s objective to increase resilience to natural and man-made disaster, emergency and response services are on the increase, also in order to back newly devised policies and strengthen the structures created under this regime. While the response-segment of the crisis management cycle is only one pillar of successful resilience patterns, this part is no less important. Many of such services are of higher training intensity degrees, requiring e.g. medical or paramedical training. Other services include a strong management component, e.g. evolving around a disaster where an emergency perimeter has to be set up and run, along with security functions such as the detection and control of unauthorised persons, resource mobilisation, and mass casualty events (incl. triage services). Other services are bundled in the concept of business continuity management, which has already been covered extensively in standardisation efforts. In order to fully embrace resilience as
planning and design paradigm in crisis management, the functions were to be extended to also include anticipatory, prospective measures and concepts of preparedness. It should be noted though that, as resilience is not primarily about prevention but rather about dealing with radical uncertainty, the prevent-functionality would rather remain in the backdrop against other approaches such as various foresight tools and services that aim to grasp or display future events in a broad array of alternatives. So security services on crisis management are probably the most distinct compared to all the other application areas.

Finally a strongly policy-driven area, are security services relevant to the transport domain that have been applied broadly, to cover not only (mass) public transport systems, but also security challenges to the supply chain, logistics and other, more specialised aspects such as cash-in-transit services. Again, it becomes evident that service providers can be attributed to several functions. It should have become clear by now that professional titles, such as “security guard” (who, in one shift, could, for example, detect, locate, track, identify or authorise persons) or “beat patrol” or “alarm & CCTV monitoring” can perform several functions and should play a much more dominant role in future standardisation and certification schemes, tailoring the standards to the specific areas that should be covered. Some security services, like airport security services or port security services are already covered like this by standardisations.

### 7.1.2 Additional Functions

Regarding the security functions, the security services largely draw on the same as the security products and systems, thus also aiming at a similar outcome of their deployment in security related areas. Still two additional functions have been identified, one being a more broad one applicable to several application areas, the other one being specific for crisis management services. An implementation of these functions in the glossary of security products, systems and services can be considered as a further expansion of the glossary.

**Detect:**

The function to detect can be defined as “to discover or notice the presence of (something that is hidden or hard to see, hear, taste, etc.)”\(^{109}\) and is thus one of the security functions that, similar to locate and track, can be seen as a primitive security function as defined by the CRISP Glossary.\(^{110}\)

---


Respond:

Respond “encompasses the decisions and actions taken to deal with the immediate effects of an emergency”,\textsuperscript{111} and is thus a specific function related to the security area of crisis management. Especially in regard to Emergency Site Management Systems (ESM) and the corresponding security services, emergency response is a crucial functional.\textsuperscript{112}

Thus based on a slightly adapted version of the security products and systems taxonomy, the taxonomy of security services will try to show how the services can cover on the one hand a multiple amount of application areas and on the other hand still be very specific within their domain. Furthermore for the services a colour-coded taxonomy has been chosen: this facilitates a better understanding of the service with regard to its nature – is it more manpower-oriented or is it more of an intellectual service. Roughly, this might to some extent correlate with the amount and intensity of training the security professional needs (by standards, or other legal/compliance codes) to perform this service and thus also plays an important role for the certification and standardisation of the training. For this a colour-scheme has been chosen, reflecting a Likert scale, starting from very light (being (1)) to dark (being (5)). Thus the darker therefore the node, the more the respective service is of an intellectual nature and, typically, the more training is required. For a better readability, most of the taxonomies have been divided on two pages.

\textsuperscript{112} Canadian Emergency Preparedness College, Summary of the Emergency Site Management System for CBRN intermediate level course, no date, Online at: http://www.nfpa.org/~media/Files/Member%20access/member%20sections/metro%20chiefs/MetroEmanage.pdf.
7.2 **Border Management Taxonomy**

[Diagram showing the Taxonomy of Security Products, Systems and Services for Border Management]
Border Management

Asset/freight/cargo security

Cybersecurity

Access control

Detect

Identify

Verify

Authorise

Prevent/protect

Forensic Investigator

Security Specialist

Security Analyst

Information collection, storage and management

Network Defense Architect

Encryption Specialist

Security Administrator

Data Analyst

Security Administrator

Forensic Investigator

Prevent/protect

Detect

Track

Identify

Prevent/protect

Detect

Alarm and CCTV Monitoring

Track

Alarm and CCTV Monitoring

Identify

Cargo (incl. mail) screening services

Prevent/protect

Security Policy Plans, documentation

Security Risk Management

Security Consulting

Security Guard

Interview Services with passengers (e.g. air, sea)

Security Guard

Interview Services

Security Guard

Detect

Screening Services (Cargo, Passenger)

Alarm and CCTV Monitoring

Notify

Security Guard

Detect

Cargo (incl. mail) screening services

Prevent/protect

Security Policy Plans, documentation

Security Risk Management

Security Consulting

Forensic Investigator

Data Analyst

Security Administrator

Private Investigation Services
7.3 Critical Infrastructure Taxonomy
7.4 Crisis Management Taxonomy
### 7.5 Household and Individuals Taxonomy

![Household and Individuals Taxonomy Diagram]

- **Households**
  - Access Control
    - Detect: Alarm and CCTV Monitoring
      - Key Holding
    - Identify: Alarm and CCTV Monitoring
      - Concierge Services
      - Key Holding
    - Verify: Mobile alarm response and call-out services
      - Alarm and CCTV Monitoring
      - Concierge Services
      - Key Holding
    - Authorise: Concierge Services
  - Asset security
    - Detect: Alarm and CCTV Monitoring
    - Locate: Alarm and CCTV Monitoring
    - Identify: Alarm and CCTV Monitoring
    - Verify: Mobile alarm response and call-out services
      - Key Holding
      - Alarm and CCTV Monitoring
    - Prevent/protect: Mobile alarm response and call-out services
      - Key Holding
  - Cybersecurity
    - Assess: Virus Scanner Support Service
      - Virus Removal Service
      - Certified security analyst
      - Technology Consulting
      - Data Protection Consulting
    - Create Situational Awareness
    - Protect: Virus Scanner Support Service
7.6 **Industrial and Retail Taxonomy**
7.7 **PUBLIC AND SEMI-PUBLIC VENUES TAXONOMY**
D1.2: Taxonomy of Security Products, Systems and Services

CRISP project

Public and semi-public spaces
7.8 **Transport Taxonomy**
7.9 **CONCLUSION**

Future standards and certification schemes of security related services should better take into account the fact that existing “professions” such as “security guard” or “beat patrol”, “aviation security services” or “port and maritime services” are subject to a broad scope of deployment: in many cases, they can (and even should) perform more than one function. Better building standards on these functions could help raise the profile of specific security providers.

Also, such schemes should take into account that service provision operates at different levels of governance, ranging from strategic security, to security management to the operative level. In some instances, training intensity correlates with level of governance, e.g. in the case of security management as envisioned by university curricula. In other instances, services requiring certification of high-intensity training such as cyber-forensics expertise can operate directly at the operative level, i.e. directly interacting with a threat. Little surprisingly, the taxonomy shows that there is a tendency towards more training-intensive services in the area of cyber-security, cutting across all the application areas.

As the European Internal Security Strategy calls upon the **EU’s Member States** (and thus state authorities) to step up efforts in tackling the threats already mentioned here (including organised crime, terrorism, enhanced disaster resilience), it should be noted that reaching these objectives does not – an cannot – exclude privately provided security services. Rather, and this would be in line with contemporary discussion in disaster resilience, public-private partnerships could emerge, and this is something future standardisation and certification efforts might want to take into account: that standards on security services might also include interfaces with the “public”, i.e. state-authority sphere, and foresee basic patterns of cooperation or exchange of information with the policies, public prosecutors and other services at the core of “the state”.

There is a crosscutting theme that needs consideration when designing standards and certification schemes for security services: very often security work affects legally defined standards and involves interventions in citizens’ individual spheres of freedoms (incl. freedom of movement, bodily integrity, protection of person related data). Most operational service provision is embedded in such legal contexts. Hence it is necessary to integrate legal knowledge into the training and certification schemes. When looking at the present situation in the field of security services one can see an interesting difference. While service provision by public authorities (from police to customs to health services) is strongly focussing on the legally defined rights and the limits of intervention into sphere of individual rights, training schemes in the private security sectors have a strong emphasis on the operational competencies required for professional security work. Integration of both dimensions into a joint set of standards would improve the situation and facilitate cooperation.
8 CONCLUSION

The objective of this task was to produce a useful and needs-based taxonomy for security products, systems and services on the market in order to categorise them. The analysis placed particular stress on classification through application areas, seven of which were identified through the abovementioned review. It is important that application areas provide a starting point for the taxonomy as any evaluation and certification scheme of products and systems will need to work across security sectors. The CRISP taxonomy contributes to this task in providing a clear way of categorising products according to a 4 level taxonomy to application area > demand > need/function > security product/system/service.

With the on-going shift in the domain of security provision from being state-driven towards more market-driven dynamics, the concept of the security professional has been undergoing considerable change. One major ramification of this trend is the increasing specialisation: as the taxonomy shows, there are many services / job titles which serve more than one security functionality. The relevant functionalities are determined by the context or areas of application.

Any attempt to pin down a “final” definition of security, will inevitably run up against boundaries created by the problem that security – conceptually – is determined by context. This is no less true for security services that are being provided on the European security market(s): “When we use the term security without context, it can and does mean many things to many people.” Yet, the authors acknowledge that “security can be defined given context.” This deliverable has shed some light on the discussion around the concept of a general “security professional” vs. security guards or forensics experts being standardised (and certified) in very specific application areas such as the service duties related to an airport/aviation security officer or cyber network defence tasks.

This taxonomy adds value and contributes to a better understanding of security services by such context: the application areas and distinct functionalities which security staff can perform. It should be noted that, contrasting with security products, it is not the functionality as such that determines the job: a security guard is a security guard because this is the professional title and that is what the person is paid for. However, there is ample space and a broad scope for more detailed analysis of the profession, especially when it comes to certification: how much of the actual job description does require certification, i.e. to what extent does the person serve a genuine security-function (such as detection, identification, or tracking), and what parts of the profession are not core elements, and could be performed also by non-security-certified staff, such as, for example, communication services, etc.?

With the proliferation of security as a societal frame to understand social processes and problems a security dimension is added to a growing number of domains – from transport to infrastructure to general social services. One should keep in mind the dynamics fuelling this

113 Smith, op. cit., 2013, p.2.
114 ibid. p.2
process that is based on the logic of risk. Understanding complex systems as risk prone immediately calls for some sort of security action. Designed to prevent future damages security action entails pre-emptive interventions in standard procedures. This again opens a wide array of opportunities for the application / implementation of security products, systems and services. Whether or not this form of “securitization” is a rational option for redesigning social processes from a risk/security perspective is beyond the scope of this task.

Nonetheless, when developing standards for security PSS this underlying dynamic should be kept in mind and be used as a general guidance by asking whether the perceived problem at hand is a security problem in the first place.

The taxonomy of security PSS is important as we move towards creating a certification and standardisation scheme for Europe. The CRISP project aims to transcend, while harmonising and co-ordinating, national differences in security standards and certification, and as such European security policy lays the foundation for the taxonomy. Hence, the EU Internal Security Strategy (ISS) and its five priority areas detailed in section 2 provide the context within which the CRISP taxonomy exists. However, the ISS priority areas proved too broad and intangible for building the taxonomy, as they do not clearly present who the key actors are, what their security demands and needs may be and what security PSS may help to meet those needs. Consequently, for the purpose of building a taxonomy, the ISS can only provide the broad boundaries within which security work takes place. The EC Security Industry Policy, however, set forth a categorisation of security sectors, which fed into the seven application areas for the CRISP taxonomy.

The review of EU-funded security projects furthermore revealed the multidimensionality of the security/security products field of study and fed into the taxonomy in different ways. The Ecorys reports provided insights into the division between “traditional” and “new” security products, which may have different certification and standardisation needs. The IRISS project provided an overview of different application areas and an extensive list of surveillance technologies. However, these projects proved somewhat lacking in helping to clarify a clear system for categorising systems and products on the basis of application area and need/function. These were most instances either too broad (e.g., “commercial solutions”) or intangible (e.g., “movement of people”) to provide a practical level 1 – application area, under which demands and needs could be ascribed.

The ways in which commercial actors defined and categories application areas, market demands, user needs and appropriate products and systems proved most useful for the building of the taxonomy. They provide a clear and concise manner to organise (according to user, need and function) the complex and fragmented landscape which security provision presents. The commercial categorisations are contextualised within risk discourses in that they lay out possible security scenarios and offer solutions in the forms of products, systems and services. Furthermore, they offer tangible market demands and needs under which PSS can be further classified.
As acknowledged above, security can be defined in myriad ways depending on context, political, public, policy and commercial viewpoints and with regard to standardisation. There is currently somewhat of a disconnect between the ways in which security is prioritised in the political and policy areas, which are in many instances threat and risk driven, and the commercial and standardisation areas. The security policy priorities change rapidly and hence the prioritisation laid out in political and policy security literature may differ from that of commercial and standardisation spheres and as such offer broad strategies under which security PSS are categorised and subsequently standardised and certified.

Further examination of different stakeholder priorities, current best practice in security standardisation and certification and the introduction of the CRISP scheme will further serve to align, harmonise and co-ordinate stakeholder/national differences in security standards and certification in Europe.
9 REFERENCES


Canadian Emergency Preparedness College, *Summary of the Emergency Site Management System for CBRN intermediate level course*, no date, Online at: http://www.nfpa.org/~media/Files/Member%20access/member%20sections/metro%20chiefs/MetroEmanage.pdf.


CEN, EN 16082:2011, Airport and aviation security services.


Griffiths, Mel, David Brooks, Jeffrey Corkill, „Defining the security professional: definition through a body of knowledge“, proceedings of the 3rd Australian security and intelligence conference, Edith Cowan University, Perth, 30th November 2010.


Lagazio, Monica, *Report on Research Approaches and Results*, D2.2 ETTIS project, July 2012.


Wright, David, Ivan Szekely, Michael Friedewald, Rowena Rodrigues, Reinhard Kreissl, Johan Cas and Charles Raab, *Surveillance, fighting crime and violence*, D1.1, IRISS project, 1st February 2012.
### APPENDIX A. LIST OF REVIEWED SECURITY COMPANIES

<table>
<thead>
<tr>
<th>Company name</th>
<th>Specialisation/products</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axis Communication</td>
<td>Network video surveillance</td>
<td><a href="http://www.axis.com">www.axis.com</a></td>
</tr>
<tr>
<td>BAE Systems</td>
<td>Global defence, aerospace and security.</td>
<td><a href="http://www.baesystems.com">http://www.baesystems.com</a></td>
</tr>
<tr>
<td>Brickhouse Security</td>
<td>GPS Trackers, Hidden Cameras, PC and Cell Phone Monitoring solutions and Video Surveillance tools.</td>
<td><a href="http://www.brickhousesecurity.com">www.brickhousesecurity.com</a></td>
</tr>
<tr>
<td>G4S</td>
<td>Security solutions - Electronic tagging</td>
<td><a href="http://www.g4s.com">http://www.g4s.com</a></td>
</tr>
<tr>
<td>Honeywell</td>
<td>Biometrics, video analytics, UAV’s, remote home monitoring, wireless sensing etc.</td>
<td><a href="http://www.honeywellcity.com">http://www.honeywellcity.com</a></td>
</tr>
<tr>
<td>Indra Sistemas</td>
<td>GIS Software, Airborne intelligence systems, Electronic surveillance measures (ESM) and alert systems. Intelligence and tactical electronic war systems, radar systems etc.</td>
<td><a href="http://www.indracompany.com">www.indracompany.com</a></td>
</tr>
<tr>
<td>Safran Morpho</td>
<td>Identification and detection systems - e.g. AFIS (Automated Fingerprint Identification System), smart cards,</td>
<td><a href="http://www.morpho.com/detection/?lang=en">http://www.morpho.com/detection/?lang=en</a></td>
</tr>
<tr>
<td>Company</td>
<td>Description</td>
<td>Website</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>QinetiQ</td>
<td>Special areas of expertise include remotely operated robots, unmanned aerial vehicles (UAVs), vehicle armour and sensor networks.</td>
<td><a href="http://www.qinetiq.com/">www.qinetiq.com/</a></td>
</tr>
<tr>
<td>Siemens</td>
<td>Integrated surveillance system called Surveillance, a security solution integrating different surveillance solutions (like video intelligence analysis and surveillance).</td>
<td><a href="http://www.siemens.com">http://www.siemens.com</a></td>
</tr>
<tr>
<td>Tyco</td>
<td>Intrusion detection, fire detection, video surveillance, access control, critical condition monitoring, health and elder care monitoring, electronic article surveillance, radio frequency identification and integrated systems.</td>
<td><a href="http://www.tyco.com/">http://www.tyco.com/</a></td>
</tr>
</tbody>
</table>
APPENDIX B. LIST OF REVIEWED SECURITY SERVICES

This list builds on a literature review including industry reports, policy guidelines and recommendations, existing standards and certification approaches, as well as scientific literature, as well as the CRIPSP Description of Work.\textsuperscript{115, 116, 117, 118, 120, 121, 122, 123, 124, 125}

It should be noted that the list blends service descriptions with professional titles, which can be understood as “umbrella term” of the various and more detailed the respective person performs in the job. This list, other than the graphical taxonomy, is not presented in a specific order.

- Alarm monitoring services
- Accompanying of secured special transports
- Alarm and CCTV monitoring
- Aviation security
- Beat Patrol
- Bodyguarding (close protection)
- Canine services (security dog handling)
- Cash-in-transit services (including cash handling/processing)
- Chief Information Security Officer
- Civil Security personnel
- Close Protection
- Commercial manned guarding
- Computer Hacking Forensic Investigator
- Critical infrastructure protection
- Cyber forensics professional
- Data analysis

\textsuperscript{117} Coess, op. cit., 2011
\textsuperscript{120} Sempere, op. cit., 2011 pp. 58-107.
\textsuperscript{122} ASIS, op. cit., 2009.
\textsuperscript{123} CEN, EN 15602:2008, op. cit.
\textsuperscript{124} CEN, EN 16082:2011, op. cit.
\textsuperscript{125} Gerhold, et. al., op. cit., 2014.
• Data protection
• Door supervision (bouncing)
• Door supervisors
• Encryption specialist
• Ethical Hacker
• Event security (crowd control)
• Fire prevention and protection services
• Guarding
• Guarding and protection of persons
• In-house manned security
• Incident Handler
• Investigation Services
• Key Holding
• Maritime security
• Mobile alarm response and call-out services
• Mobile Hacking and Forensics
• Museum guard
• Network defence Architect
• Network Security Administrator
• Norm on Business Continuity
• Norm on Risk Manager
• Passenger and cabin baggage screening
• Penetration Tester
• Physical protection
• Private investigation
• Protection of goods and guarding of building
• Receptionist, Concierge services
• Secure programmer
• Security analyst
• Security consulting
• Security Guards
• Security specialist
• Staff carrying firearms
• Store detective (retails)
• Threat assessment and risk management
• Traffic guard with security objective
• Urban security (train/metro stations, city patrols complementing the police etc.)
• Vehicle Immobilisers
• Access control system design,
• Alarm system design,
• Architecture,
• Armed guards (uniformed and plain clothed),
• Blast modelling
• Bodyguards,
• Business administration and security management
• Business continuity management,
• Casual guarding (e.g. major event),
• CCTV system design,
• Close protection,
• Communication system design,
• Competitive intelligence
• Compliance services, such as enforcement of established company rules, regulations, policies and practices related to crime reduction
• Corporate risk management
• Correctional and detention facilities design,
• Crime prevention through environmental design,
• Criminal investigation
• Crisis & emergency management,
• Crisis and disaster management
• Critical asset identification,
• Crowd controllers,
• Drug testing,
• Emergency practitioner
• Engineering vulnerability analysis,
• Enterprise security planning & assessment, Intelligence planning, provision or analysis,
• Environmental protection and management in rural and maritime domains
• Executive and close personnel protection,
• Facility hardening,
- Fire and safety,
- Firefighting
- First response healthcare
- Forensic Perimeter security design,
- Forensics services
- Fraud prevention Loss and prevention
- Information Security
- International emergency and disaster relief
- Kidnap, ransom and extortion support,
- Luggage Screening
- Overseas travel security support,
- Patrol services,
- Personnel screening and vetting,
- Physical security assessments,
- Physical security reviews,
- Polygraph (aka lie detector) services,
- Prevention or detection of intrusion, unauthorized entry or activity, vandalism or trespass on public or private property
- Prevention or detection of theft, loss, embezzlement, misappropriation or concealment of merchandise, money, bonds, stocks, notes or valuable documents or papers
- Private investigators,
- Protection and screening of airplanes
- Protection of individuals from bodily harm
- Public space surveillance (CCTV)
- Red teaming,
- Risk and security management
- Risk compliance,
- Risk management,
- Scenario planning,
- Screening of passengers, personnel/crew and objects
- Screening vehicles
- Security and risk prevention
- Security architecture and engineering
- Security drivers,
• Security guard dog handlers,
• Security management
• Security management benchmarking or gap analysis,
• Security policy, plans, documentation,
• Security project management,
• Security risk management,
• Security systems design,
• Specification writing,
• Surveillance and counter-surveillance,
• Systems integration,
• Technical surveillance counter measures (e.g. de-bugging)
• Threat analysis,
• Training & education
• Uniformed security officers
• Vulnerability analysis