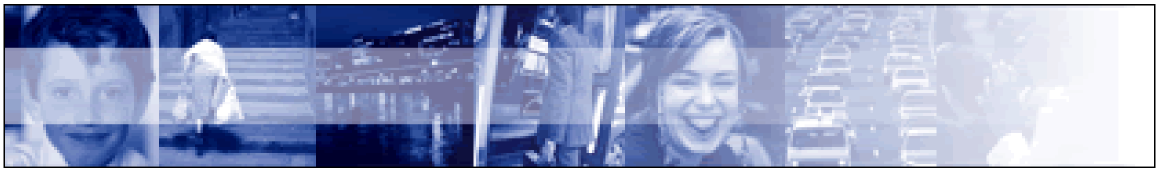
Staccato

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research



STACCATO

Main Conclusions and Recommendations *on the European Security Equipment Market (ESEM)*

and

Executive Summary of the Final Study Report

STACCATO – Stakeholders Platform for Supply Chain Mapping, Market Condition Analysis and Technologies Opportunities

A study funded by the European Commission in PASR call 3 2006

September 2008

This document includes:

- *The STACCATO main conclusions and recommendations on European Security Equipment Market*
  (pages 4 - 13)

- *The Executive Summary of the Final STACCATO Study Report*
  (pages 169 - 80)

*STACCATO (**STA**keholders platform for supply **C**hain mapping, market **C**ondition **A**nalysis and **T**echnologies **O**pportunities) started on 15th January 2007 as a European funded supporting activity under the Preparatory Action for Security Research (PASR) call 3 / 2006 and lasts 16 months. It is a follow up activity of SeNTRE (Security Network for Technological Research in Europe) which was a supporting activity funded under PASR call 1 / 2004.*

STACCATO supporting activity aims at proposing methods and solutions for the creation of a security market and a structured supply chain in Europe. In line with ESRAB (European Security Research Advisory Board) recommendations, it goes beyond research needs and gap analysis already undertaken through efforts supported by PASR, by identifying implementation measures.

Contact

Ms Gloria Martini

STACCATO Project Coordinator

ASD – AeroSpace and Defence Industries Association of Europe

Tel : +32-(0)2-777 02 53
Fax : +32-(0)2-775 81 12

E-mail : gloria.martini@asd-europe.org
Website: http://www.asd-europe.org

Dissemination Policy and Restrictions

The current document is to be considered for public distribution. Intellectual Property Rights belong to the STACCATO consortium. The utilisation and reproduction in whole or in part of the content of this document for commercial initiative is not allowed. The prior written authorisation of the STACCATO Consortium shall in this case be required.

STACCATO Main Conclusions

The STACCATO project arrived at several key conclusions on European security technology and market issues by establishing a community of public and private stakeholders and developing common language methodology – the **STACCATO "tools"** – that are presented in detail in this report (database, security taxonomy, report on dynamic scenarios...) in order to maintain and further develop this network.

It is evident from the work conducted in STACCATO that in many cases **technology** exists but adaptations or specific developments are necessary towards integration, interoperability and innovation. The exhaustive exploitation of current technologies as well as accessibility and affordability (cost issue) are also key issues that need to be examined when looking for new technologies.

As far as the **European security market** is concerned, it exists but is very fragmented. Taking into account the specificities of security technologies and market and each security area/sector, it needs to be consolidated and developed at the EU level with related regulations, standards and funding mechanisms (including new additional and complementary). The consolidation should include emerging actors and sectors as well as new developments such as the liberalization of markets and the developments within the EU in sectors like energy, communications, environment.

The development of an European Security Equipment Market (ESEM) should also include competitiveness as a key issue 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. In general, security could be seen as a big opportunity for European competitiveness in terms of industry and R&T developments, through concrete research projects and more national and European programmes, including more joint and structuring approaches and innovative funding mechanisms. These activities will have to be developed in close cooperation, since the identification of needs by the (end-) users towards the procurement, delivery and support services.

To set a favorable environment to help the emergence for such a market, Europe should foster a set of the procurement policies to drive the innovation in the security field. The Communication (COM(2007) 799 final Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe, outlines a number of issue that should be examined, adapted to cover research and development activities in the security area. As an example, identifying public purchaser in a selected number of areas should be possible, especially if demonstrators are to be developed under the ESRP. In this way, concrete organising the risk benefit and sharing of such procurement could be established.

Security constraints may not only hinder the use of the technology, but also the innovating solutions and products may generate new threats and new vulnerabilities. There will be tradeoffs between public acceptance of the additional constraints and the improvement of the citizen's security.

In general, to improve the citizen's security these "human" related factors must be taken into account. Actions and Member States policies should also take into account the fight against the roots that are generating insecurity. Reducing societal difference and gaps, more communication and education about the cultural and ethnic differences should benefit from the support actions.

The role of Member States will of course have to remain important and taken into account since security is a key issue of national sovereignty, but this should not prevent from more interactions and cooperation at the EU level. New policies and initiatives at European level also generate new opportunities for European security actors, contributing at the end to the security of the European citizen.

STACCATO's recommendations will be disseminated to ESRIF and can also be useful to European and national security R&T programmes.

Finally, further studies are needed for ESEM specificities and common opportunities, to be considered as a key European and national priority.

*

STACCATO Recommendations

on European Security Equipment Market (ESEM)

The main objective is to foster, facilitate, enlarge and consolidate the European Security Equipment Market (ESEM).

These recommendations are based on the STACCATO study, and aim at contributing to the ESRIF (Working Groups dedicated to Security Technological and Industrial Base –STIB-, ESEM and innovation), as well as to other related security activities undertaken at national, European and international level.

There should be particular attention to mid and long term objectives advising European and national level in coherence with ESRAB-ESRIF context and perspectives.

On the basis of the key issues identified during the study, the following recommendations have been identified[1].

[1] Including the ones discussed during the STACCATO Final Forum held in Brussels (European Commission premises) on 24 April 2008.

<u>STACCATO Recommendations:</u>

1. Security as a High Priority for the EU

- *1.1.* It is essential to integrate the creation, enlargement and consolidation of the European Security Equipment Market (ESEM) as an EU priority in the key political initiatives and related documents (communications, green papers, regulations, etc. taking into account the draft Directive on Defence and Security Procurement).

2. Security Needs

- *2.1.* In terms of security needs, it is important to further analyze the threats, to define priorities, taking into account urgent needs, towards a common set of security requirements at EU level. It has been suggested to establish permanent and structured dialogue between customer and supplier, including with the support of simulation tools ("living labs"), through potential EC support actions (process to support the definition of needs).

3. Programmes and Funding Mechanisms

- *3.1.* In order to better use the European funds it's important to create "interdisciplinary" programmes (going beyond research in a more long term and structured, coordinated, integrated approach), including complementary funding mechanisms between EC, Member States and other bodies, among different thematic area such as the best practice already developed in Space (GMES) and in Software Defined Radio, and in development for Unmanned

Aerial Vehicles (UAVs) and Maritime Surveillance, in order to better use the European funds. In this context, there should be possible evolutions with the new EU Lisbon Treaty principles, for more cooperation, synergies and interactions between the (former) pillars.

- *3.2.* To further develop the mechanisms for funding of ESEM at an optimal level :

    - *3.2.1.* taking into account strategic vision for the security in Europe including for R,T&D activities, new integrated innovative and cost-effective services approaches, taking into account the level of “sensitivity” of security missions and technologies, as well as Private Public Partnership -like approach.
    - *3.2.2.* To develop and implement potential complementary funding (to EC FP7 and Industry/RTO contribution, from Member States and/or from other EU bodies such as more joint actions, programmes and associated joint calls, between DGs, themes, EC and other bodies such as FRONTEX, EDA, ESA, etc.).
    - *3.2.3.* To create new budget lines dedicated to security into the EU budget.

- *3.3.* To create dedicated budget lines for the acquisition of equipments, systems and services in the budgets of the European agencies involved in security matters (ex. FRONTEX). The question on a “single European agency” for security procurement was discussed during the Final Forum. This is today not envisaged but could be potentially discussed at ministerial and EC level, future group; related agencies already exist and (for example FRONTEX) could be considered and developed in this direction.

- *3.4.* Various options for cooperation could be envisaged, through pooling, specialization; need a toolbox at EU level (including benchmarking analysis) of available and future solutions.

- *3.5.* There is a clear need to transform research into products, and it could also be done by focusing research activities on the (large scale) demonstrations in the future; beyond research, towards transformation into concrete products with associated effects on security at European level.

- *3.6.* To develop and further integrate innovative and cost-effective service approaches in the field of security.

- *3.7.* To develop capacity of programme management, including contract management, at national and European level.

- *3.8.* In order to further analyse the key issues of the European Security Equipment Marlet, and in particular the procurement aspects, STACCATO recommends to launch a dedicated study on funding and procurement issues in the field of security.

4. Norms, Standards and Regulations

- *4.1.* It's important to foster the development of norms and regulations (and to promote wide dissemination of already existing results and documents) related to European Security Market, between European Commission, Member States, other European Bodies and Industry.

- *4.2.* It's essential to foster Standardization activities in the field of security.

    - *4.2.1.* Dedicated budgets should be increased and oriented more specifically towards the efficient and concrete elaboration and implementation of standards.
    - *4.2.2.* In addition, EU funds allocations (for examples structural funds and external border funds) should be conditioned to the integration and development of a minimum of standardization and interoperability (for

equipments, systems and services, including for maintenance and logistic aspects, between end users and between different countries).

  - *4.2.3.* There is a clear need to define mechanisms to address urgent needs of standardization (consultation processes between customer and supplier).
  - *4.2.4.* Standardization's actors should be involved, with more networks between them, at national European and international level.
  - *4.2.5.* Taking into account the global approach there is the need to support the links between standards, sensitivity and IPRs.
  - *4.2.6.* To make a mapping of laboratories, including tools for certification; towards a "European security label".

- *4.3.* A limited scope proof of concept Technology Watch demonstration should be set up, e.g. under the auspices of ESRIF or other network, containing at least 8-10 actors from industry and academia. To gain the trust of the user community it should use a transparent process, open to scrutiny.

- *4.4.* To establish a list of the more relevant existing standards, technical norms and regulations (i.e. intra-EU transit, security classification, certification…), in order to further propose the potential adaptation supporting the ESEM.

- *4.5.* To develop the role of the EC as a Regulatory Body in charge to address :

  - *4.5.1.* The possibility of defending local policies compatible with the rules organized by the EC should be left to the Member States.
  - *4.5.2.* The impact of the rules in sensitive technologies should be evaluated :
    - ITAR
    - Export regulation
    - Dual use regulation
  - *4.5.3.* Among other possibilities under discussion, it could be interesting, on the basis of the existing lists, to build up a new consolidated list of security products, services and related technologies

in order to facilitate the monitoring by the different actors operating in the domain.

5. European and National Security Networks

- *5.1.* Participation, in the European security network should be rewarded by access to information and online networking tools.

  - *5.1.1.* This would especially benefit SME’s and actors in the new member states. The STACCATO database is a step in this direction, by providing a networking tool which not only helps the ESTIB to self-define itself; it also helps create new partnerships across Europe.
  - *5.1.2.* It is important to organize meetings, workshops and networks at European level, but also at national level for more interactions between local actors, interfacing with European level. National security workshops can also help to prepare position at EU level, using also the EU Working Groups composed by Member States representatives.
  - *5.1.3.* On key priorities, concepts papers should be elaborate at EU level, setting up public-private task forces and defining action plans (examples DG JLS priorities : radiological, chemical, terrorism, border monitoring and control, false documents, maritime surveillance, airspace surveillance).
  - *5.1.4.* After ESRIF there should be a more institutionalised platform for PPP dialogue.
  - *5.1.5.* There is a need to create a platform (potentially through a virtual network) dedicated to test, exploitation of results, review or projects.
  - *5.1.6.* There is a need to further integrate the private security market in addition to the public procurement market.
  - *5.1.7.* Centres of excellence should be promoted, at national, regional and European level, with objectives and concrete programmes.

6. Sensitivity Issues

- *6.1.* STACCATO recommends also to further analyse the meaning of “sensitivity” related to technologies and missions in the Security field (in cooperation with the European Commission, Member States, other Bodies (EC agencies…) and Industry/RTOs). In this contest in fact the meaning does not depend only on the technology and its relation to the missions, but it’s strictly related also to the Context in which the mission will take place and the level of confidentiality (example of criteria: Security of Information, Security of Supply, special security measures, essential interest of MS, …) considered as appropriate by the relevant authorities.
- *6.2.* Data privacy, respect of human rights, acceptance by the public opinion; security – democracy have also to be taken into account.

7. Competitiveness

- *7.1.* In order to ensure competitiveness, it is important to know well the solutions and their potential evolutions. Security is (and will be more and more) a global market, more and more inter-dependent. There is a need to keep advance with regard to competitors (some are already global) - time to market issue - and therefore there is a constant need for investments, R&T activities and standards (here considered as cornerstone, for technology issues, but also cultural, privacy aspects, etc.).

8. Intellectual Property Rigths (IPRs)

- *8.1.* To consider the proper treatment of IPRs of prime importance to the interests of all contracting parties: European Commission (and all relevant Agencies), Member States and Industry, with consequences for the quality of results delivered.

- *8.1.1.* Industry is always looking for flexible “instruments” able to take into consideration the level of funding, the importance of the background brought by industrial stakeholders, the technology maturity and aiming to avoid unnecessary duplication in the European STIB.
- *8.1.2.* IPRs principles ensuring flexibility should be negotiated to treat in priority :
  - Foreground dissemination for further cooperation with Third Parties.
  - Background dissemination (not foreseen during the bid phase)
- *8.1.3.* Patents should also be protected.

* * *

STACCATO Final Study Report –

Executive Summary

Table of Contents

Introduction

Presentation and Main Objectives

STACCATO (**STA**keholders platform for supply **C**hain mapping, market **C**ondition **A**nalysis and **T**echnologies **O**pportunities) started on 15th January 2007 as a European funded supporting activity under the Preparatory Action for Security Research (PASR) call 3 / 2006 and lasts 16 months. It is a follow up activity of SeNTRE (Security Network for Technological Research in Europe) which was a supporting activity funded under PASR call 1 / 2004.

STACCATO supporting activity aims at proposing methods and solutions for the creation of a security market and a structured supply chain in Europe. In line with ESRAB (European Security Research Advisory Board) recommendations, it goes beyond research needs and gap analysis already undertaken through efforts supported by PASR, by identifying implementation measures.

To this end, STACCATO:

- maps existing competencies in the EU-27, highlighting particularly the role of the SMEs in order to integrate their innovation potential and examine ways to effectively undertake a coordination of the European Security and Technological Industrial Base (STIB),

- proposes a methodology for a technological watch,

- analyses the conditions and propose recommendations to develop a common European Security Equipment Market (ESEM), by identifying common needs, taking into account regulatory issues and coordinating with regional, national, international and EU security research programmes.

These activities are supported by an enlarged multi-sector stakeholders platform composed of users, industry, SMEs, academia and think tanks of the EU-27 based on the SeNTRE and ESRAB experience.

The Origin

STACCATO built up on the legacy of "SeNTRE" (Security Network for Technological Research in Europe) a previous supporting Activity (PASR call 1 / 2004) which delivered in March 2006 a final report on « Strategic Research Plan for Security ».

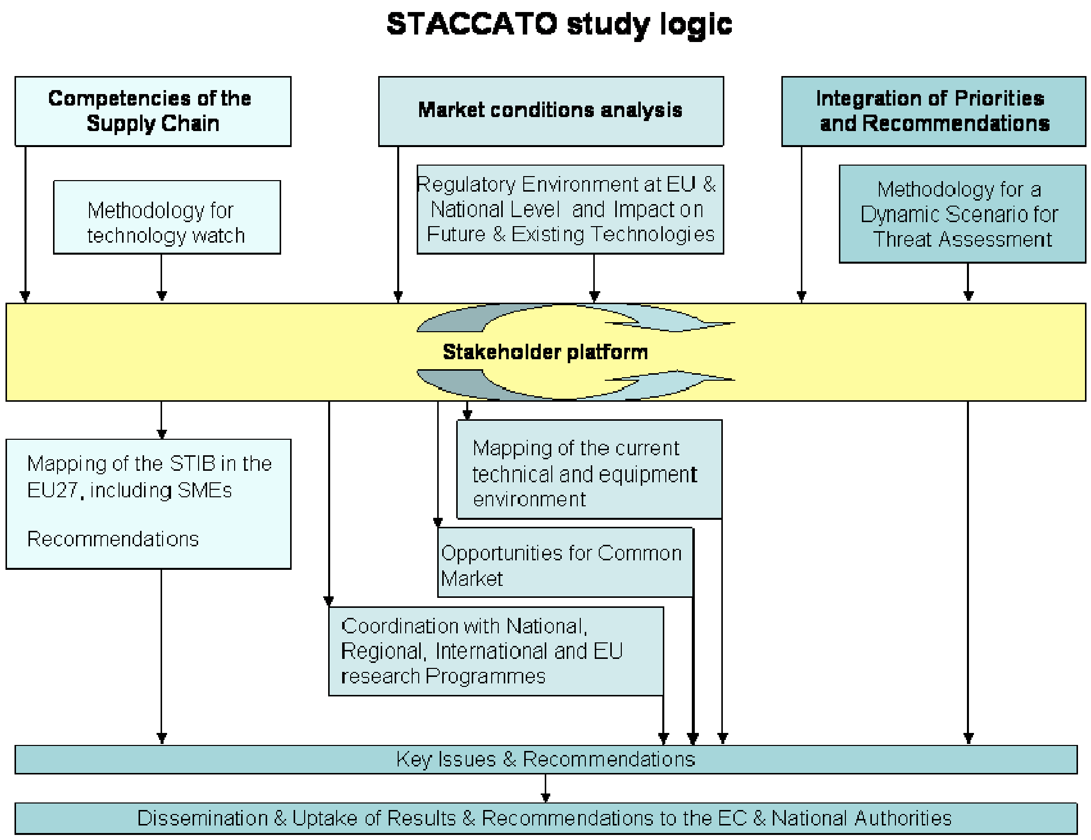
The added value provide by SeNTRE was an organised Community of Security Stakeholders across Europe, a short-, medium- and long-term capability and technology requirements and an unique Security Taxonomy (further improved in STACCATO (*see hereafter*).

STACCATO starting point raised form the consideration of needs such as the need to link research results with policy strategies and end users requirements, to understand the existing environment for security applications in Europe, to enhance a European Security Equipment Market (ESEM) and to identify a European Security Technological & Industrial Base (ESTIB).

STACCATO was therefore tailored to go beyond the SeNTRE results by identifying concrete recommendations.

The STACCATO Study Logic

STACCATO is implemented following the rules of an industrial project. Beside the project support activities (Work Package – WP – 1) running through the whole duration of the project, the implementation logic will be as indicated in the figure below.


STACCATO study logic
Competencies of the Supply Chain
Market conditions analysis
Integration of Priorities and Recommendations
Methodology for technology watch
Regulatory Environment at EU & National Level and Impact on Future & Existing Technologies
Methodology for a Dynamic Scenario for Threat Assessment
Stakeholder platform
Mapping of the STIB in the EU27, including SMEs
Recommendations
Mapping of the current technical and equipment environment
Opportunities for Common Market
Coordination with National, Regional, International and EU research Programmes
Key Issues & Recommendations
Dissemination & Uptake of Results & Recommendations to the EC & National Authorities

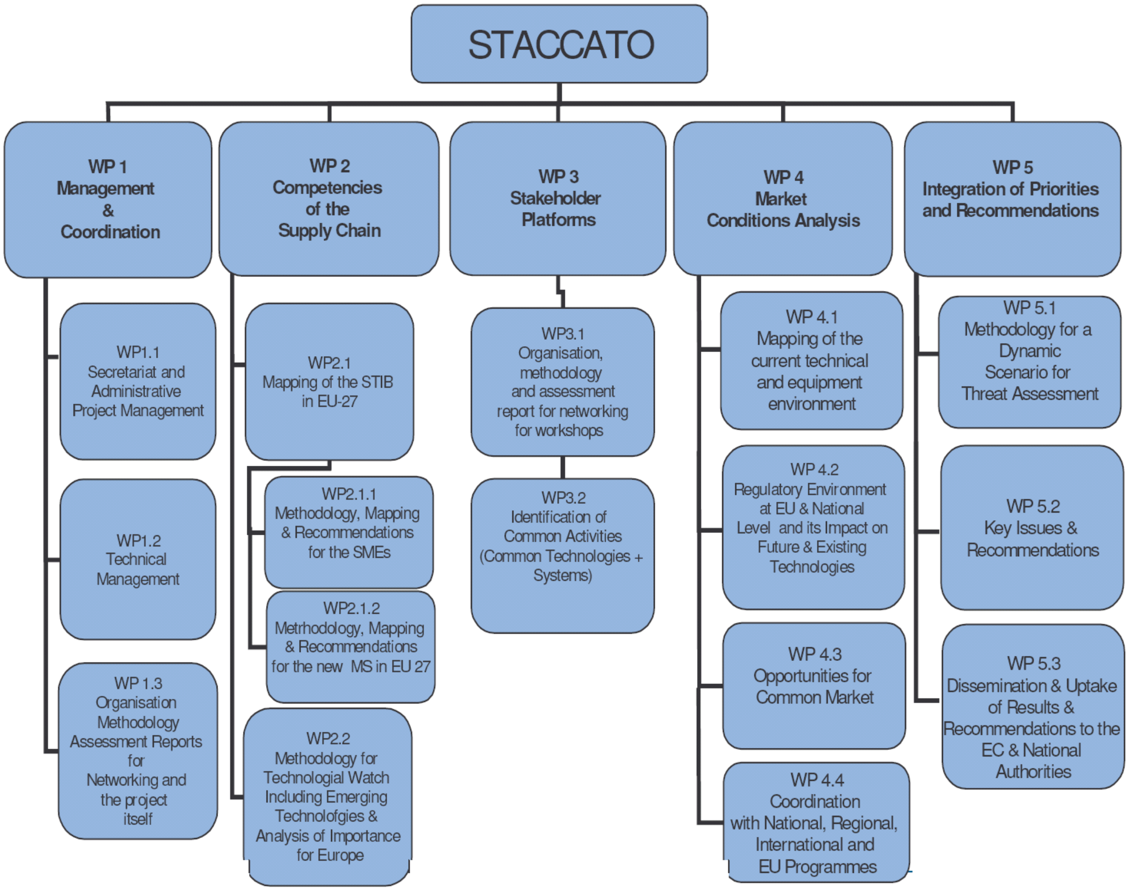
The first tasks of the project are the definition of the methodology for the STIB mapping and the scenarios preparation, the regulatory environment analysis and the preparation of the stakeholder platform work and workshops.

The stakeholder platform contributes to a preliminary identification of common needs, systems and opportunities for common market. It contributes to the STIB mapping and to the inventory of existing or planned research programmes.

These inputs are gathered and reviewed to address key issues and draw recommendations to be discussed and disseminated, according to their level of confidentiality with the stakeholder platform participants, EC and national authorities and the STIB.

The STACCATO Work Packages Structure

The project was structured alongside five work packages (WP).


STACCATO
WP 1 Management & Coordination
WP1.1 Secretariat and Administrative Project Management
WP1.2 Technical Management
WP 1.3 Organisation Methodology Assessment Reports for Networking and the project itself
WP 2 Competencies of the Supply Chain
WP2.1 Mapping of the STIB in EU-27
WP2.1.1 Methodology, Mapping & Recommendations for the SMEs
WP2.1.2 Metrhodology, Mapping & Recommendations for the new MS in EU 27
WP2.2 Methodology for Technologial Watch Including Emerging Technolofgies & Analysis of Importance for Europe
WP 3 Stakeholder Platforms
WP3.1 Organisation, methodology and assessment report for networking for workshops
WP3.2 Identification of Common Activities (Common Technologies + Systems)
WP 4 Market Conditions Analysis
WP 4.1 Mapping of the current technical and equipment environment
WP 4.2 Regulatory Environment at EU & National Level and its Impact on Future & Existing Technologies
WP 4.3 Opportunities for Common Market
WP 4.4 Coordination with National, Regional, International and EU Programmes
WP 5 Integration of Priorities and Recommendations
WP 5.1 Methodology for a Dynamic Scenario for Threat Assessment
WP 5.2 Key Issues & Recommendations
WP 5.3 Dissemination & Uptake of Results & Recommendations to the EC & National Authorities

WP 1 was devoted to **Management and Coordination** and assured therefore the Secretariat support and Administrative Project Management, the technical Management in terms of coordination of technical activities, the organisation, methodology and assessment report for networking for the project itself and assured the inter project coordination between STACCATO and SECURE SME.

WP 2 – Analysis of Competencies of the Supply Chain – deals with the mapping of the competencies of the European Security Technological and Industrial Base (STIB) (covering all relevant technologies, technical and industrial players in all the EU-27 Member States with specific attention to SME), recommendations for new member States and methodology for technology watch.

WP 3 – Stakeholders Platform – is devoted to the enlargement and sustainability of the existing SeNTRE networks of users, industries and academia with representative of SMEs and the new EU MS and other sectors like bio-technology, biometrics ecc... , the identification of common activities and priorities at European level and the contribution to the STIB and technical equipment environment market, technology gaps and preliminary recommendations.

WP 4 – Market Condition Analysis – aims at providing a close analysis on the security market conditions, looking to the supply demand by mapping the existing and planned equipment systems in EU, the current European regulatory environment and the on-going and planned research projects and the identification of opportunities for a European Common Market.

WP 5 – Integration of Priorities and Recommendations – is devoted to the elaboration of a methodology for a dynamic scenario for threats and vulnerabilities assessment, identify technological challenges and first implementation of security research activities based on the integration of priorities identifies during the study, to propose recommendation to structure and strengthen the ESTIB and to support the common market development in Europe and the identification of a methodology for the dissemination and uptake of results through a final Forum and the Stakeholders Platform.

The STACCATO Study Outputs

The output of STACCATO is:

- A strategic **analysis of the key competencies**, including those of the SMEs, in the Europe of the 27 coupled with a **methodology for a technology watch** and monitoring of worldwide trends in security-related technologies.

- The refined security technology taxonomy, the **"STACCATO Security Taxonomy"**, using the unique SeNTRE security technology taxonomy as a starting point.

- A **multi-sector public private network** to support an efficient security dialogue in Europe in key areas such as Bio, Biometrics, Transport, Energy,…, involving all stakeholders (users, regulators, Industry and services, SMEs, RTOs, Academia and Think Tanks,…).

- An **analysis of the market conditions**, including an understanding of the regulatory environment at EU and national level and its impact on the existing and future technologies and systems.

- A detailed report presenting a **methodology for a dynamic scenario for threats and vulnerabilities assessment**, technological challenges, priorities and recommendations for the future as well as short and long term R&D needs along with the FP7 and the national programmes' timescales.

- **The « STACCATO Database »** providing an overview on the EU Security competences that can be used by all registered bodies and allowing the information to be displayed in a logical format i.e. by technologies or geographical location

- The Database will remain in operation following the conclusion of the project. The Database is accessible through the ASD website (www.asd-europe.org) or directly through the link http://staccato.jrc.it/staccato

The Partnership

COORDINATOR	A S D
INDUSTRY	DASSAULT AVIATION DIEHL EADS EADS ASTRIUM EDF FINMECCANICA INDRA SAGEM SECURITE THALES
RTOs	ARSENAL CEA FOI IABG TNO VTT
THINK TANKS	FRS IAI
ASSOCIATIONS	EBF EUROPABIO
EC	JRC

Contribution to other Initiatives

STACCATO contributes its main results to other initiative relevant in the field of security research. Among them is the European Security Research and Innovation Forum (ESRIF). STACCATO contributes its Security Taxonomy to be used as a common language of understanding, the mapping of the European STIB and the Recommendations on ESEM. STACCATO anticipates actively to two ESRIF working groups devoted to “Innovation” and “Foresight and Scenarios”.

The results of STACCATO are also to be contributed to future research activities, to the 7th Framework Programme (FP7) and national programmes in the field of security research.
The STACCATO Security Taxonomy has been contributed to ISO. At the ISO/TC 223 meeting in Seoul it has been agreed to form an ad hoc group tasked to conduct a study for 6 months on "Societal security technological capabilities" (Resolution 60).

The overall objective is to foster the security market in Europe.

Presentation of the Structure of this Report

This final project report consists of three parts:

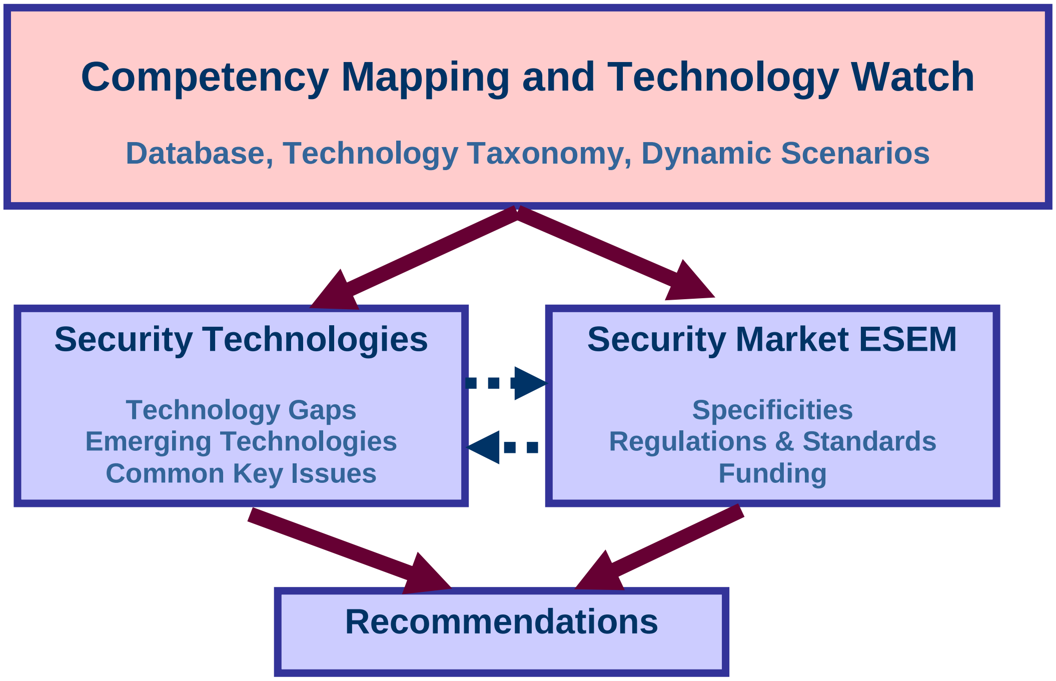
- **The first part** is dedicated to the presentation of the “tools” identified and developed within the STACCATO study, in particular the competency mapping and methodology for technology watch, the database, the technology taxonomy, the report on methodology for dynamic scenarios and threat assessment and also the stakeholders platforms.

On the basis of these STACCATO tools, two other parts generate analysis and recommendations on technology and on market issues

- **Part 2** will present the key security technologies and issues identified: technology gaps, emerging technologies and common key issues.

- **Part 3** will focus on the market issues, including national security regulations and research programmes, and in particular the following points towards opportunities for common market: the specificities of the European security market, the regulations and standards and the funding issues.

Finally, this report will present the main conclusions of the STACCATO project, and in annex the synthesis of the priority research areas.



Part 1. The STACCATO “Tools”: Mapping of Competencies and Technology Watch

Recommendations for how to introduce a technology watch, and for which primary purposes, have been elaborated. It should primarily be tasked with supporting R&D policy decisions on National and European levels and work through the mobilisation of existing actor networks in a new transparent framework.

For the sake of promoting networking and creating a tool for the continuous mapping of the European STIB, an online database was fielded. Its core consists of the new security taxonomy which will act as a key tool for dialogue and visualisation of the various parts of the STIB. This Database will continue in operation, and will grow until it spans the entire STIB in EU and associated nations, helping policy-makers understand the market, and helping the market actors to form connections and learn from each other.

1.1. Mapping of Competencies and Database

An online database has been created in the framework of STACCATO. In this database European security actors are encouraged to register on behalf of the organisation they represent. The database is built on top of the new STACCATO security taxonomy. When an organisation is registered in the database the registering person selects capabilities according to the taxonomy which best match the competencies of his/her organisation.

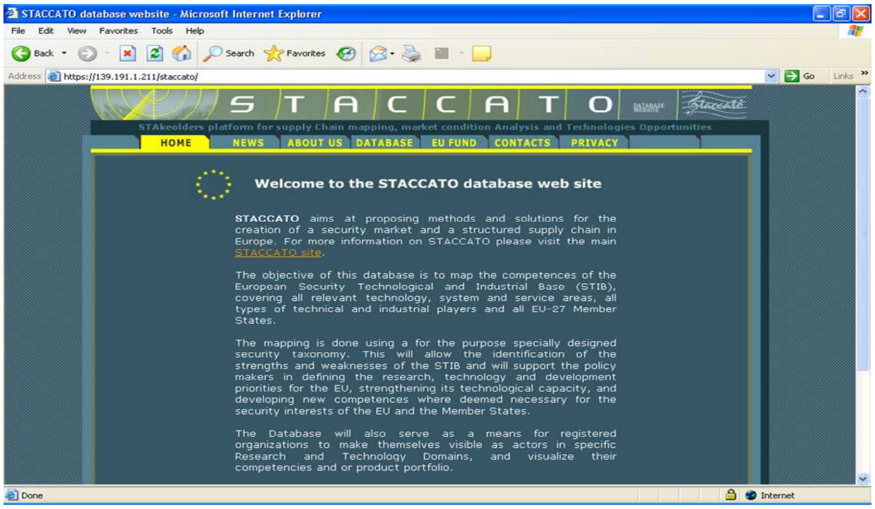
Thus for each registered organisation, being it an SME, an University etc, its security competencies will be mapped. As an incentive to register, registered organisations can access the contents of the database, for example by using taxonomy terms to find partners in a specific security domain.

This tool, which primary purpose is the mapping of the European Security Technological and Industrial Base (ESTIB) using the security taxonomy developed by STACCATO, will remain in operation beyond the end of the project and will also serve as a networking tool where potential partnerships/clients/suppliers in the European security field can be quickly located and their potential contributions and needs easily ascertained. This ICT network support tool will help to keep alive the network of public and private stakeholders established in STACCATO.

In return for registering, the new members are, after scrutiny that they fulfil the ESTIB criteria, granted a personal login to the Database. The use of a new security taxonomy as the core of the online database has the advantage of helping all users share and use a common semantics and common language, regardless of their organizational or linguistic background. In this way a very basic networking tool has been fielded, capable of bringing its users one step closer to bringing together SME's, Industry, Academia, Government and Research Institutes in Europe.

Interested stakeholders can register either via ASD website: www.asd-europe.org
or directly through http://staccato.jrc.it/staccato

STACCATO Database – 1 (example)


STACCATO database website - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://139.191.1.211/staccato/
Go Links
STACCATO
STAkeolders platform for supply Chain mapping, market condition Analysis and Technologies Opportunities
HOME
NEWS
ABOUT US
DATABASE
EU FUND
CONTACTS
PRIVACY
Done
Internet

Welcome to the STACCATO database web site

STACCATO aims at proposing methods and solutions for the creation of a security market and a structured supply chain in Europe. For more information on STACCATO please visit the main STACCATO site.

The objective of this database is to map the competences of the European Security Technological and Industrial Base (STIB), covering all relevant technology, system and service areas, all types of technical and industrial players and all EU-27 Member States.

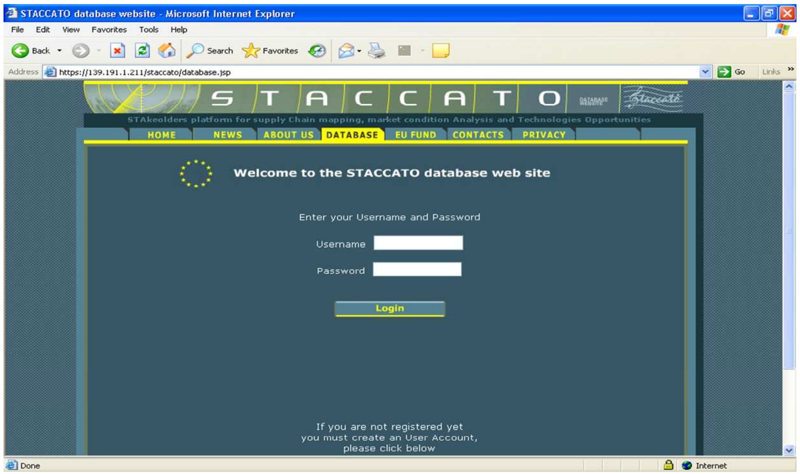
The mapping is done using a for the purpose specially designed security taxonomy. This will allow the identification of the strengths and weaknesses of the STIB and will support the policy makers in defining the research, technology and development priorities for the EU, strengthening its technological capacity, and developing new competences where deemed necessary for the security interests of the EU and the Member States.

The Database will also serve as a means for registered organizations to make themselves visible as actors in specific Research and Technology Domains, and visualize their competencies and or product portfolio.

Slide 14

Figure 1.STACCATO Database main page. It contains general project information. Navigation between the database pages can be conducted using the menu on top of the page.

STACCATO Database – 2 (example)


STACCATO database website - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://139.191.1.211/staccato/database.jsp
Go Links
STACCATO
STAkeolders platform for supply Chain mapping, market condition Analysis and Technologies Opportunities
HOME
NEWS
ABOUT US
DATABASE
EU FUND
CONTACTS
PRIVACY
Login
Done
Internet

Welcome to the STACCATO database web site

Enter your Username and Password

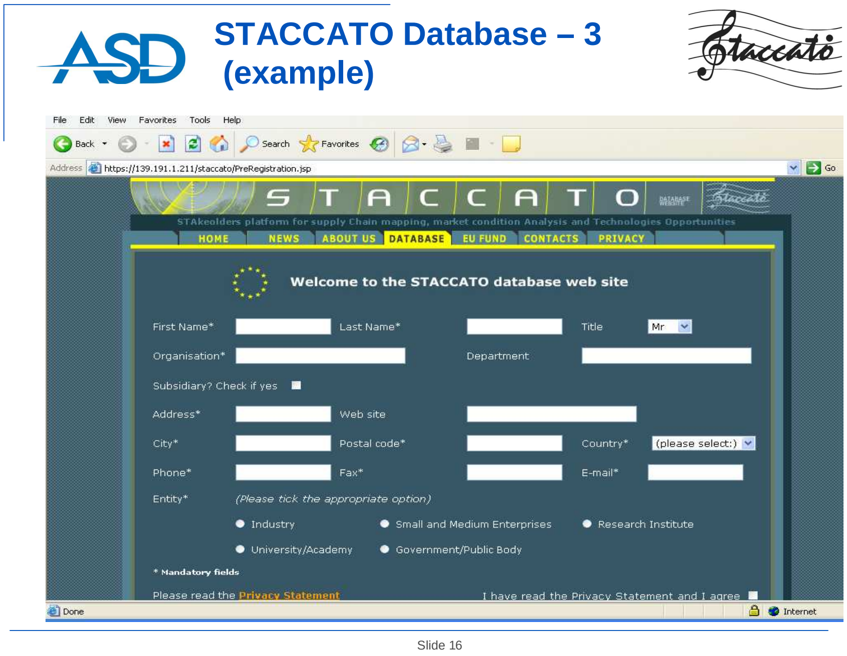
Username

Password

If you are not registered yet
you must create an User Account,
please click below

Slide 15

Figure 2. STACCATO Database "Login page". Each user has its own personal login and password, enabling the modification of organisation information and the conduct of searches on the contents of the database.



STACCATO Database – 3 (example)

File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://139.191.1.211/staccato/PreRegistration.jsp
Go
S T A C C A T O
STAkeolders platform for supply Chain mapping, market condition Analysis and Technologies Opportunities
HOME
NEWS
ABOUT US
DATABASE
EU FUND
CONTACTS
PRIVACY
Done
Internet

Welcome to the STACCATO database web site

First Name* Last Name* Title Mr

Organisation* Department

Subsidiary? Check if yes □

Address* Web site

City* Postal code* Country* (please select:)

Phone* Fax* E-mail*

Entity* *(Please tick the appropriate option)*

○ Industry ○ Small and Medium Enterprises ○ Research Institute

○ University/Academy ○ Government/Public Body

* Mandatory fields

Please read the Privacy Statement I have read the Privacy Statement and I agree □

Slide 16

Figure 3. STACCATO Database, contact information page. Here the information necessary for identifying the organisation and it's designated contact can be inserted or modified.

It is evident that the STACCATO database is not a targeted survey. It is a ongoing operating tool whose contents are continuously updated by the users, all of which are volunteers who have classified themselves (within limits, the administrators is free to reject registration requests) as part of the European security market. Their main incentive for volunteering this information is networking, the ability to be found, and to find other players in the security market. This will also ensure that the contents of the database stay up to date and provide a continuous, near real-time view of the market.

1.2 Methodology for Technology Watch

The European Union strives to enhance the innovation and competitiveness of its Member States and has in recent years increasingly focused on enhancing the European Security. A European Technology Watch (ETW) will support both these goals, by helping clarify the European Security Industry Structure, and by identifying market growth potentials and deficient industry factors.

The task of an ETW will be to observe, track, filter out and assess potential technologies from a very wide field. Life-cycles of new technologies are becoming shorter. As a consequence, the process of introducing them from R&D to standardisation and markets must be fast, flexible and practical.

In order to cover all thematic fields and lower the risk of missing potentially disruptive technologies, it is suggested to combine ‘hard’ methods such as literature study with ‘soft’ methods, such as interviews, expert panels, questionnaires, workshops, etc. The efficiency of an ETW will be based on its ability to get broad input, of varying precision and partiality and reflecting the international bandwidth of innovation.

In order to be truly useful, an ETW must be able to gain the trust and acceptance by all its stakeholders and target groups. Outmost care must be taken to ensure that there is no suspicion of commercial or political bias in its output. The key to this is transparency and impartiality, to meticulously link individual conclusions to their related sources.

Two Potential main User Groups for a European Technology Watch (ETW)

A crucial step in the creation of an ETW is to clearly define who the users are. The specific user requirements will determine both the form and function of any ETW. There may be large differences between mechanisms required for policy support and those needed for industry support. In order to fill all potential needs this may require several distinct ETWs working in parallel, optimised for differing purposes and using different methods. Private technology watch mechanisms are already in place by many industry and other market actors, and these may well question or oppose the need for and the conclusions of an ETW. There exist, however, two target groups that would significantly benefit from an ETW: SMEs and policy makers on the national and European level.

For the sake of strengthening the European market competitiveness policy makers require policy support by *monitoring developments* within and beyond the EU to identify important research and innovation areas, offering a comprehensive and realistic picture including the identification of deficient support factors, such as possible regulatory gaps. Moreover, often the ultimate goal of policy measures is hard to define, as well as which policies will best lead to this goal. For this reason, *policy impact assessment* tools and methods for obtaining rapid feedback on the effect of policy measures, and particularly on any unexpected negative side-effects, have a clear value.

Another requirement of policy makers may be the need for *technology warnings.* This entails monitoring evolving technologies not only for their economic potential but also for their potential security value or threat, and possibly also their political implications. Technologies that may have negative consequences on society need to be monitored as they appear and mature. Negative effects are here used both denoting a direct threat potential such as e.g. small and effective EMP generators, or more indirect threats, such as disruptive technologies that in themselves are no danger but which when widely introduced may generate new security liabilities unless action is taken early enough to ensure mitigation.

And finally, there is the need to get a *definition of critical components* and equipment which could negatively affect European economy and security if internal or external supply was cut off or degraded, i.e. by essential foreign dependencies.

The *methodology* of an ETW should not be limited to identifying new potential technologies and services and surveying the current situation, it should also include mechanisms for determining which incentives are most important for stimulating their growth in the European market, which blocking mechanisms there may be in place that would hinder the adoption of the technology, and how to mitigate each blocking mechanism.

The means available for policy makers at the European level to make use of information gathered through ETW and other sources in order to promote innovation and security can range from networking and facilitating partnerships, (i.e. working to bring industry alliances together around common goals and roadmaps, bringing users together around common requirements), to more direct approaches (such as directing research through direct funding, tax incentives, reformulating regulations, promoting the creation and adoption of new standards, and increasing university funding in certain educational topics to increase the human capital available).

Small and Medium-sized Enterprises (SMEs) require more individual support for their respective fields of activity. Mostly, SMEs are lacking the resources to conduct their own competitive technology watch. ETW support would help them keep track of technical developments, find innovative solutions, possibly from outside their primary technical sector, and speed the transfer from R&D to market. They do not only need to know about upcoming technologies but their main interest is technology niches and technology gaps that may offer a chance for their innovative ideas and products.

One specific example of an innovation booster for SMEs can be found in the US Small Business Innovation Research (SBIR) program which provides an opportunity for small, high technology companies and research institutions to participate in Federal Government sponsored research and development efforts in key technology areas.

Special emphasis should be accorded to SMEs coming from the New Accession Countries (NACs). They usually do not work in clusters like Western SMEs do, which makes it harder for them to be integrated and become known market players. Including them in an ETW process would be a way to offer them insight in upcoming developments and make their own competencies visible.

Building a European Technology Watch on Existing Structures and Actors

An ETW should not reinvent the wheel but make use of existing proven methodologies, structures, networks and actors. It is advisable to develop a co-ordinated Technology Watch network with academia, research institutes and other entities, structured according to their technological specializations and with appropriate interactive tools in order to respond quickly to requests for technology feasibility advice, technology performance advice, state of the art, risk assessment, etc. Additional partners in the network will provide added value by reviewing and assessing the results.

In a next step, a steering board should be created in order to coordinate the work and disseminate the results. The steering board could perform meta-analyses, putting together several studies and impact analyses, in order to identify the political implications. As more funding becomes available, studies of all kinds can be commissioned by the steering board, and performed by the ETW partners in collaboration.

Virtually all European countries have for many years conducted Technology Foresight exercises on a national level. The purpose has been to determine the expected development of society perhaps 10 years or more into the future as regards health, services, ICT etc, using scenario-drafting and experts consultations. From these estimates it is aimed to develop long range national strategic goals for R&D and other societal important policies.

While a Technology Watch for security would have more near term focus, other primary aims, and a different working methodology, the networks established for foresight on a national level could and should be leveraged. They constitute an important link with the national political levels for dissemination of the results, are capable of bringing in a balanced set of regional interest groups as well as constitute a significant labour pool for the day to day activities of the ETW. Coordinating the national efforts will provide advantage to all stakeholders since the combined effort will be able to look wider and yield results not possible on a purely national level without unreasonable effort and expense. Coordination can be achieved by leveraging supranational networks such as the ones formed in ESRIF.

1.3 STACCATO Security Taxonomy

In order to have a useful common language tool not only for the STACCATO consortium and security equipment and system providers but also for interfacing with end users, the STACCATO taxonomy has been elaborated.

The SeNTRE taxonomy has been taken into consideration for the mapping of European competences in two ways:

1. Technology codification
2. Product/service codification

The five levels of the SENTRE taxonomy have been renamed in relation to the elaborated definition, aiming at taking into consideration user and supply oriented taxonomy as well.

Definitions have been therefore elaborated and a correlation has been done with ESRAB functions, especially for what concern user oriented part.

On the basis of the new Definition the existing taxonomy has been structured along seven sections and has been simplified in order to make it a genuine working tool for the Stakeholders' platform work and workshops.

The seven top level/sections of STACCATO taxonomy are:

- **(I) Technologies and Components**
- **(II) Equipments 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**

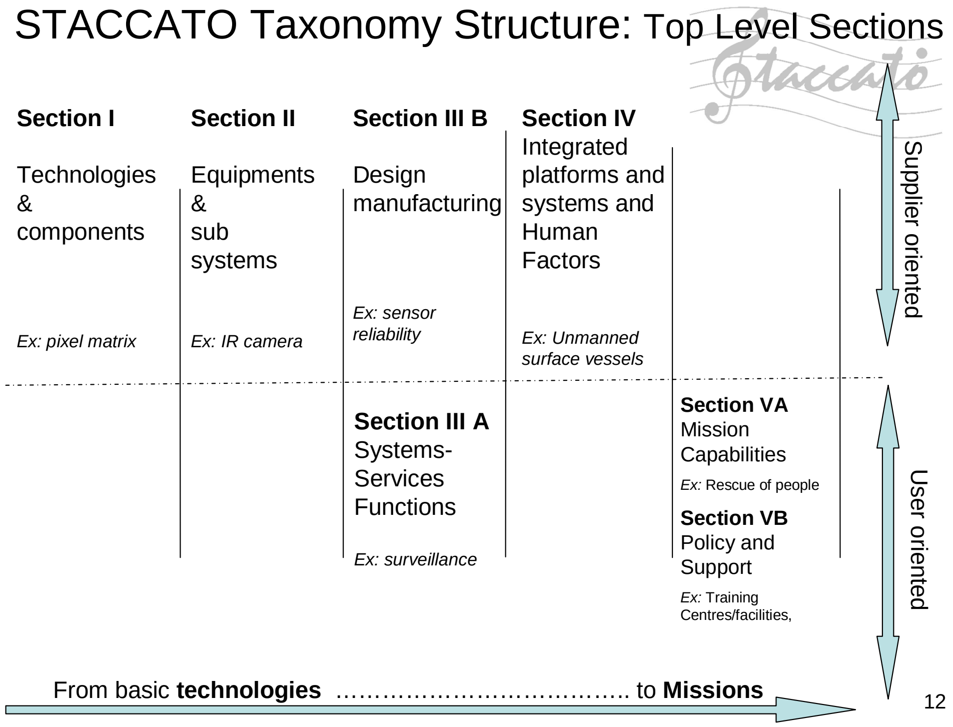
The seven top-level sections are provided with roman numbering for traceability; no internal hierarchical ordering between them is implied.

The SeNTRE/STACCATO taxonomy is dual-use taxonomy for the domains of security and defence. As such it contains also items from the so-called WEAG taxonomy which was developed for the defence domain. However, the WEAG taxonomy was aimed at Research & Development.

The STACCATO taxonomy forms also the basis for the STACCATO data base in which we aim to capture both the systems and subsystems offered by the supply side and the requirements of the user side.

Therefore the need is to have entries which can be used by the representatives of suppliers to indicate their capabilities and users to identify their needs.

The descriptions on the various levels do meet this need.



STACCATO Taxonomy Structure: Top Level Sections

Section I Technologies & components. *Ex: pixel matrix*

Section II Equipments & sub systems. *Ex: IR camera*

Section III B Design manufacturing. *Ex: sensor reliability*

Section IV Integrated platforms and systems and Human Factors. *Ex: Unmanned surface vessels*

Section III A Systems-Services Functions. *Ex: surveillance*

Section VA Mission Capabilities. *Ex:* Rescue of people

Section VB Policy and Support. *Ex:* Training Centres/facilities,

1.4 Dynamic Scenarios

In the early history of future studies a scenario was a “story” generating a possible future starting today and moving forward through a number of formative events. Due to uncertainties concerning events and the outcome of these it was often considered necessary to create several different scenarios. The scenarios were often used as backdrops against strategies for your organization (company, defence…) were analyzed. The scenarios were different for different organizations. Events having a major impact on an organization are very organization dependent.

For different reasons the term scenario has been changing its meaning from the “story” to the end-state. Scenarios have developed to mean possible futures in which your organization can find it self. Futures described in terms relevant to your organization’s need for constructing strategies.

Based on plausible scenarios it is possible to estimate the capabilities required to meet the challenge posed by the scenario, and how best to use those capabilities, as well as identify possible shortcomings in current abilities. Thus, scenarios are to be considered as a methodology tool for analysis of threats, needs, related technology solutions and their use.

The types of scenarios just described have been used extensively, missing however the dynamics of the courses of events and the successive interplay between different interacting actors and factors. To gain further insights you could use dynamic scenarios as a complement to today’s standard scenarios. The application in our case is on terrorism.

Actors:

- Governments, agencies…
- The terrorists
- The ordinary citizens. (the “audience” of the deeds).

Factors:

- The balance between protections of national security and protection of civil liberties.
- The technical development.
- The development of infrastructure.
- The impact of the internet
- The mass media
- Globalisation.
- The changing demand of security.
- Root causes.

Just commenting on one factor as an example:

Development of new technologies could facilitate countermeasures against terrorism (defensive means). New technologies could however also give the terrorists access to new more effective means (offensive). As in war there is a contest between measures and countermeasures. A very complicated contest since there are many types (very different) of measures and countermeasures. There are also several dimensions of possible impacts (casualties, economy, disturbances…).

Examples of defensive means:

- A more robust technical infrastructure (IT, energy…)
- A better defence against bio-agents by better detectors (real time detection and identification) and better vaccines and medications (faster to produce, multi-purpose…)
- Improved technical means in the intelligence area.

Examples of offensive means:

- New explosives (easier to produce and handle and with higher effect)
- New “cyber war” – concepts
- New methods to produce and spread bio-agents.

Technology forecasts combined with some sort of action-reaction gaming could be supportive to the analyses.

<u>To summarize concerning dynamics:</u>

The terrorists, at least part of them, seem to be agile and adaptive. For this reason it is important to be able to counter yesterday's threats as well as tomorrows. A three part strategy is necessary:

- Countermeasures against the repetition of attacks which have already taken place.
- Countermeasures of a more generic type i.e. they provide countermeasures against several threats. An example could be a good crisis management capability.
- Countermeasures against a clever selection of low – probability – high – consequences – cases.
- An agile (reacting on early warnings etc.) defence against threats towards which no countermeasures have been prepared (for economic reason you cannot prepare for all possible threats even if it would be possible to foresee them).
- Develop tools to simulate the dynamic relationship between "offence/defence" as the "modern terrorist" will want to anticipate the defensive "societal" response and will try to include it in its advanced planning of attacks.

To be able to form a viable counterterrorism strategy it is necessary to understand the dynamics of terrorism[2].

[2] Cronin A.K.: Ending Terrorism. Lessons for defeating al-Qaeda. *ADELPHI PAPER* 394, IISS, ROUT LEDGE 2008.

1.5 Stakeholders Platform

In order to enlarge and sustain the SeNTRE network of users, industry and academia with representatives of Small and Medium Enterprises (SMEs), new EU Member States and other sectors (such as energy, bio-technology, biometrics etc...) and contribute to European STIB and Technical and equipment environment mapping, a series of technology workshops and interviews has been conducted focusing on the identification of technology gaps, of common needs and opportunities for common market, and of concrete recommendations for the future.

Furthermore, a methodology for organizing and networking in a stakeholders' platform framework has been elaborated. The workshops included Industries (large and SMEs), RTOs, think tanks, academia and users participation. Particular attention was devoted to the broadest possible participation from all EU Member States.

The list of STACCATO workshops; indicating the topic, the title, the coordinator and the dates they were held, is presented below:

List of workshops

Date	Mission	Location	Coordinator
04/06/2007	Critical infrastructure and network protection / cyber security	Vienna	Arsenal Research
06/06/2007	CBRNE, including decontamination	Brussels	CEA, Europa Bio
11/06/2007	Interoperability	Brussels	FOI
12/06/2007	Crisis Management	Brussels	VTT
25/06/2007	Human factors	Ottobrunn/Munich	IABG
18/09/2007	Wide area surveillance	Ispra	Finmeccanica, TNO
19/09/2007	Movement of People	Ispra	EU Biometrics Forum
20/09/2007	Movement of Goods	Ispra	JRC

13/02/2008	2nd CBRNE workshop (focus on Bio-preparedness).	Brussels	Europa Bio, CEA
5/03/2008	Technology Watch Workshop	Brussels	Arsenal Research, JRC

For the Standardisation mission, there was no dedicated workshop organised since the consortium was in close contact with the CEN and obtained valuable material from the relevant CEN working group.

After the first set of workshops in June and September 2007, instead of organising a 2nd set of workshops in the beginning of 2008 as initially planned, it was considered as more efficient at that stage of the project to conduct targeted interviews with public stakeholders and European agencies/ associations (apart from the CBRNE topic, for which a 2nd specific workshop was organised).

As a result, interviews were organised with the following stakeholders in the EU Member States in the period December 2007-March 2008 :

- Austria
    - *ASFINAG (Austrian highway provider)*

- Germany
    - *DEUTSCHE BAHN AG (German Railways)*

- The Netherlands
    - *NL Coastguard*
    - *NL Royal Marechaussee*

- Finland
    - *Finnish Ministry of Interior*
    - *Finnish Frontier and Coast Guard*
    - *Finnish Crisis Management Centre*

- *Finnish Rescue Force/ Emergency Centre Helsinki*

- Sweden
  - *Swedish Rescue Services Agency*
  - *Swedish Emergency Management Agency*

- Latvia
  - *Ministry of Interior (State Fire and Rescue Service)*
  - *Ministry of Defence (Crisis Management and Mobilizations Department)*
  - *Public Health Agency Riga*
  - *Ministry of Health (Disaster and Emergency Medicine Centre)*

- Lithuania
  - *Ministry of Interior (Fire and Rescue Department)*
  - *Ministry of Defence (Crisis Management Centre)*

- Estonia
  - *Estonian Ministry of Interior (Rescue and Crisis Management Department)*

- UK
  - *MBDA Human Factors Unit*

- Malta
  - *Malta Maritime Authority*

The following agencies/organizations were also interviewed:

- FRONTEX
- EU Satellite Centre
- EDA
- Eurocontrol

An interview was also organised in Switzerland with the Security Infrastructure and Crisis Management department of SBB (Schweizerische Bundesbahnen / Swiss Railways).

Concerning the workshops/interviews organised in the framework of STACCATO WP3, the following remarks can be made:

- Participants invited to the workshops represented several sectors: Industries, (large and SMEs), RTOs, think tanks, consultancies and public stakeholders.
- Participation varied depending on the workshop (from 8 participants in the Interoperability workshop to 55 in Wide Area Surveillance).

- In some workshops there were very few or no users. Industry (big and SMEs) represent the majority of the participants in the workshops. Indeed, it was difficult to convince public stakeholders to participate and be active in the workshops. However, a particular attention was given when organising the WP3 targeted interviews so that relevant users/public stakeholders (also form new Member States) were identified and convinced to participate in the procedure.

- Key issues discussed in the workshops and interviews were :

  - *Capability needs/gaps*
  - *Technology gaps/bottlenecks*
  - *Emerging or breakthrough technologies*
  - *Problems across the supply chain*
  - *Regulatory issues*
  - *Common market Issues/Opportunities*

I

Part 2. STACCATO – Identification of Technology Priorities.

The objective of this chapter is to present the key results from the stakeholders' platform consultation concerning the security technologies aspect. It focuses on technology gaps/bottlenecks, emerging technologies and priority research areas identified in 9 security missions/areas. A list of common technology issues to all missions is also presented.

2.1. Presentation of the 9 Mission Areas

STACCATO has identified 9 missions -both demand-driven and supply-chain driven-corresponding to an equal number of technological areas with a homogeneous community of experts and users. These missions were selected on the basis to be comprehensive enough in order to facilitate the contact with a homogeneous community of public and private stakeholders and receive concrete feedback from them.

The missions/areas identified in STACCATO 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*

This list of missions is in line with SeNTRE, ESRAB and FP7 security work programmes and has also contributed to the definition of ESRIF missions.

2.2 Common Key Technology Issues

The table presents the technology gaps/bottlenecks common to all STACCATO missions (with the exception of standardisation mission being handled a different way).

Technology Gaps/ Bottlenecks
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

2.3 Detailed Technology Issues per Mission Area

The table below presents the key technology issues (technology gaps/bottlenecks, emerging technologies and priority research areas) per STACCATO mission.

Mission Area	**Key Technology Issues**
	Technology Gaps • Architecture (long life cycles of platforms require that components with new security capabilities must have

Critical Infrastructure and Network Protection / Cyber Security	the option to be integrated into existing environments). • Standardisation: interconnectivity of systems • Fault tolerant systems • Technologies supporting assessment routines • Need for improvement of video surveillance in railway parking areas and generally in public spaces, looking at real-time analysis and developing intelligent systems using advanced analysis methods like pattern recognition The mobile video surveillance units should work autonomously with a reliable but simple energy supply • Signalling • Filter technologies for railway cars (in case of bacterial attacks or pandemia) **Emerging Technologies** • Surveillance technologies (detection capacity, improved analysis) • SatCom • Tailored SCADA / Industrial Control Systems protocols and security mechanisms **Priority Research Areas** • Fault tolerant systems • CIP System Architecture • Risks and Vulnerability assessment methodologies and tools • Analysis and visualization of traffic data • Co-operative Systems • Defense-in-depth for SCADA / Industrial Control Systems • Information sharing and exchange • Threats and attacks modelling
CBRNE	**Technology Gaps** • Biological detection is less mature than chemical detection technologies. • Real time Biological detection: Emitter -laser sources -available power -compact, -robust, -self-starting (no manual intervention) Detector -spectral resolution

	-data processing electronics -data algorithm development. • Most Bio-detection technologies are designed for laboratory analyses and suffer from false positives and negatives. The false positive issue is a very serious one and is generally addressed by characterizing the backgrounds extremely thoroughly and with replication. This does not address the need for sampling from diverse environments with large unknown backgrounds and being able to test hundred of potential threats rather than a well defined one **Emerging Technologies** • Decontamination by nano-particles. • Environmental biochips (potential portability, low cost, ability to screen a wide variety of targets including nucleic acids and proteins on the same platform, and potential use ability for environmental samples of unknown content). • Broad spectrum pathogen surveillance system. • Current technology is still focused on centralized laboratories and RT-PCR. Speed and diagnostic confidence in the field will be essential for both near-term and future threats including Bio-detection techniques that identify threats that have not been previously defined. This implies assays using molecules targeted by threats agents rather than oligo nucleotides or antibodies. • Alarm electronic system of light detection and ranging (short range biological LIDAR). **Priority Research Areas** • First responders • Prevention • Resilience • Risk assessment • Human Factors • Medical counter-measures • De-contamination • Epidemiology modelling • Usability lab
Crisis Management	**Technology Gaps** • Biosensors - in mid term • Mass market warning systems • Use of new frequency sensors • Language problems, symbology, common symbols,

	(automatic translation) **Emerging Technologies** • Emergesat & SatCom systems • Satellite/terrestrial configurations • New frequency bands • TETRA based systems • Seamless communication **Priority Research Areas** Need for devices that could (easily) be used in the field, and a "mass-market" alert and warning system.
Wide Area Surveillance	**Technology Gaps** • Detection of abnormal behaviour. • Detection of very small targets irrespective of material. • Need for new sensors: better infrared cameras for vessel detection at night as well as triggering sensors, like a lazer fence. • Need of a sensor with higher resolution, with larger coverage and with higher update frequency, especially for operations and for surveillance in the pre-frontier (country of origin of immigrants). • Unmanned systems with capability of automatic detection. • Need of a tool for planning and tasking of the capability of remote sensing satellites. • Prominent need for cameras in small harbours • Detection of non cooperative vessels, most importantly leisure craft. • Demilitarized technology. **Emerging Technologies** • Low-light cameras for sea border surveillance • New sensors, for example the ultra wide swath type. **Priority Research Areas** Further improvement and development of detection technologies
Movement of People	**Technology Gaps** • Remote identification technology. • Reliability of data in old databases. • Lack of quality usability testing of systems both from the perspective of the subject who is being validated and the Border control operative who is carrying out the validation process.

	• Slow real time validation of a subject resulting to delays with impact on the perceived reliability of the system. **Emerging Technologies** • The use of Neural Network Technology using Concurrent Self Organising Maps in the decision making process. • Ultra Wideband Radar Technology. • Wireless Sensor Networks in the area of Remote Automated Surveillance Systems. **Priority Research Areas** • Multi Modal Fusion. • HCI& System Usability • Privacy & Data Protection methods
Movement of Goods	**Technology Gaps** • Split Command and Control • Accuracy of information. • Data security and vulnerability of e-seal/reader interface **Emerging Technologies** • 100% scanning/ sealing tools. • Data- sharing prototype for Customs to Customs communication as well as for electronic pre-notification. **Priority Research Areas** • Promote disaster resilience, Seek to ensure that cascade effects from failures don't propagate through the supply chain, and that systems are able to restart operation as soon as possible after an incident. • The impact that new technology will have on an organization and its users. How to structure the organization so that it uses the technology in an optimal manner, and also to ensure that the technology fits in to the pre-existing operational routines of organizations while causing minimal disruption to operations. A common problem is that operators are worried of security technology because they don’t want their routines to be disturbed.
Interoperability	**Technology Gaps** • Need for more system-concept orientated solutions • Security of communications (crypto etc.)

	• Scenarios/ « risk profiling ». • Open technical standards. • Analytical support. • Sensors • There is a lack of surveillance/ monitoring system on the technical level, systems which make it easy to get an overview of the status of technical system. However, what is even more important from the technical systems is command/control and classification of roles. **Emerging Technologies** • Radio system for exchange of classified information. • Internet based information distribution system. • CBRN detectors • Simple-to-handle material which could be used by first responders to classify the type of emergency rapidly. • Management systems (internet based).
Human Factors	**Technology Gaps** • Actor agent communities. • Network centric operations, but newly designed for civilian security applications. • CBRNE scenarios and databases, newly designed for civilian security applications. • Ergonomically ill designed systems must be redesigned, which leads to more than double effort and costs. • Automatisation concepts don’t have the desired results, because they cannot be used as specified. Automatisation is a HF problem, i. e. one of function allocation between man and machine and then a matter of its intelligent usage. • Different mental models between users and designers. **Emerging Technologies** • Basic and applied research in the areas of behavioural and social sciences are still not sufficiently enough integrated into industrial development of security products and services. There must be a better chaining between academia and industry in this respect. • Simple, reliable and validated tools for demanding applications are preferred to complex and experimental systems. The later are important in a R&D context. • More reliable and simpler mobile computing. • Tools and methods for real time audio-visual and text crisis communication.

	• Team-working metrics. • Methods and tools to display selected heterogeneous situational data in a concise and aggregated manner to be understood by (non expert) political decision makers. • Text mining” technology is required for handling mass data. • Translation software for highly demanding texts and situations (much better than the actual state of the art). • Sensors to detect flying objects with minimal radar profile. • HCI design. • HF performance testing tools. • HF in multi-level operations. • Software tools for information processing and evaluation. • With regard to the lack of specialised support SW-tools for analysis and decision support, the FASTI-project is an example for the direction to take (introduction of HF centred support tools on Conflict Detection, Monitoring Aids and Coordination). **Priority Research Areas** • Simulation of HF in operational contexts (e.g. flight simulation) is still a challenge. • Simulation tools for analysis and training of human behaviour and “thinking” support. • Tools which structure and support “Computer Managed communication”. • Decision support tools.
Standardisation (a key transversal topic covering all missions presented above. Standardization security activities focus mainly on the following subjects: Buildings and Civil Engineering Works, CBRN(E), Energy Supply, Border Management).	Focus on standards for CBRNE and Crisis Management technologies **Priority Research Areas** • CBRNE prevention and preparedness • CBRNE response**.** • Vulnerabilities assessment. • Crisis prevention • Crisis recovery • Material discrimination • Automated alarm system • Low false alarm rates • Real time results • Speed of operation • Flexibility to adjust the alarm settings to take account of changes in risk or location.

	• Low manpower commitment • Ease of set up and use. • Health, safety and legal constraints on personal privacy

3. STACCATO – Analysis and Recommendations for the European Security and Equipment Market

In order to analyse the European Security Equipment Market several actions have been conducted. In particularly it has been analysed the specificity of the demand side, taking into account users installed and planned technical equipments, regulatory environment and Security Research Programmes both at National and European level. These data gave a first picture of the situation that is described below and it represents the base on which final recommendation has been taken.

3.1. Major Results on ESEM

The collected data on end user equipment installed and planned were clustered into for each mission, and key information is reported below:

3.1.1. Critical Infrastructures and Networks Protection/ Cyber Security

For this mission the key equipment installed are:

- Sensors, in general
- Identification equipment
- Navigation, guidance, control and tracking equipment (especially for networked infrastructures)
- Equipment to monitor built infrastructures.

End users have identified some planned procurement needs in equipment for improving in information technologies (secure information treatment) and identification techniques (including Biometric technologies).

3.1.2. CBRNE

CBRNE, and especially CBRN, missions are highly specialised and sensitive, and related to mainly public operators and first responders, in a limited number in each country.

It is not a potential “large” market but it deserves specific attention due to the importance of the impacts of such threats and the high level of technology required.
In this field, there is a small but very active scientific and operational community in Europe but very limited in terms of budget. Specific conditions of level of co-funding (due to the limited market) and public support are needed to develop.

For this mission, the key equipment already in use are :

- CRN local and stand off sensors equipment,
- B samplers and analyzers,
- X ray sensors,
- decontamination techniques,
- rather heavy human protection equipment.

There is a specific need for :

- more reliable (with less false alarms) CRNE detection and identification,
- stand off B detection and in the longer term identification,
- fast stand off E detection (real time),
- decontamination light techniques,
- light and intelligent protection.

3.1.3. Crisis Management

For this mission the key equipment already used are :

- Sensors equipment

- Communications equipment
- CBRNE protection equipment
- Enable equipment for Command and control Centres.

There is a specific need for improving systems for training and definition of standards for Radio Equipment (e.g. TETRA) versus interoperability.

3.1.4. Transportation/Movement of People and Goods

The end users contacted for the interviews are quite all involved in both movement of People and movement of goods, so the analysis has been conducted considering only one mission.

The key equipment already in use :

- Identification equipment
- Navigation, guidance control and tracking equipment
- Access control (on public transport means) equipment

There is a specific need for improving in identification techniques (including Biometric technologies) and tracking equipment.

3.1.5. Border Control and Security

The key equipment and platforms already in use are:

- Sensors equipment (especially surveillance technologies: Satellite, Radar, VTS ...)
- Identification equipment
- Biometric equipment
- Marine, space, ground and air platforms

There is not a specific need for new components or technologies but the end users express requirements for improving the capacities of existing technologies, towards lower cost and better reliability.

3.1.6. General Remarks

The end users involved in the process have been selected to have a good representation of the European needs on security equipment. The performed analysis can be used to have a panorama of installed and planned equipment. Further improvements can be developed in specify more in detail the key characteristics of sensors equipment for each mission.

3.2 Characteristics of the European Security Equipment Market

3.2.1. The ESEM in an International Context

The analysis would not have been complete without some general considerations, facts and figures presented to illustrate what represents today and in the future (according to studies[3]) the European security market, including some examples of areas of interest[4]. These elements have to be taken into account in the development of opportunities for common market.

Europe is considered as a key player in “homeland security” :

- Europe is a huge market for security equipment and is second only to North America in terms of market share.

[3] (Sources : Frost & Sullivan, GSPR, CSO online)

[4] See also other parts of the STACCATO study reports dealing with the analysis of key issues per mission (critical infrastructure protection, border security, etc.).

- This market is still in the hands of the private sector except for information security, where the state accounts for 50% and can therefore influence orientations.
- With the increase in terrorist threats across the European Union (Madrid, London Tube, Glasgow Airport), countries are placing a greater emphasis on improving homeland security through the monitoring of entry and exit points

    - *Zoom on European airport security market* earned revenues (top 47 participants) of $2.37 billion in 2005 and estimates this to reach $10.35 billion in 2010.

      The European airport security market looks set for robust growth, particularly in the wake of continued terrorist threats, new European Union (EU) airport security regulations, rising passenger traffic and the increasing need to upgrade installed security equipment, as well as integrate this with newly implemented technology.

      Opportunities are particularly lucrative in the biometrics and explosive detection sub-segments, where small start-up companies offer innovative technologies on their own or with large systems integrators.

- Further, the expansion of the EU has made borders relatively more porous and policing the borders more effectively is crucial to checking the inflow of illegal immigrants (sea, air, land borders control and surveillance).

  There is therefore a strong demand for technologies that helps detect threats at airports, seaports and borders, including demand for biometric identification/authentication systems, radio frequency identification and explosive detection systems.

- Tighter link between EU and US regarding foreign policy and transatlantic trade.

3.2.2. European Security Market Specificities:

- European Security Market is not consolidated like in the USA therefore this fragmentation makes it difficult to provide big figures without loosing quality of the data. Example: In the USA, infrastructures are 85% privately owned. In Europe, the proportion is significantly lower.

- Definition of “Homeland Security / internal security / civil security” varies from one country to another with various stakeholders.

Key Figures :

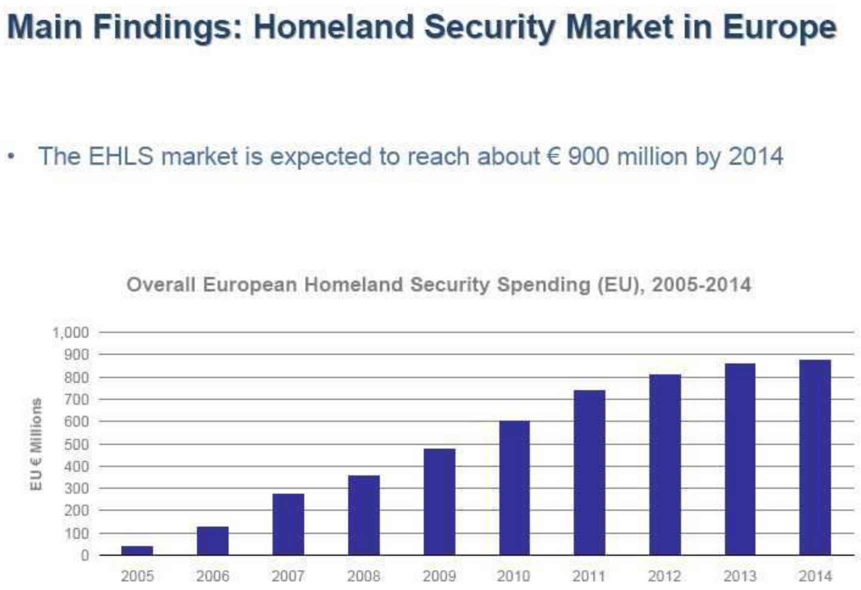
- The world security market is estimated at $100 billion. But it is very fragmented (the turnover of market leaders does not generally exceed €1 billion) and is dominated by the UK and the USA.
- The sovereign security market is estimated at around €50 billion. It consists of several segments, the largest and most homogeneous of which is the telecommunications- infrastructure segment.
- At the EU level, the market was estimated at €700 million in 2004.
- In 2004, The EU also contributes over €400 million for upgrading security in new member states, candidates and neighbouring countries (Schengen Facility, Phare, Meda, etc.).
- Three Sub markets (examples): electronic, mechanical and human security.
- Scope market security (examples): IT Security / Physical Security.

IT Security

Growing fears about cyber-crime are boosting the European market for security systems. Spending on IT security will grow from $8.7 billion in 2005 to $30.3 billion worldwide in 2015. Similar tendency is in Europe.

Physical Security:

By 2014, the European homeland security technologies market (comprising biometrics, screening, RFID, unmanned aerial vehicles (UAV) and closed circuit television (CCTV technologies) is set to amass nearly EUR874.0 million.



Main Findings: Homeland Security Market in Europe

- The EHLS market is expected to reach about € 900 million by 2014

Overall European Homeland Security Spending (EU), 2005-2014

3.3 Diversity and Complexity of Actors in the Security Market

3.3.1. Variety of Actors

There is an important variety of actors in the field of security. They can be defined taking into account the following aspects:

- By nature: Public actors (Ministries, National or international Agencies, EU agencies,…) but also Public / Private actors (i.e. Harbour authorities, Airport operators….) and full private Actors (i.e. Banks,…).
- By mission: operators, services providers, technology providers…
- By position in the supply chain: prime contractors, subcontractors, suppliers…
- By position at local, national, European or international level (issue of sovereignty vs. European cooperation).

Private Security Actors

There is a need to develop the analysis of the growing private security market and related actors, and to further integrate the “services approaches” into the European security market. Services could provide innovative and cost-effective solutions in the field of security.

European Agencies

There is a specific need to take into account the various agencies recently created at the European level that address security issues, such as FRONTEX, EMSA or ENISA. These European bodies are already involved in the definition of security policies and the preparation of future security research and acquisition programs (ex. EUROSUR and FP7 security for FRONTEX). Therefore, these will contribute to defining the European security market.

In particular, it is important to strengthen their capacity to develop and support concrete projects and to envisage the creation of new dedicated budget lines (including in their respective budgets) for the acquisition of equipments, systems and services.

Another key issue is the comparative analysis between the defence domain and the security domain as well as their respective regulations and specificities.

3.4 Sensitivity of Security Technologies

The above elaborated analysis shows that one of the key factors of the European security market is the sensitivity of the security technologies that would potentially be used in security missions, taking also into account the strict interconnection between security and defence.

Similarity, at national level the operational integration of security and military forces has increased, thus requiring a suitable level of interoperability and commonality of systems and capabilities.

3.4.1. Definitions

“Sensitivity” could be defined taking into account the following criteria :

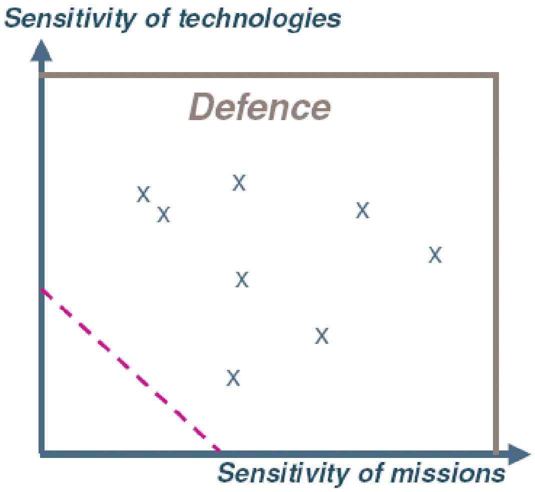
- The Context in which the mission will take place: peace, war, peacekeeping, peacemaking etc;
- The level of confidentiality (security of information) considered as appropriate by the relevant authorities: confidential, secret, top secret etc;
- The level of governance: National and/or European and/or international;
- The Customer: government (public) and/or private;
- The domain: Security vs. Defence.

3.4.2. Illustrations

The following pictures illustrate the possible differences between the defence and the security domains.

A large majority of the technologies involved in Defence equipments and systems are sensitive, independently from their assigned or foreseen missions (see the X-covered area in the above chart).

It is only some of the basic technologies that might be considered as non-sensitive (see the area divided by the dotted line)



On the contrary, the sensitivity of the technologies for security has communality with defence but could be different.

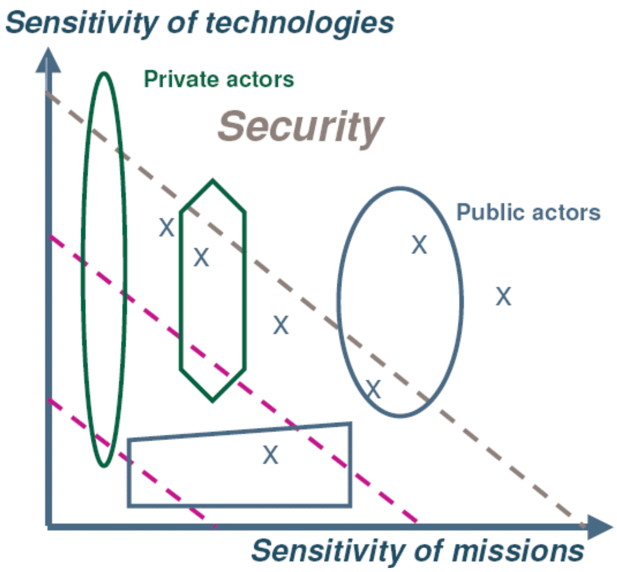
Practically, the actors (whatever their status might be) may generally use less or more sensitive technologies, depending on the specific cases.

As seen in the above chart, the technology sensitivity depends on the missions to be addressed by the final user: private entities in charge of citizens' protection at a low level or public bodies in charge of police missions.

It is important to remark that the sensitivity depend also on the specific Member state's interests.

The dotted lines represents the fact that generally we can assume that the sensitivity of the technologies depends on the missions that the different "actors" are supposed to achieve, namely of a low or a high intensity.

Some of them are considered as sensitive as in those in the defence case.



It is also necessary to note the potential difference between actors and end users, and their role in procurement, notably when end users are not the buyers of the systems and equipments. For example, in some countries and in some specific contexts, fire fighters can purchase equipment for the customs management bodies, or infrastructure operators can act as buyers for other end users.

3.4.3. Assessment and Lists of Security Related Technologies

Among other possibilities under discussion, it could be the interesting to analyse – or to update - a dedicated list (one or several list(s), in principle just one) of security related technologies, with a level of detail to be further defined (global or sectoral approach…). It seems important, in order to define the parameters of the sensitivity of security technologies and of the European security market, to address these issues and to launch a debate at European level in order to identify the possible solutions and alternatives.

- Existing reference documentation:
  - Wasenaar,
  - Dual-use code of conduct,
  - Taxomonies (SeNTRE document, improved by STACCATO…),
  - ESRAB Report,

- Frascati code (TRLs approach)
- CPV (Common Procurement Vocabulary) of the European Commission

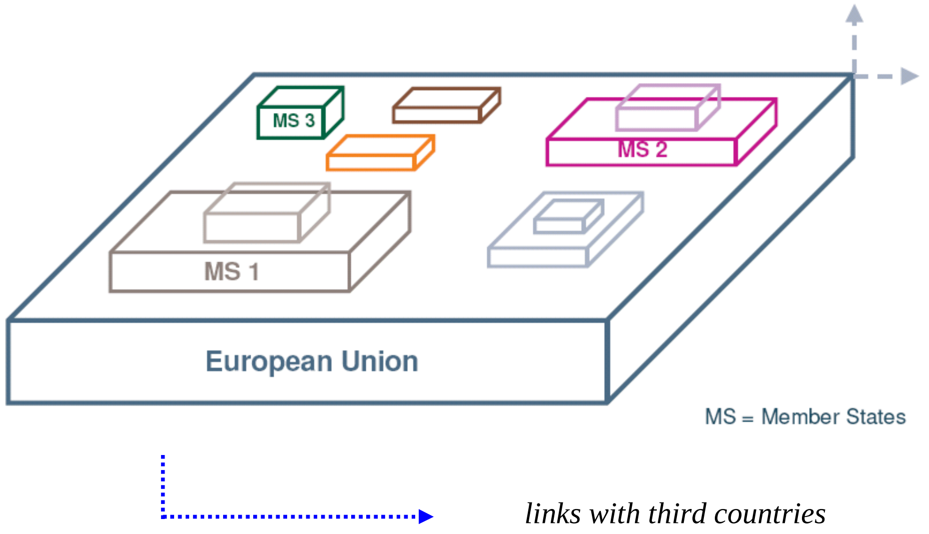
- New list(s) :
  - On the basis of the existing lists, it could be interesting to build up a new consolidated list of security products, services and related technologies in order to facilitate the monitoring by the different actors operating in the domain.

In parallel, there is a need to take into account the potential sensitive topics and their level of sensitivity, including their evolutions.

3.5. Regulatory Aspects, Normalisation and Standardisation Activities for Security

The following issues related to regulations have been identified :

- Coherence and complementarities with defence regulations;
- Intellectual Property Rights (IPRs).



This scheme recalls that the European Union should remain in charge to elaborate the general baselines on regulations and standardisation with the permanent aim to permit any national or local stakeholder to further develop concepts more specifically dedicated to local constraints and specificities.

The analysis conducted at European level on the legal framework environment put in evidence some key points :

- Even if, at EU level, there is a clear difference between the civil security and military security organizations and programmes, military and civilian forces cooperate more and more often in trans-national defence operations, while some military specialists are involved in civil security emergencies management, sharing equipment and logistic means.

- Cross-fertilisation between civilian-developed technologies and defence technologies allow to provide some rapid solutions, even if not fully tailored for the mission. However, little is currently done to complement the programmes in order to optimize the developments and the investments.

- In addition, some coordination is done at European level and at national level but very little in a multi-national approach.

- Overlaps appear structural to functional security, e.g. proliferation of security authorities. At EU level we can count at least 28 operating agencies in different manners involved in security management. It is clear that there is an urgent need for coordination.

An analysis has been also conducted at National level, in 13 countries (Austria, Finland, Germany, The Netherlands, Sweden, United Kingdom, Poland, Denmark, Belgium, France, Portugal, Italy, Greece), to understand the legal framework environment, along the following axis :

- Documenting the institutional arrangement in each country with the objective to implement the security policies and practices;

- Documenting the related national legal corpus, laws and policies regarding the European dimension of the issue;

- Providing the official definition of the related domain (in this instance the notions of “homeland security”, “civil protection” and “critical infrastructure”).

The result of this analysis pointed out the following considerations (this is only a picture “as it is” of the situation not a recommendation):

- In almost all the countries the concept of “Security” is strongly related to the Defence.

- There is at the same time a clear understanding in almost all the countries that Security should be a European Issue.

- Security cannot be guaranteed by the efforts of one country or by armed forces alone. It requires an all-encompassing approach that can only be developed in networked security structures.

3.5.1. Regulatory Aspects and Standardisation

Regulation may be considered as a factor that encourages the procedural and cultural differences by setting barriers and protect sectoral approaches. However, regulatory regimes should, if they are used to remove barriers and foster co-operation, contribute to overcome the European markets fragmentation and to enhance the emergence of some common markets in some security areas. Efficiency of such activities could be increased if it is associated with the Standardisation activities.

The benefit of such an approach will, for example, increase the interoperability and integration of systems and devices, foster better and more flexible communication, among the existing and future security systems and networks. That will reduce the number of variants of technologies and interfaces as well as, when deemed appropriate, costs of implementation and maintenance, including logistic aspects and related standards (because of potential vulnerabilities across the whole supply chain, from production to logistic and maintenance). Nonetheless, it would open markets and allow for a greater freedom of choices.

Standardisation and importance of the Standards for Security

Standards and related Standardisation activities are also of paramount importance to enhance the Security Market for equipment and products as they address a wide range of different purposes:

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

To support the emergence of an ESEM, standards and standardisation activities should in priority tackle 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 economical and technological impact);

- Define a method for the prioritisation of the areas of actions in this area. This could be undertaken within the ESRIF activities.

There is a lot of work at both European and international level on standardisation.

This is more and more related to security issues and EU budgets already exist for support of such activities.

However, it should be increased and oriented more specifically towards the efficient and concrete elaboration and implementation of technical standards.

In addition, the allocation of EU funds (for examples structural funds and external border funds) should be conditioned upon the integration and development of a minimum level of standardisation and interoperability (for equipments, systems and services, between end users and between different countries).

Finally, regulations should be considered in a positive manner, they are a key contributor to a market driven approach that is to be further developed and adapted in order to address current and future security issues.

These regulations are going to be decisive factors and if properly targeted could have positive impacts, such as harmonisation, interoperability and flexibility. Contrary to this, the general perspective on regulations holds that their lack is negative.

Nevertheless, the more sensitive activities will continue to be subject of specific controls, which could *de facto* put a brake on their development and implementation.

Moreover, it is also important to take into account the fact that regulations could have “collateral” impacts – generally more positive than negative, such as the strengthening of surveillance and control in transport infrastructures and contributing to the security of the global supply chain.

On top of that, compliance to standards has to be controlled by Authorities to guarantee that the “EU flag” is justified. It is so proposed to establish in some critical areas a European test and certification lab(s) under a neutral and competent organisation, in order to test the performances and provide this European label, or not.

3.5.2. IPRs – Intellectual Property Rights

Industry and RTOs express regularly their concerns on IPRs and consider that their proper treatment is of prime importance to the interests of all contracting parties : European Commission (and all relevant Agencies), Member States, RTOs and Industry.
The consequences for the quality of results delivered :

- Used appropriately, IPR can be a catalyst for a stronger Security Technological and Industrial Base.

- Conversely, inappropriate IPR stipulations might produce the opposite effect in terms of customers and industrial interests with a potential increasing duplication and continuing market fragmentation.

General Industry Position on IPRs for R&T :

Industry is always looking for flexible “instruments” able to take into consideration the level of funding, the importance of the background brought by industrial stakeholders, the technology maturity and aiming to avoid unnecessary duplication in the European STIB.

IPRs principles ensuring flexibility should be negotiated to treat in priority:

- Background dissemination (not foreseen during the bid phase)
- Foreground dissemination for further cooperation with Third Parties.

All these issues must be treated with a clear consideration of the two most important contractual instruments: grant actions and procurement contracts.

Industry considers as more appropriate any principles focusing the IPRs main dissemination within the individual projects instead of any mechanisms granting automatically to all “contributing” Members States “used” and “have used” rights for large and broad security purposes whatever being the level of co-funding and funding of the respective contributing Members States.

That is why Industry should continue to explain the most important message on the IPRs: individual projects might give rise to more specific arrangements to be negotiated on a case-by-case basis.

Specific Comments for IPR on European Collaborative R&T :

Collaborative research, by its very nature, will rely on the members of the consortia combining their pre-existing background knowledge and generating, through project execution and delivery, foreground knowledge.

For example it must be said that FP7 rules of participation, like those of FP6 before it, address in a detailed manner how background and foreground IPR will be treated in terms of ownership, protection, access rights and use.

Industry felt that “security research” has certain specificities which needed to be taken into account:

- Firstly the possibility for the Public Authorities (i.e European Commission, Members States) to control the transfer and dissemination of knowledge for sensitive projects,

- and secondly the requirement to identify for specific project information (with the eventual assistance of the Programme Committee) in order to be able to inform “end-users” of research of potential interest to them and to co-ordinate national research.

In a general comment, there is a need for simplification of procedures and rules, and for a coordinated body in charge of these issues.

3.6. Funding Issues in Security Procurement Activities

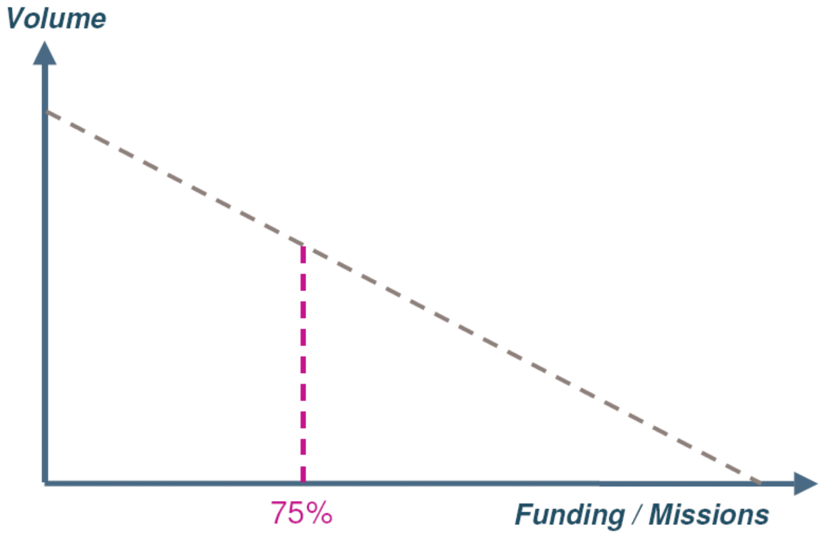
R&T

In terms of funding for R,T&D: the following key issues have been identified :

- Level of funding, to be defined taking into account :
    - The parameters of the ESEM (actors, regulations, etc.);
    - The level of sensitivity of security technologies;
    - Self-funding (Industry);
    - Rules applied to security theme with regard to other DG and themes;

- Potential complementary funding (i.e. to EC FP7 and Industry/RTO contribution) for security technologies, for a better level of funding (including for R,T&D) and for acquisition:
    - From Member States
    - From other EU bodies (i.e. such as more joint actions and associated joint calls, between DGs, themes, EC and other bodies such as FRONTEX, EDA, ESA, etc.)
    - From a joint initiative among MS and EU functional to European common initiatives such as the best practice of Space (GMES) and in development for Unmanned Aerial Vehicles (UAVs) and Maritime Surveillance.

- The need to take into account the ESRAB report recommendations



As it has been detailed in the ESRAB report, the funding level for the R&T will depend on the accessibility of the potential market.

The more the market will be controlled by security regulations, the more the technology providers will pursue for a higher level of funding.

This principle has been taken into consideration when EC has finalized its regulation for the 7th Framework Programme Agreement. This is applicable for the FP7 Security.

Procurement

In order to further analyse the key issues of the European Security Equipment Market, and in particular the procurement aspects, STACCATO recommends to launch a dedicated study on funding and procurement issues in the field of security.

3.7. Analysis of National Research Programmes

10 EU Member States have published specific National Security research programs or have a specific part in their national programs on Security themes.

All of them have been analyzed.

Nation	Budget	Beginning of the Programme
Austria	9 M€ 2006 --- 15 M€ 2007 110 M€ (up to 2013)	2005
Czech Republic (only part for security)	161 M€ for 2004-2010 (only part for security)	2004
Finland	80 M€ (2007-2014)	2007
France	11,1 M€ (2006) ; 11,7 M€ (2007)	2006
Germany	20 M€ 2007 100 M€ (2007-2013)	2007
The Netherlands	80 M€ (2008 – 2011)	2007
Poland	10,5 M €	2006
Spain	To be decided year per year	2004
Sweden	6 M€ per year for 4 years	2007
UK	New Programme 2008-2011 budget (TBD)	2000

This analysis underlines a growing need for investment on security research in most of the European countries (from 2004 to 2008 the number of national programmes increased from 3 to 10).

Looking at the contents of the programs there are some commonalities:

- Crisis management capabilities
- Critical Infrastructures protection
- Information security

And there is a need for more coordination, pooling, complementarities, potential joint calls, programmes and budgets, between Member States (national programmes) and between Member States and European institutions.

3.8. Synthesis of Key Market Issues for the 9 Mission Areas

The table below presents the key ESEM issues identified in the project per STACCATO mission area.

Mission Area	Key Market Issues
Critical Infrastructures and Networks Protection/ Cyber Security	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 can not 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.
CBRNE (Including Decontamination)	There is currently a limited market for Bio-detection products and the defence related market is minimal. The best way forward is to design Bio-detection system for dual use (e.g. defence 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).
Crisis Management (Focus on Information and Communication Issues)	From the market perspective, crisis management is abstract and not preventative, when compared to non-crisis fields.
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. Standardization 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…
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 defence 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	*See related part to standardisation (3.3)*

3.9 Synthesis of Key Issues for One Example of Mission Area

The following table aims at presenting the key market issues (diversity of actors, sensitivity of security technologies, regulations/norms/standards and funding mechanisms) applied to one mission area analysed during the STACCATO study.

Mission Area	**Key Market Issues**
Mission **Wide Area Surveillance** ***(focus on the blue area surveillance)*** This mission includes several activities, such as border security, port security, fight against terrorism, illegal immigration and illegal fishing, anti-pollution measures or also the transport-related monitoring.	**Diversity of Actors** There is a huge diversity of actors in the field of wide maritime area surveillance, at different level : - local, national, regional, European and International - at national level, different organisations exist for the various missions, coordinated at inter-ministerial level or not, or only partially (between the Navy and Coastguards for example). In several countries there is one authority in charge of actions at sea (ex. Préfet maritime in France) - at European level, European Commission (including different DGs : JLS, Enterprise & Industry, TREN, MARE…), EU Council and bi-multilateral cooperation, European Agencies (such as EMSA, FRONTEX, EDA, ESA…), NATO… - at international level : IMO (International Maritime Organisation)… - public and private, such as Customs or Navies and security and services company providers, transport operators… - organisations and associations of companies, regions, operators… - links with an more and more involvement of third countries (EU strategic partners, EuroMed…) **Sensitivity of Security Technologies** This point needs to be further developed, taking into account the responsibilities of the actors involved in the mission, but also new evolutions at political level and technologies. But there are more and more synergies, potential economies of scale, and cost savings to be developed in order to ensure more interoperability, lower cost measures and better operational and flexible capabilities, better reliability. **Regulations, Norms, Standardisation** Regulations and norms exist at national, European and international level. Depending of the mission, Member States and/or European Union are in charge to elaborate the norms and ensure their implementation. New EU policies are also to be considered : future maritime policy, integrated border management strategy, etc. Particular emphasis should be made on standards and new technologies. **Funding Mechanisms** Some funding sources exist at national and European level to develop wide maritime area surveillance capabilities, but still relatively limited. There is a need for new and more complementary and additional budgets, including new types of acquisition or services offers, dedicated to joint and structuring programmes, based on existing initiatives (maritime policy, EUROSUR…) and pilot projects.

This kind of analysis per mission should be further developed in order to identify the key issues and opportunities related to the market.

STACCATO Main Conclusions

The STACCATO project arrived to several key conclusions on European security technology and market issues by establishing a community of public and private stakeholders and developing common language methodology – the **STACCATO "tools"** – that are presented in detail in this report (database, security taxonomy, report on dynamic scenarios...) in order to maintain and further develop this network.

It is evident from the work conducted in STACCATO that in many cases **technology** exists but adaptations or specific developments are necessary towards integration, interoperability and innovation. The exhaustive exploitation of current technologies as well as accessibility and affordability (cost issue) are also key issues that need to be examined when looking for new technologies.

As far as the **European security market** is concerned, it exists but is very fragmented. Taking into account the specificities of security technologies and market and each security area/sector, it needs to be consolidated and developed at the EU level with related regulations, standards and funding mechanisms (including new additional and complementary). The consolidation should include emerging actors and sectors as well as new developments such as the liberalisation of markets and the developments within the EU in sectors like energy, communications, environment.

The development of an European Security Equipment Market (ESEM) should also include competitiveness as a key issue 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. In general, security could be seen as a big opportunity for European competitiveness in terms of industry and R&T developments, through concrete research projects and more national and European programmes, including more joint and structuring approaches and innovative funding mechanisms. These activities will have to be developed in close cooperation, since the identification of needs by the (end-) users towards the procurement, delivery and support services.

To set a favorable environment to help the emergence for such a market, Europe should foster a set of the procurement policies to drive the innovation in the security field. The Communication (COM(2007) 799 final Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe, outlines a number of issue that should be examined, adapted to cover research and development activities in the security area. As an example, identifying public purchaser in a selected number of areas should be possible, especially if demonstrators are to be developed under the ESRP. In this way, concrete organising the risk benefit and sharing of such procurement could be established

Security constraints may not only hinder the use of the technology, but also the innovating solutions and products may generate new threats and new vulnerabilities. There will be tradeoffs between public acceptance of the additional constraints and the improvement of the citizen’s security.

In general, to improve the citizen’s security these “human” related factors must be taken into account. Actions, and Member States policies should also take into account the fight against the roots that are generating insecurity. Reducing societal difference and gaps, more communication and education about the cultural and ethnics differences should benefit from the support actions.

The role of Member States will of course have to remain important and taken into account since security is a key issue of national sovereignty, but this should not prevent from more interactions and cooperation at the EU level. New policies and initiatives at European level also generate new opportunities for European security actors, contributing at the end to the security of the European citizen.

STACCATO’s recommendations will be disseminated to ESRIF and can also be useful to European and national security R&T programmes.

Finally, further studies are needed for ESEM specificities and common opportunities, to be considered as a key European and national priority.

* * *

The STACCATO recommendations on European Security Equipment Market are presented in the first part of this document.

ANNEX :

STACCATO List of Priority Research Areas

Missions	**Priority Research Areas**
Critical Infrastructures and Networks Protection/ Cyber Security	• Fault tolerant systems • CIP System Architecture • Risks and Vulnerability assessment methodologies and tools • Analysis and visualisation of traffic data. • Co-operative Systems. • Defence-in-depth for SCADA / Industrial Control Systems • Information sharing and exchange • Threats and attacks modelling
CBRNE	• First responders • Prevention • Resilience • Risk assessment • Human Factors • Medical counter-measures • De-contamination • Epidemiology modelling • Usability lab
Crisis Management	Need for devices that could (easily) be used in the field, and a "mass-market" alert and warning system
Wide Area Surveillance	Further improvement and development of detection technologies
Movement of People	• Multi Modal Fusion. • HCI& System Usability • Privacy & Data Protection methods
Movement of Goods	• Promote disaster resilience, Seek to ensure that cascade effects from failures don't propagate through the supply chain, and that systems are able to restart operation as soon as possible after an incident.

	• The impact that new technology will have on an organization and its users. How to structure the organization so that it uses the technology in an optimal manner, and also to ensure that the technology fits in to the pre-existing operational routines of organizations while causing minimal disruption to operations. A common problem is that operators are worried of security technology because they don't want their routines to be disturbed.
Human Factors	• Simulation tools for analysis and training of human behaviour and "thinking" support. • Tools which structure and support "Computer Managed communication". • Decision support tools.
Standardisation	• CBRNE prevention and preparedness • CBRNE response**.** • Vulnerabilities assessment. • Crisis prevention • Crisis recovery • Material discrimination • Automated alarm system • Low false alarm rates • Real time results • Speed of operation • Flexibility to adjust the alarm settings to take account of changes in risk or location. • Low manpower commitment • Ease of set up and use. • Health, safety and legal constraints on personal privacy.

* * *