...ETCETERA

Evaluation of Critical and Emerging Security Technologies
for the Elaboration of a Strategic Research Agenda

Final Report

Joachim Burbiel, Ruth Schietke
Fraunhofer Institute for
Technological Trend Analysis INT

ETCETERA is an FP7 co-funded project
Contract No. 261512

...ETCETERA

Evaluation of Critical and Emerging Security Technologies
for the Elaboration of a Strategic Research Agenda

Final Report

Joachim Burbiel, Ruth Schietke
Fraunhofer Institute for
Technological Trend Analysis INT

1 Executive Summary

Background:
Within the FP7-supported project ETCETERA ("Evaluation of critical and emerging technologies for the elaboration of a security research agenda", Oct. 2011 to Nov. 2013) two kinds of technology evaluation have been carried out:

- Technologies that are critical for security functions in Europe were checked for dependencies on extra-European sources (e.g. materials, know-how, production facilities, IPR).
- Technologies that are now just emerging and will reach maturity in 10 to 15 years were assessed concerning their relevance for European security, with a focus on opportunities for enhanced security functions.

To address these two temporally separated issues, the project was divided into two research strands. Research issues were proposed to overcome Critical Dependencies in the near future and to capitalise on the opportunities offered by Emerging Technologies. Furthermore, new methodologies were developed and applied, e.g. a "serious gaming" approach and a new economic model to assess high risk, high pay-off research options. These activities were closely accompanied by work on ethical aspects, as decisions about research funding should take into consideration all possible implications of novel technologies on society.

Critical Dependencies:
Starting from the STACCATO taxonomy, a set of approx. 200 technologies that are indispensable for European security was selected. This selection process was supported by five "parallel" workshops in different countries (Spain, Sweden, Germany, Italy, and France), using the local languages but applying the same methodology to insure comparability of results.

Through a multi-factor approach, taking into account IPR, trade restrictions, production gaps and raw material constraints, those technologies which rely on non-European sources or providers were identified. These "Critical Dependencies" include sensors technologies (e.g. for detection of radioactive radiation), security equipment (e.g. advanced X-ray scanners) and a large group of electronic components. Ideas on how to overcome these dependencies were developed.

Emerging Technologies:
A set of 127 Emerging Technologies with security implications was identified through three different methods applied in parallel. These technologies were prioritized concerning their expected impact on security and on the expected time of commercialisation (focussing on 2020 to 2030). This priorisation process was supported by a series of scenario workshops and two "Security Technology Assessment Games" (SETAG). The Emerging Technologies with the highest priority included encryption methods (e.g. homomorphic and quantum encryption), communication systems (e.g. cognitive radio), sensors (e.g. terahertz and hyperspectral sensors, and "through the wall" radar), technologies associated with mobility (e.g. autonomous passenger cars and indoor navigation), and advanced algorithms (e.g. automated human behaviour analysis and reality mining).

Project homepage:
Further information is provided at:
www.etcetera-project.eu

2 Summary Description of the Project

2.1 Structure and context

The ETCETERA project was a contribution to efficient security research planning on a European level. It took up the two-fold structure of topic "SEC-2010.7.0-3 Critical and emerging technologies for security" by dealing with the issues "Critical Technologies" and "Emerging Technologies" in two separate but interrelated research strands. Each strand was further divided into three Work Packages (WP), which were carried out in a sequential manner. Two Consultation Campaigns generated input from technical experts, end-users, and public authorities for both strands (Figure 1).

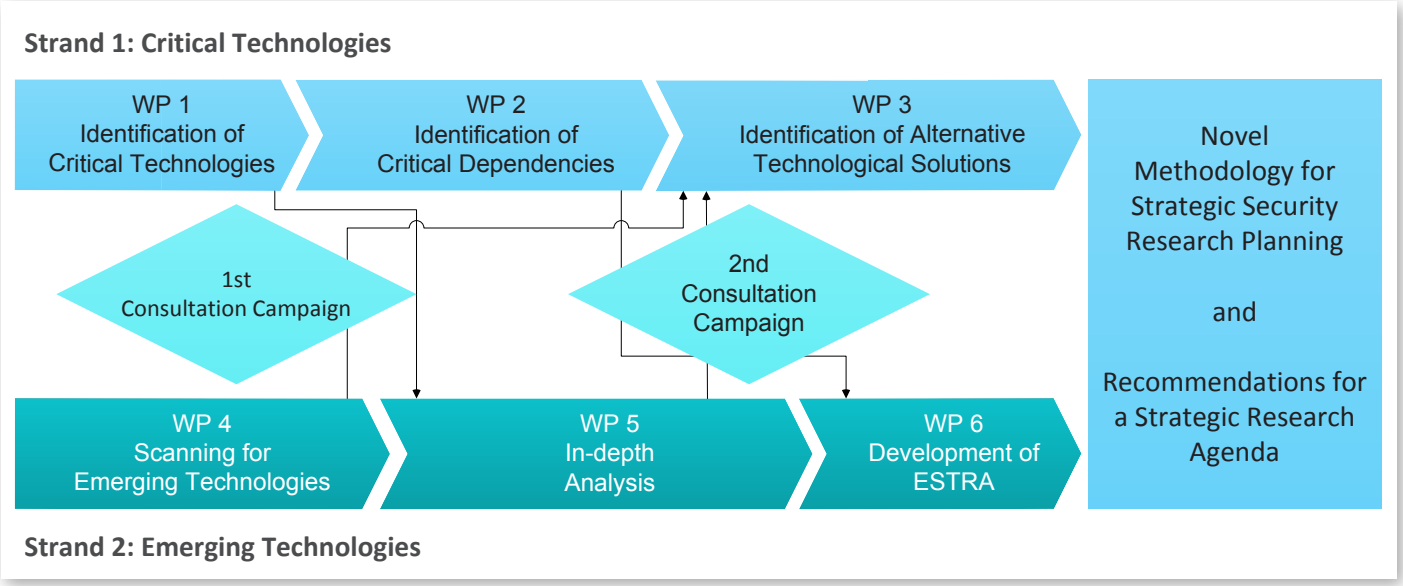


Figure 1: Workflow of the ETCETERA project

While the division into the two strands is quite obvious, a further division is more subtle: two kinds of objectives have been pursued by the ETCETERA project.

- On the one side the delivery of the lists and plans called for in topic SEC-2010.7.0-3:

1. A list of critical technologies and a plan to deal with these to allow ‚non-dependence' for Europe and
2. a list of emerging technologies and a plan to deal with these to set out high risk, high pay-off research priorities.

- On the other side the development and application of novel approaches and methods for the evaluation of Critical and Emerging Technologies and for strategic security research planning.

Although the call topic was formulated in early 2009, the issues of Critical and Emerging Technologies are still on the agenda today. The Communication of the European Commission "Towards a more competitive and efficient defence and security sector"[1] addresses the issue of criticality under the headline of improving security of supply. It names "control and ownership of critical industrial and technological assets" as a key factor and calls for a "Green Paper on the control of defence and security industrial capabilities".

The "Draft Report on the European Defence Technological and Industrial Base" by the Committee on Foreign Affairs of the European Parliament[2] even goes beyond these assessments. Relating to the security of supply, it "calls on the EDA and the Commission to submit a joint non-dependency strategy on **critical technologies**, in particular as regards unlimited access to and availability of civilian and military (dual-use) **emerging and key enabling technologies**, such as cutting edge micro-/nano-

1 EU Commission, "Towards a more competitive and efficient defence and security sector", Brussels, 24 July 2013, COM(2013) 542

2 Committee on Foreign Affairs of the European Parliament, "Draft Report on the European Defence Technological and Industrial Base", 28 August 2013, 2013/2125(INI)

electronics and photonics (…)" (highlighted by the authors).

Only two of several recently completed FP7 projects related to ETCETERA shall be mentioned here. One is "Foresight Security Scenarios - Mapping Research to a Comprehensive Approach to Exogenous EU Roles" (FOCUS, April 2011 to March 2013) which mainly dedicated itself to potential security scenarios in 2035. Its results concentrate on a holistic approach towards security issues, highlighting the importance of societal and organisational measures for ensuring security. Technological issues, which are in the centre of the ETCETERA activities, are mainly dealt with on the "threat side" of the FOCUS project. As a result, the two projects present complementary views concerning the planning of future security research.

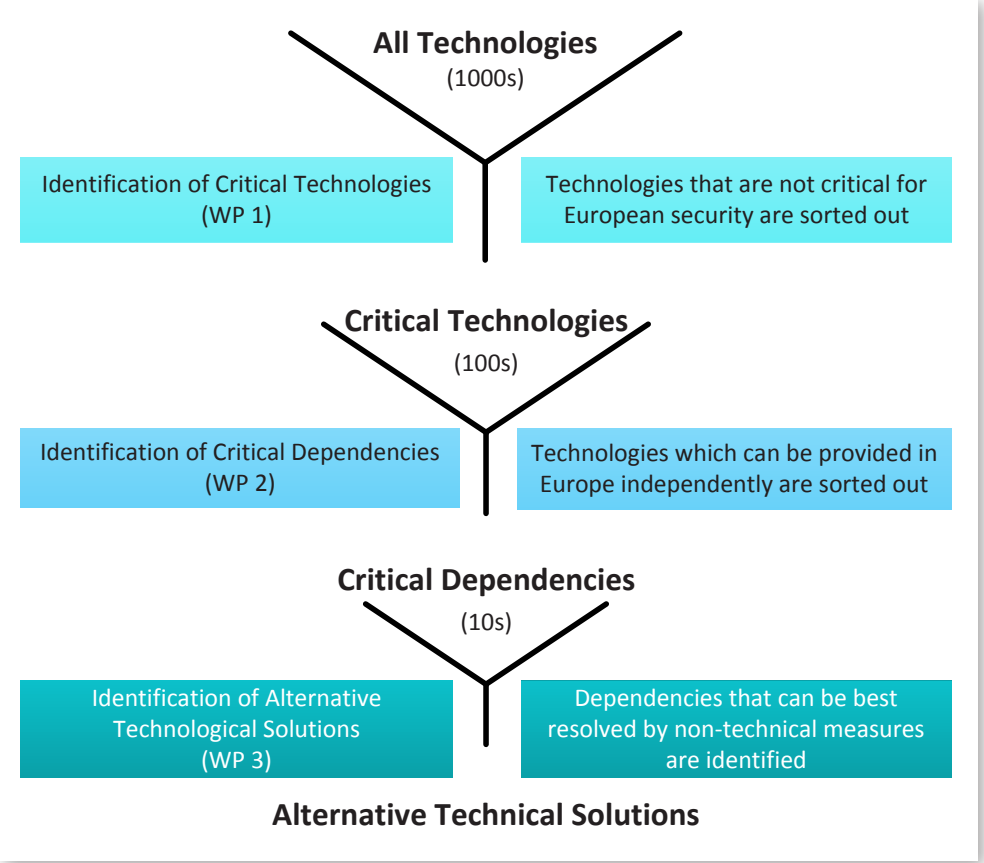


Figure 2: Strand 1 "Critical Technologies" as a filtering process.

Another relevant project was "Foresight of Evolving Security Threats Posed by Emerging Technologies" (FESTOS, March 2009 to October 2011). This project dealt with the "dark side" of Emerging Technologies and thus ideally complements the ETCETERA approach of looking at the chances that Emerging Technologies offer for civil security and security industry.

The next sections document how the ETCETERA concepts of Critical Technologies and Emerging Technologies complement these perspectives and provide approaches how to deal with these pressing issues.

2.2 Critical Technologies

A Critical Technology is broadly defined as a technology that is currently available or expected to be available in the near future and that is indispensable for European security.

A Critical Technology can for example be a basic component (e.g. computer chip or a cryptography algorithm), a subsystem (e.g. atomic clock in a communication satellite or a bacteria detector for water supply) or even a manufacturing facility (e.g. for producing vaccines).

To a large extent, Strand 1 "Critical Technologies" was planned as a filtering process (Figure 2). Starting from all thinkable technologies, only those that are critical to European security should pass Work Package 1.

It was expected that European industry is capable of providing systems based on most of these Critical Technologies quite independently to end-users. Only those Critical Technologies that show serious dependencies should pass Work Package 2.

Technological solutions were further analysed in Work Package 3. The output should both include possible alternative technological solutions, and

recommendations for short-term applied research priorities to overcome existing dependencies.

The filtering process itself was documented and evaluated to provide a method that can be easily adapted to future analyses of this kind. The process developed will thus be of further use in European technology assessment efforts.

2.2.1 Identification of Critical Technologies and 1st Consultation Campaign

In the first Work Package of Strand 1 Critical Technologies were identified. The STACCATO taxonomy was used for classifying security functions and technologies in order to prepare the Critical Technologies List. This taxonomy was chosen because it not only includes the basic technology level, but also higher levels of sub-systems, systems and systems of systems. It is highly flexible and *de facto* becoming a standard.

Work Package 1 was planned as an iterative analysis and consultation process. In this process, background technical knowledge of the Consortium Parties was to be combined with input from external stakeholders including technical experts, industry, end-users, branch organisations and public bodies as needed.

The 1st Consultation Campaign was closely associated to Strand 1 "Critical Technologies" with additional relevant results being expected for Strand 2 "Emerging Technologies". The most prominent activity within this campaign was the staging of five workshops held in five European countries in the respective languages but applying the same methodology ("Parallel Workshops", see section 3.1.2.2).

2.2.2 Identification of Critical Dependencies

Work Package 2 dealt with the identification of Critical Dependencies. Such Critical Dependencies arise if European industry is not self-sufficient in providing critical technologies/systems/capabilities to end-users.

To identify Critical Dependencies, the Critical Technology List obtained from Work Package 1 was checked for extra-European dependencies concerning

- intellectual property rights (IPR, through patent analysis),
- trade and academic restrictions (though analysis of publicly available legal texts),
- restrictions due to high classification in dual-use technologies, and
- economic challenges (e.g. shifting production sites, lack of specialisation in EU industry, deficient research orientation, hindering or underdeveloped norms and standards, failing business models).

The analysis of Critical Dependencies in security technology was a novelty in itself. As in other parts of the ETCETERA project, the analysis was performed by combining known methods that have not been connected before.

2.2.3 Identification of Alternative Technological Solutions

Work Package 3 proposed and prioritised alternative technological solutions to alleviate the Critical Dependencies identified in Work Package 2.

Before the ETCETERA project started, the types of Critical Dependencies encountered were unknown. They could be limited to an essential component (e.g. radiation hardened electronic chips) from a non-European supplier, or be more complex sub-systems or systems (e.g. software defined radio or ion mobility spectroscopy for detection of dangerous substances). The nature of the Critical Dependency was also unknown (see above). For this reason, a flexible and multifaceted approach was planned to be used, based on the TEPID-OIL method,[3] which was originally developed to optimise defence acquisition strategies. The specific advantage of the TEPID-OIL method is its very broad approach that reaches far beyond just evaluating scientific and technological solutions. For example, a Critical Dependency may be removed by using available technologies in a new or different way, or by changing the way information or infrastructure are used. As the TEPID-OIL methodology stems from a military context, it had to be adapted for the use in civil security research planning (see section 3.1.4.2).

3 The acronym stands for "lines of development": Training, Equipment, Personnel, Infrastructure, Doctrine & concepts, Organisation, Information & Logistics

2.3 Emerging Technologies

2.3.1 Scanning for Emerging Technologies with security implications

In Work Package 4, Emerging Technologies were scanned for their security implications in a 10 to 20 years' timeframe. Implications were taken into account regarding future high risk/high pay-off opportunities (main focus), but also of future threats (secondary focus).

Three methods to scan for Emerging Technologies were performed in a parallel fashion:

- Fraunhofer INT exploited its broad technological knowhow gained from activities like the Overall Technology Forecast and the Defence Technology Forecast, a comprehensive description of technological developments with relevance to defence use.
- Isdefe applied a technique originally established for the Spanish Ministry of Defence to prepare a further independent list of Emerging Technologies with security implications.
- AIT used bibliometrics for the survey.

A comparative analysis of the results of these three methods was then performed. To the best of our knowledge, such a broad integration of methods and results has never been attempted before in the field of security research. Furthermore, a novel method for the priorisation of technologies based on the Weighted-Bit Assessment Method (WBAM) was introduced and applied (see section 3.2.1.2).

2.3.2 In-depth analysis and 2nd Consultation Campaign

Some of the Emerging Technologies identified to be most relevant were further analysed in Work Package 5. These in-depth analyses were carried out by experts of consortium members, with external specialists being asked for highly specific input. These analyses did not only include technical aspects, but also economic questions like future market potential. Furthermore, ethical aspects of the introduction of these novel technologies were analysed by CSSC, who also provided an "ethical helpdesk" that was consulted by all other consortium partners.

The 2nd Consultation Campaign was characterised by the parallel execution of three methods of expert involvement:

- a workshop methodology based on the Weighted Bit Assessment Method (WBAM, see section 3.1.3.6),
- an adapted Disruptive Technology Assessment Game (DTAG, see sections 3.2.2.3 and 3.2.2.4), and
- a scenario process (see sections 3.2.2.5 and 3.2.2.6).

These very different methods to assess future developments were applied in a parallel way to enable methodological comparison. The parallel execution of these methods had another advantage: The WBAM and the DTAG/SETAG (a serious gaming approach) were highly innovative and had never been tried before in the context of assessing technologies for civil security. As the risk of failure was thus inherent to both, they were combined with the well-established scenario method to ensure that, even in the worst case, input of sufficient quality could be produced for the further proceeding of the ETCETERA project.

2.3.3 Development of recommendations for an Emerging Security Technology Research Agenda (ESTRA)

In Work Package 6 all results on Emerging Technologies, including the results of the 2nd Consultation Campaign, were considered for the development of recommendations for an Emerging Security Technology Research Agenda (ESTRA). Lessons learned from the analysis of Critical Dependencies were planned to be included in the recommendations. Measures were taken to ensure that ESTRA is compatible with existing national and European research strategies. Ethical aspects were also taken into account.

Additionally, further economic modelling was developed and used to cover the high risk/high pay-off aspect of Emerging Technologies (see section 3.2.3.2).

3 Proceedings and Results of the ETCETERA project

3.1 Strand 1 "Critical Technologies"

3.1.1 Definition

There is no commonly accepted definition of a Critical Technology. The ETCETERA process started with the definition given in section 2.2, which was refined at the start of the project. This led to the following definition:

A Critical Technology is any technology (including equipment, skill, system, service, infrastructure, software or component) that is required by any organisation with a legal or contractual responsibility for security of citizens in Europe to properly perform its duties.

While this definition is still not perfect and open to interpretation, it does include less tangible aspects such as skills, services and software. Hence any "technology" fulfilling the above definition is to be considered as a Critical Technology. During the process of identification a wide range of technologies has been included, even such ubiquitous technologies like cement production.

3.1.2 Critical Technology List (CTL)

3.1.2.1 Generation of the Critical Technology List

The STACCATO taxonomy[4] was used as a starting point to generate a list of Critical Technologies. The general idea was that if a technology, listed in STACCATO, has at least one security application for which it is found to be essential, it was included in the Critical Technology List. The STACCATO taxonomy is extensive, containing several hundred items which are all in some way related to security as defined by the authors of the original STACCATO taxonomy. One task of the ETCETERA project was to distil from this list those technologies essential for security (as distinct to simply related to security). An additional task was to complement the STACCATO taxonomy with any missing items.

The method used to complement the STACCATO taxonomy was primarily through expert consultation and use of open scientific and commercial literature. More concretely, the process has been to search the open literature and analyse this from the point of view of security (drawing, where possible, a distinction between applications for security and applications for defence). Additionally, a series of workshops ("Parallel Workshops") was organised, using the World Café method.

Table 1 represents an exemplary selection of technologies assessed for the Critical Technology List. For a detailed description of the process and the results please refer to Deliverables 1.2 "Validated List of Critical Technologies" and 1.3 "Documentation of methods and workshops".[5,6]

4 The STACCATO taxonomy was produced by a previous EC funded PASR project: http://www.asd-europe.org/site/fileadmin/ user_upload/ STACCATO_final_taxonomy.pdf

5 Malek Khan, Steven Savage, Aziz Ouacha (FOI), "Validated List of Critical Technologies", ETCETERA Deliverable 1.2, September 2012

6 Malek Khan, Steven Savage (FOI), "Documentation of methods and workshops", ETCETERA Deliverable 1.3, October 2012

	STACCATO Taxonomy	Security aspects	Suppliers (examples only)
100	**Structural materials and technologies and structural effects analysis**		
100-7	Metal-matrix composites	Used as heat sinks for electronics in demanding applications, e.g. space where low/controlled thermal expansion is needed. Most common are aluminium-based MMCs containing SiC, but for some applications copper/diamond has been tested. Also used as structural elements, e.g. tubular frames where thermal expansion must be limited, e.g. in optical systems (telescopes), satellites and similar applications. Boron-aluminium composite is used in the space shuttle, graphite-aluminium used in Hubble space telescope. Some studies on titanium-titanium carbide fibre composites are relevant for e.g. aerospace turbines.	Special metal matrix composites might be a critical technology, but not the common composites often used in automotive and transport. E.g. Lockheed-Martin Marietta, but they likely only build the structure and another manufacturer produces the material.
100-11	EM radiation absorbers	Absorbers for EM (electromagnetic) radiation include e.g. stealth coatings for military applications, but these are also used in electronic equipment (e.g. microwave communications) and in anechoic chambers for testing and certification of electronic equipment	Information on EM absorbers for military applications is highly restricted. In the military domain this is definitely a critical technology, but if military applications are excluded, purely civilian uses do not demand high performance. The materials used (carbon, metals, etc.) are not likely to be critical.
100-12	Magnetic metals	This is a very broad category, including iron, nickel, cobalt, metallic glasses, and some of the rare earth metals. They are used in transformers, many types of sensors and actuators, both at room temperature and high temperature. This topic could also include rare earth metals and their widely used magnetic alloys of neodymium-iron-boron and cobalt-samarium. These are widely regarded as critical materials.	Nickel and cobalt may be critical, iron occurs widely in Europe. The rare earth metals are supplied to a very large degree by China, where there are several manufacturers.
101	**Light and strong materials, surface treatments.**		
101-13	Smart textiles	Meaning textiles with sensors integrated for monitoring the wearer's health, e.g. 1st responders. This is an emerging technology area, but dedpite of the current low TRL it will definitely mature within the near-midterm future (5-10 years).	See FOV Fabrics, Öztec Textiles (Turkey)
104	**Survivability and hardening**		
104-2	Blast and shock effects	Protection of humans against blast and shock involves many materials. How they are used in structures is also important, i.e. design of the structure and use of the optimum material in the best way. Materials such as Kevlar, Nomex, Dyneema and other ballistic fibres are important for protection against blast, splinters, knives and bullets. Ceramics for body armour are used by both military and civil organisations, including police and civilian security forces. Blast curtains in security installations and government buildings, also simple constructive designs as defence perimeters, blast wave deflection elements can mitigate human injury and construction damage in extreme events.	Kevlar (http://www2.dupont.com/), Dyneema (dyneema), Scanfiber (http://www.scanfiber.dk/), Twaron (http://www.teijinaramid.com/)
108	**Photonic/Optical Materials and Device Technology**		
108-3	Active and adaptive optical systems (material, sensors, actuators,...)	Adaptive optics are used e.g. in astronomy, to correct for atmospheric disturbance and for correcting defects in other optical systems. Optical devices are increasingly being used in security devices, e.g. retina scanners	See e.g. Silas (http://www.cilas.com/adaptative-mirrors.htm)

	STACCATO Taxonomy	Security aspects	Suppliers (examples only)
110	**Sensor Technology and Components**		
110-1	Neutronic detection technologies (neutron tubes, ...)	The definition of this item was deemed unclear. Nevertheless the detection of nuclear material is a relevant topic for civil security.	
110-2	X-ray technologies	Detection of weapons and dangerous devices (bombs) in bags, suitcases, packages	See e.g. (http://www.airport-suppliers.com/supplier/Detection_Technology_Inc/) for components of X-ray scanners and Smiths Detection for a complete range of detection technologies including x-ray scanners
110-12	Hyperspectral technologies	Today emerging in the military field for detection and identification, useful for detection of fats, contaminants in food	There seem to be 2-3 European suppliers, see e.g. http://www.kayser-threde.de/
111	**Electronic components**		
111-2	III-V Compounds	This is a commonly used term to include a family of semiconductors created from aluminium, gallium, and indium (group III elements) with phosphorus, arsenic, and antimony (group V elements). Common componds are GaP, GaN, AlGaAs, etc.	The chemical element itself may be a critical material, e.g. indium is not widely available. The other elements should be checked for critical dependence.
113	**Information technologies**		
113-4	Data and Information fusion technologies	Many existing sensor systems, but also emerging technologies like data fusion combining physical data from a sensor system with contextual data from e.g. data mining on the www	
113-10	Jamming and anti-jamming technologies	Protect against IEDs during VIP transport, protection of sensitive infrastructures	See e.g. SESP (http://www.sesp.com/)
120	**Human sciences, including research and studies**		
120-14	Human behaviour models	Crisis management and human behaviour models could be used for: preventing or mitigating a crisis situation by means of models to evaluate/optimise the safety and security level of any critical infrastructure according to potential or implemented protective measures.	
121	**Biotechnology**		
121-11	Decontamination techniques	Security of food and water	See NIJ (https://www.ncjrs.gov/pdffiles1/nij/189725a.pdf) for a list of equipment suppliers

Table 1: Critical Technology List (CTL, examples only)

3.1.2.2 Parallel Workshops

Five "parallel" workshops were organised from March to June 2012, in Spain, Germany, Italy, Sweden, and France. Each workshop was held in the national language to enhance communication. Participants in the workshops were selected to represent end-users, companies, scientists and others. For the recruitment of these stakeholders a double stranded, multi-level strategy was applied:

- The "push" strategy used the networks already available to the consortium parties (technical experts, knowledge networks, and points of contact in external organisations), information available from previous security R&D activities (both by consortium

parties and other research organisations), and information gained through network analysis methods. Especially the Research and Technology Organisations (RTO) in the consortium could draw from a large pool of technical experts.
- The complementary "pull" strategy was a very open approach using advertising through professional organisations, press releases and via the internet.

A preparatory meta-workshop was held to both train the organisers of the parallel workshops in regard to the World Café method and to discuss questions apt to obtain useful information about Critical and Emerging Technologies. The following two questions were chosen for all five parallel workshops:

Question 1
Imagine you are an end-user that wakes up one morning, goes to work and finds a few things broken or missing. They cannot be replaced within a few days. Which things are gone in your worst nightmares? Do you have inspiring ideas for alternatives?

Question 2
Imagine you are an inventor. What would you create to help you at work if there were no time limits or budget constraints? Feel free to bend the laws of physics!

A total of 72 stakeholders participated in the five workshops, many of whom had not been involved in European security research before. The participants enjoyed the World Café format, as it allowed easy participation and provided good opportunities for networking.

For several reasons it was hard to align the workshops with the generation of the Critical Technology List (CTL). The challenges included delays in the production of a first version of the CTL and the problem that the workshop format (World Café method) was not suitable to discuss more than a few technologies. Nevertheless, the results gathered from the workshops were used at a later stage for the validation process of the nearly final CTL version (Question 1). Furthermore, the results from Question 2 were fruitful for the work of Strand 2 "Emerging Technologies", where identification and analysis of Emerging Technologies were conducted (see section 3.2.3).

In general, the approach of performing parallel workshops as described above proved to be more complex and costly than to just organise an "ordinary workshop". Nevertheless, it clearly facilitated the involvement of stakeholders that would normally not be available to European research planners simply because of language barriers. The World Café method was very useful for participant motivation and involvement. On the other hand, it has been shown to be more conducive for the generation of novel ideas than for the assessment of a large number of possible options.

For details concerning the method applied during the workshops please refer to Deliverable 1.3 "Documentation of methods and workshops".[5] The reports from the workshops were gathered in Deliverable 1.1 "Stakeholder Workshops".[7]

3.1.3 Analysis of Critical Dependencies

3.1.3.1 Critical Dependencies

Critical Dependencies arise if European industry is not self-sufficient in providing critical technologies/ systems/capabilities to end-users. To identify such Critical Dependencies the Critical Technology List was analysed regarding extra-European dependencies. The objective of this activity was to unveil factors leading to dependencies of the European security industries due to patents, trade restrictions, contraction restrictions, new economic models and shifting production to third countries, long-term research insufficiency, industrial concentration, and other factors.

A set of analyses was applied to the list of Critical Technologies in order to end up with a shorter list of technologies in which Europe is dependent:[8]

- Several types of patentometric analyses
- A bibliometric analysis
- An analysis of knowledge protection measures and trade barriers
- An analysis of economic barriers

7 Joachim Burbiel (Fraunhofer), Stefanie Goymann (Fraunhofer), Javier Herrera (Tecnalia), Carlo Dambra (Ansaldo STS), Françoise Simonet (CEA), Steven Savage (FOI); "Stakeholder Workshops", ETCETERA Deliverable 1.1, September 2012

8 Antonia Bierwirth, F. Javier Herrera (Tecnalia), "Intermediate report on critical dependencies", ETCETERA Deliverable 2.1, July 2013

A "Weighted-Bit Assessment Table for Critical Dependencies" (WBAT-CD) was developed to condense the results and to prepare the exploration of alternative technological solutions.

3.1.3.2 Patentometrics and bibliometrics

Two project partners conducted scientometric analyses in order to identify Critical Dependencies.

The Austrian Institute of Technology (AIT) started by correlating STACCATO taxonomy items with International Patent Code (IPC) groups. The IPC groups were then analysed for the number of patents granted to European entities as compared to non-European entities to identify the relative strength of European knowledge production (years 2004 to 2008). This was followed by an analysis focussed on Critical Technology areas in which Europe is comparably weak. The analysis of AIT was completed by a closer look at patenting trends for some selected technologies in recent years (2010 to 2012).[9]

The Commissariat à l'énergie atomique et aux énergies alternatives (CEA) analysed nine technologies more in depth:

- 110-2 X-ray technologies
- 110-3 Gamma-ray technologies
- 110-5 IR Spectroscopy
- 110-10 RF sensor technologies
- 110-19 Techniques for discrete surveillance (uncooled IR sensors)
- 119-8 Rapid diagnosis of infectious disease
- 121-9 Food testing and control techniques
- 200-11 Biological substances detectors
- 200-23 Terahertz detectors

CEA looked at the distribution of patents concerning the localisation of the applicants. Strengths and weaknesses of European applied research were thus identified for these areas. Furthermore, CEA conducted a bibliometric analysis of scientific publications in selected areas in order to assess the relative strength of European basic research.

3.1.3.3 Knowledge protection and trade barriers

In order to assess the availability of extra-European technology to European industry and security end-users, a set of knowledge protection protocols and trade control regimes were analysed by Isdefe and Tecnalia:

- the Information Sharing Traffic Light Protocol (ISTLP)
- World Intellectual Property Organization (WIPO)
- World Trade Organization (WTO)
- the Trade Barriers Regulation (TBR)
- entries in the EU Market Database (MADB)
- several international agreements on weapons trade and dual-use products

3.1.3.4 Economic barriers

As a last step in the process of unveiling the factors that lead to the dependence of the European industries in the security sector, regarding the Critical Technologies previously identified, the task of analysing economic barriers was focused on the analysis of market restrictions.

For this, both open source literature and economic causes for market failure were analysed for the EU security market as a whole and by subgroups defined by economic criteria. As a result, several hypotheses have been advanced to account for the deficiencies of the EU security market and form the basis of this research task:

- Market fragmentation
- Inefficient research funding in EU Member States
- Limited industrialisation and commercialisation support
- Certification and standardisation barriers

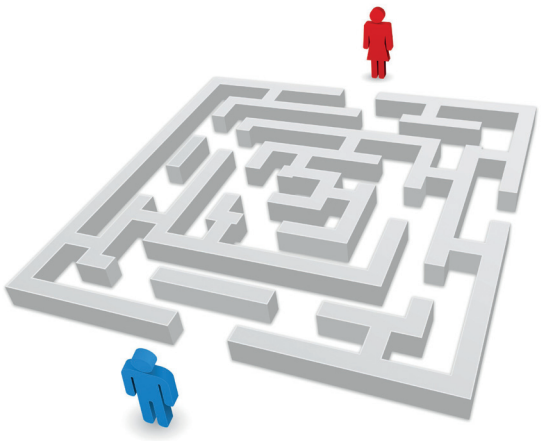
3.1.3.5 Conclusion of the critical dependency analysis

Taking into account all activities described above, the following conclusions were drawn:

Conclusions on technology dependence

- The share of the EU-27 on worldwide patents is slightly below average for all Critical Technologies. Even though differences might be small, it is worrying that it affects virtually all technologies

9 Beatrix Wepner, Manuela Kienegger, Georg Zahradnik (AIT), "Report of the Analysis of the Regional Distribution of Patents", ETCETERA Working Document 2.2, May 2013



unveiling a characteristic trait. The USA and Asian countries exhibit a converse feature.

- In the security sector, Europe is especially weak in technologies encompassed in the physics and electricity categories of the IPC coding system.
- Other figures resulting from the analyses revealed that Europe is falling behind in the subclasses Wireless Communication Networks and Electrical Digital Data Processing, at least with respect to patents in the period of the study.
- Even when only looking at a small sample of technologies within a given domain of Critical Technologies for security, the position of Europe relative to the number of patents is comparably weak.
- The countries of the European Union only produce high numbers of scientific papers in areas that constitute major research areas around the world. Consequently, no European dominance can be identified for any research area. This could point to poor research prioritisation.
- Insufficiency in research activities can be clearly identified at least in the following areas: automation and control systems; manufacturing and petroleum engineering; material sciences and textiles; and primary health care.
- Incentives on research are not able to change the conservative position of end-users concerning the adoption of new technology. Current metrics and evaluation criteria with respect to research do not consider the concept of dependency as crucial.
- Growing social concerns on the use of technology are imperfectly taken into account in security technologies business models, blocking innovation and prospective European leadership.
- The absence of an EU-wide scheme for standardisation and certification of security equipment hampers efficiency in technological response to security threats.
- There is a market failure stemming from the current culture of joint operations between integrators and technology-niche SMEs regarding innovation absorption. Value chains in the sector must be improved.
- Models of technology and knowledge transfer from research institutions and technology innovators need serious refining as they are regarded one of the main factors of the low impact of research in the market. Creativity in agreements and exploitation conditions are highly demanded.
- In order to consolidate European technology, a "fast-track to first references" with the support of local end-users through innovative mechanisms including IPR sharing seems promising.[10]

Areas for improvement

- A permanently updated list of Critical Technologies for security is needed. Current lists lack homogeneity and will become outdated swiftly.
- Consistent criteria are required as to what a Critical Technology is. Clear separation between technology, systems, and services would help concentrate technology efforts while handling the rest of the dependencies in a different way.
- Aspects related to human sciences are underrepresented in STACCATO.
- For the analysis to be conclusive, it must be undertaken on a one technology or technology family basis only. If cross-analysis is needed between two or more technologies it needs to be based on individual analyses. Big scale analysis of all the technologies seems out of reach even for an experienced team in a reasonable timeline.

10 The "Pre-Commercial Procurement Scheme" within HORIZON2020 can be seen as such a process.

3.1.3.6 Weighted-Bit Assessment Table for Critical Dependencies (WBAT-CD)

The Fraunhofer Institute for Technological Trend Analysis INT has previously created a Weighted-Bit Assessment Method (WBAM) for the evaluation of dangerous chemicals[11]. A prominent feature of this method is that all information is depicted as one bit (zero/one) answers to yes/no-questions. The WBAM was mainly devised to serve as an easily understandable planning support tool that enables interaction between stakeholders of different backgrounds.

For the ETCETERA project an adapted WBAM table, called "Weighted-Bit Assessment Table for Critical Dependencies" (WBAT-CD), was developed and used for the evaluation of findings within Work Package 2 "Identification of Critical Dependencies" and Work Package 3 "Identification of Alternative Technological Solutions". For this, a set of items, sorted in sections and sub-sections was developed through an iterative process (see Figure 3). While the section "Nature of the Dependency" is associated to Work Package 2, the section "Obstacles to closing the gap" prepared Work Package 3.[12]

The functioning of a typical Weighted-Bit Assessment Table relies on a completely filled binary matrix (yes = 1, no = 0). In the case of the WBAT-CD the lack of information concerning the many "Critical Technologies" was a major problem. In order to incorporate all information available, which was in some cases of the nature "a specific problem exists for a given technology" and in other cased of the type "we know that a specific problem does not exists of a given technology", a ternary system of yes = 1, no = -1, and unknown = 0 was introduced.

A WBAM-assisted workshop took place on 23 April 2013 as part of the ETCETERA Spring Meeting at the premises of FOI in Kista, Sweden.

In preparation of the workshop, information previously generated within the ETCETERA project was integrated into the WBAT-CD matrix. The sources included draft reports on the regional distribution of patents,[9] some information provided by Isdefe on raw material dependencies, and information on production facilities and research capacities provided by Tecnalia and Fraunhofer.[13]

After a brief introduction to the method, the participants were split up into four smaller working groups. Each group was assigned to work on a specific thematic area ("IPR & Trade Restrictions", "Production Gaps & Capacities", "Market Inadequacies", and "Ethics"). They were instructed to fill as many matrix fields of their assigned sub-categories as possible, starting with the STACCATO technologies they felt easiest. The results of the four groups were later collated into one "joint" table. Figure 3 shows a section of the filled WBAT-CD matrix after the workshop.[14]

Due to severe delays in Strand 1 of the ETCETERA project, the possibilities of the WBAM to create "scenario scores" and to analyse data graphically could not be explored. However, it proved to be a useful tool for technology priorisation (see section 3.2.1.2).

11 J. Burbiel, N. Engelhard, S. Grigoleit, H. John, J. Schulze, "Gefahrenpotentiale von chemischen Kampfstoffen und toxischen Industriechemikalien - das Punktesystem", Bundesamt für Bevölkerungsschutz und Katastrophenhilfe -BBK-, Bonn: Gefahren und Warnung - Drei Beiträge. Rheinbreitbach: MedienHaus Plump, 27-58 (2009)

12 Joachim Burbiel (Fraunhofer INT), "Report on the adaption of the Weighted-Bit Assessment Method", ETCETERA Working Document 2.8, May 2013

13 Joachim Burbiel (Fraunhofer INT), "Report on the WBAM-assisted Workshop", ETCETERA Working Document 3.4, May 2013

14 The full WBAT-CD contains more than 280 items.

		NATURE OF THE DEPENDENCY									OBSTACLES TO CLOSING THE GAP									
		IPR & Trade Restrictions					Production Gaps				Capacities			Market Inadequacies				Ethical Issues		
		Essential IPR is held outside Europe.	There have been relatively few patent applications by European actors in the last years.	A relevant portion of the IPR is classified by government.	The technology is included in export control lists and/or has high potential for dual use (civil/military).	IPR & Trade Restriction SUBSCORE	There are no production facilities for this technology in Europe.	There are only three or less production facilities for this technology in Europe and/or there is a tendency to "offshore" the production of the technology.	The technology requires raw materials or intermediates that are not readily available in Europe.	Production Gap SUBSCORE	There is only very limited research capacity (institutions and/or human resources) for the technology in Europe.	There is a lack of systems integration capability.	Capacities SUBSCORE	The market for the technology is highly fragmented and/or a lack of standardisation troubles the marketing of the technology.	End-users are content with the solutions currently available. There is no requirement pull for new technologies.	Public funding is currently insufficient to foster the development of the technology.	Market Inadequacies SUBSCORE	Could this technology raise privacy issues?	Is it likely that this technology will be used to provoke any physical or mental harm to humans?	Could the technology be exploited by criminal organisations in the next few years?
	WBAM Factors:	1	1	1	1	X	2	1	1	X	2	1	X	1	1	1	X			
STACCATO-Taxonomy		In general: yes = 1 / no = -1																		
xxx-xx	Pure and Applied Madness	-1	1	-1	-1	-2	-1	-1	-1	-4	-1	1	-1	1	1	-1	1	1	1	1
100	**Structural materials and technologies and structural effects analysis**																			
100-2	Ceramic composites					0	-1	-1	-1	-4	-1	-1	-3				0			
100-3	Composites materials technology					0	-1	-1	-1	-4	-1	-1	-3				0			
100-4	Powder metallurgy					0	-1	-1	-1	-4	-1	-1	-3				0			
100-5	Dense alloys					0	-1	-1	1	-2	-1	-1	-3				0			
100-6	Organic composites					0	-1	1	0	-1	-1	-1	-3				0			
100-7	Metal-matrix composites					0	-1	1	-1	-2	-1	-1	-3				0			
100-8	Carbon-carbon composites					0	-1	0	-1	-3	-1	-1	-3				0			
100-10	Synthetics fluids and lubricants	1	1			2	-1	-1	0	-3	-1	-1	-3				0			
100-11	EM radiation absorbers				1	1	-1	-1	-1	-4	-1	-1	-3				0			
100-12	Magnetic metals					0	-1	0	1	-1	-1	-1	-3				0			
100-13	Superconductors				1	1	-1	0	1	-1	-1	-1	-3				0			
100-14	New metallic alloys				1	1	-1	0	1	-1	-1	-1	-3				0			
100-15	Metallic composites				1	1	-1	1	-1	-2	-1	-1	-3				0			
100-17	Concretes resistant					0	-1	-1	-1	-4	-1	-1	-3				0			
100-18	Anti-blast glasses					0	-1	1	-1	-2	-1	-1	-3				0			
100-19	Materials for thermal control					0	-1	-1	-1	-4	-1	-1	-3				0			
100-20	Nano components and structures (tubes, ceramics, …)					0	-1	0	-1	-3	-1	-1	-3				0			
101	**Light and strong materials, surface treatments**																			
101-1	Light materials for human protection				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-2	Light materials for site protection				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-3	Armor and anti-armor materials				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-4	Self-protective and explosive resistant material technology				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-6	Structural & Smart Materials				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-7	Surfaces treatments for improvement of mechanical properties	1	1		1	3	-1	-1	-1	-4	-1	-1	-3				0			
101-8	Surfaces treatments for improvement of life duration, corrosion reduction	1	1		1	3	-1	-1	-1	-4	-1	-1	-3				0			
101-9	Paints (without CoVs…)					0	-1	-1	-1	-4	-1	-1	-3				0			
101-10	Replacement of Cd, Hg, Cr	1	0			1	-1	-1	-1	-4	-1	-1	-3				0			
101-11	Simulation for surfaces treatment				1	1	-1	-1	-1	-4	-1	-1	-3				0			
101-12	Nano surfaces					0	-1	-1	-1	-4	-1	-1	-3				0			
101-13	Smart textiles				1	1	1	1	-1	2	-1	-1	-3				0			

Figure 3: Weighted-Bit Assessment Table for Critical Dependencies (WBAT-CD, section)

Code *	Short Title	Why selected?
101-13	Smart textiles	Dual use & production gap
110-1	Neutronic detection technologies	IPR, export control & production
110-2	X-ray technologies	IPR, export control & raw materials (L13)
110-3	Gamma technologies	IPR, export control & production
111	Electronic components	IPR plus various other issues
112-2	Digital signal processing technology	IPR, dual use & raw materials
113-10	Jamming and anti-jamming technologies	IPR & dual use (L13)
116-5	High integrity and safety critical computing	IPR (L13)
117	Information Security Technologies	IPR & dual use (117-12 is in L13)
121-5	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants	IPR & dual use (L13)
200	Sensors equipment	Various issues (210-2 is on L13)
407-3	Secure database management	IPR & market (L13)
504B-2	Simulation for decision making (real time)	Market problems (L13)

** The numbers refer to the STACCATO taxonomy.*
"L13" refers to inclusion to another list of prioritized Critical Dependencies developed within the ETCETERA project.

Table 2: Main list (technologies most highly prioritised for further analysis)

3.1.4 Recommendations for alternative technological solutions

3.1.4.1 Suggestions for Critical Technologies to be further analysed

In an attempt to promote discussion about which technologies to choose for further analysis in Work Package 3 "Identification of alternative technological solutions", prioritisation lists were derived from the Weighted-Bit Assessment Table for Critical Dependencies (WBAT-CD). For this, the following criteria were applied:

- Which technology seems to be particularly critical? (= many "1" entries in the WBAT-CD)
- What is the cause of the critical dependency? (as noted in the WBAT-CD)
- How much do we know about the technology? (How many fields have been answered in the WBAT-CD?)

The suggestions were sorted into a "Main List" of technologies most highly prioritised for further analysis and into a "Reserve List" of technologies that received slightly lower scores (see Table 2 and Table 3). In some cases, STACCATO categories have been put on the lists, especially if higher differentiation did not make sense for further analysis.

3.1.4.2 Alternative technological solutions

In order to overcome Critical Dependencies of Europe regarding security relevant technologies, the ETCETERA project was to propose alternative technological solutions for such technologies.

The process of finding alternative solutions relied on input from subject matter experts that have contributed with in-depth knowledge of the technologies and their applications, their thoughts of future developments and possible alternative solutions for the future. Expert opinion has been obtained through meetings, workshops, telephone interviews and written contributions. In some cases

Code *	Short Title	Why selected?
100-7	Metal-matrix composites	Production gap?
100-13	Superconductors	Dual use & raw materials
100-15	Metallic composites	Dual use & production gap
101-7 & -8	Surfaces treatments	IPR & dual use
107	Energy generation storage & distribution	IPR (and some other issues)
108	Photonic/Optical Materials and Device Technology	IPR (and some other issues)
109	Opto-electronics: Laser, optics and related devices	IPR (and some other issues)
110-5	IR Spectroscopy	IPR & export control
110-8	Terahertz technologies	IPR & export control
110-9	Terahertz Spectroscopy	IPR & export control
110-17	BGO detectors	Dual use & production
110-18	CdZnTe detectors	Dual use & production
112-3	Analogue/digital conversion technologies	IPR & dual use
113-4	Data and Information fusion technologies	IPR & dual use
114	Artificial Intelligence & Decision Support	IPR
115-1	Virtual and augmented reality	IPR
116	Computing Technologies	IPR
118	Communication technologies	IPR & dual use
119-1	Medical products and materials	IPR
119-8	Rapid diagnosis of infectious disease	L13
204-6	CB Countermeasures - Medical	Dual use (L13)
306A-2	Positioning and localization	IPR & production
312A-1	Population warning systems	Market problems
313A	Search and Rescue and evacuation	Market problems
401-1	Communication satellites	Dual use & production & raw materials
403-5	Transport helicopters	Dual use & production
411-5	Optimisation, Planning & Decision Support systems	Dual use (L13)
413-1	Rapidly Deployable Communication Infrastructure	L13
500-4	Scenario generation	Market problems
504B	Scenario and decision simulation	Market problems

** The numbers refer to the STACCATO taxonomy.*
"L13" refers to inclusion to another list of prioritized Critical Dependencies developed within the ETCETERA project.

Table 3: Reserve list (technologies highly prioritised for further analysis)

experts have been contacted with follow-up queries and requests for additional information.[15]

Additionally, the TEPID-OIL[16] method was proposed to compile a short-list of Critical Technologies, separating those dependencies which could be eliminated by alternative technological solutions from those which could be eliminated by non-technological solutions. Nevertheless, this short-listing was not necessary, as the "main list" derived from WBAT-CD (Table 2) was considered to be short enough to study all technologies included. However, the general approach was considered to be valid and the applicability of the TEPID-OIL method was studied as originally planned.

The TEPID-OIL method was originally developed for military technologies and situations and needed adaption to a civil setting. It was therefore extended by additional parameters: Incitement/psychology and Economy/market mechanisms. This adapted method was consequently called ITIPOLITRE.[17]

To test the functionality of ITIPOLITRE the case of x-ray equipment used in airport security checks was used, and ITIPOLITRE was applied in order to identify alternative solutions. The method was found to work satisfactorily, identifying a number of "expected" alternatives and also a number of unexpected alternatives, showing the strength of the method in developing unconventional solutions.[18]

Table 4 summarises the results of the identification of alternative solutions.[19]

As expected, in some cases additional research was proposed, while in other cases different measures seemed to be appropriate (e.g. standardisation or awareness raising).[20]

STACCATO Code	Short Title	Suggested Solutions		
		Basic research	Applied research	Other measures
110-1	Neutron detection technologies	X	X	
110-3	Gamma technologies		X	
113-10	Jamming technologies and Anti-jamming technologies		X	X
117	Information security – Secure communication	X	X	X
121-5	Rapid analysis of biological agents and of human susceptibility to diseases & toxicants		X	X
200-4 / 210-2	Explosives detection sensors/equipment		X	
112-2	Digital signal processing technology		X	
101-13	Smart textiles		X	X
504B-2	Simulation for decision making (real time simulation)		X	

Table 4: Types of solutions suggested for overcoming selected Critical Dependencies

15 Steven J Savage, Malek Khan, Riitta Räty, Camilla Trané (FOI), "Report on Validated Alternative Technological Solutions", ETCETERA Deliverable 3.1, November 2013

16 The acronym stands for "lines of development": Training, Equipment, Personnel, Infrastructure, Doctrine and concepts, Organization, Information and Logistics

17 Incitements/Psychology, Technology/Equipment. Information/ Information systems, Personnel, Organization, Logistics, Infrastructure/ Facilities, Training/Education, Rules, Economy/Finance

18 Riitta Räty (FOI), Camilla Trané (FOI), Malek Khan (FOI), Steven Savage (FOI), "ITIPOLITRE – a method to identify a wide range of alternative security technologies", ETCETERA Working Document 3.1, October 2013

19 The number of items in Table 4 is lower than in Table 2, as some items have been joined.

20 Malek Khan, Riitta Räty, Steven Savage, Camilla Trané (FOI), "Identification and in-depth analysis of alternative technological solutions", ETCETERA Working Document 3.3, November 2013

More details on the solutions proposed are documented in Table 5.

There is considerable public concern about the proliferation of surveillance and monitoring technologies, many of which have been developed quickly due to urgent needs and without regard for integrity and privacy of European citizens. It is important that future security technologies take these concerns into account, otherwise there is a risk that non-acceptance will limit the applicability of certain technologies. Nevertheless, not all security technologies have the same potential to raise integrity issues. For this reason experts in ethics and integrity have been partners in ETCETERA, and have been consulted in developing the alternative solutions to critical dependencies. Each alternative solution has been assessed for ethical impact (using a 4-level scale) by the subject matter technical experts consulted. These are of course not necessarily experts in ethics, so additional expertise from the partner Centre for Science, Society and Citizenship (CSSC) has been included.

Two of the alternative technologies analysed in-depth were presented and discussed in an ethics workshop in Rome on 9 and 10 September 2013, which also served to disseminate information about ETCETERA to a wider audience.[21]

21 CSSC, "Report on the Dissemination Workshop: Ethics, Governance, and Societal Implications of Emerging Security Technologies", ETCETERA Deliverable 7.2, September 2013

Code*	Name	Security aspects (applications)	Users (examples only)	Nature of dependency
110-1	Neutron detection technologies	Detection of nuclear materials (e.g. uranium, plutonium) at borders, airports to prevent trafficking of nuclear materials	Border security personnel	**WP2:** IPR, export control & production **WP3:** Detectors manufactured in US or by multinational companies. There is proprietary development in EU (e.g. France)
110-3	Gamma detection technologies	Detection of radioactive materials at borders, airports, nuclear power plants, fuel production facilities, research labs and hospitals.	First responders, border police, radiation protection officials, personnel in nuclear facilities.	**WP2:** IPR, export control & production **WP3**: EU is less dependent than in neutron detection, there are European production facilities.
113-10	Jamming technologies	Deactivation of bombs or to prevent communication (e.g. during terrorist event)	Police, Security organisations.	**WP2**: IPR & dual use **WP3**: Jamming devices can be comparably simple therefore the technology is not critical.
113-10	Anti-jamming technologies	Anti-jamming is relevant for: Secure communication e.g. for first responders, protection of electronic equipment in critical infrastructure and anti GPS jammers	First responders, airport security, critical infrastructure security personnel, transportation of valuables, security organisations.	**WP2**: IPR & dual use **WP3:** IPR & duel use dependencies. Limited knowledge and sharing of information within Europe. Classified information is a predominant.
117, 117-18	Information security technologies, Secure communication protocols	Secure communication, e.g. internet and cell phone networks. Relates to information security and threats. Can be e.g. unauthorized access or intentional damaging/controlling of systems. Protect data during transport between two nodes (e.g. person-person, person-company, critical system-critical system).	Communication is a foundation of modern society so users span from authorities, companies, organisations, and critical infrastructural management to the individual.	**WP2:** IPR **WP3:** Manufacturers of communication equipment often located outside of EU. This is a dependency e.g. because of the risk of hardware Trojans.
121-5	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants	On site (field-based) analysis of biological agents (e.g. border controls or in subways) Detection and identification of biological agents in hospitals and experts organizations.	Healthcare personnel, expert agencies, emergency responders. Customs/border control personnel, Public transport security personnel	**WP2:** IPR & dual use **WP3**: IPR
200-4/ 210-2	Explosives detection sensors/equipment	Aviation security. Forensic analysis. Potentially the technique can be used in other critical infrastructures (e.g. harbours, subways, embassies, large events).	Airport security personnel, police.	**WP2:** Various issues. **WP3**: Within EU there is a lack of standards, which makes the market restricted. Classified information limits the markets production. Dual use dependencies.
112-2	Digital signal processing technology (for image processing)	Surveillance of public spaces and security of important facilities	Security companies, in some cases police	**WP2:** IPR, dual use & raw materials (for the entire digital signalling process field) **WP3:** The dependency is probably not that strong. Some limitations due to IPR and export limitations (specific for analysis of image processing)
101-13	Smart textiles	These textiles with integrated sensors can potentially be: Integrated in clothes to monitor the wearer's health status.	Fire-fighters and other 1st responders	**WP2:** Dual use & production gap **WP3**: Dual use restrictions
504B-2	Simulation for decision making (real time simulation)	Real time decision support tools that potentially could be used, e.g. in ambulances and emergency vehicle routing.	Emergency centre personnel, first responders.	**WP2:** Market problems **WP3:** No particular dependencies.

** The numbers refer to the STACCATO taxonomy.*

Table 5: Overview of alternative solutions and further development of Critical Technologies with Critical Dependencies.

Problems in the use of the critical technologies todays	Suggested future solutions (Reduce the dependency, Introduce novel solution, Develop the current solution, Other measures)
The supply of 3He is vital, but steadily getting less secure. Equipment exists at some borders but not all. Equipment needs specialised personnel.	**Reduce the dependency:** Develop new detection materials, to become less dependent on 3He (e.g. 6Li and 10B). **Develop the current solution:** Develop new detection techniques and methods that more easily discriminate between neutrons and gamma radiation.
Today's technology is limited in identifying exact substance(s) and compositions. False positives can be a problem.	**Develop the current solution:** New detection materials, techniques and methods to better identify exact substances and to reduce false positives. This could include: Combining high efficiency and high resolution within a cheap device; New detector materials for both neutrons and gamma. Develop spectroscopic portal monitors making it easier to discriminate the source of the gamma radiation and reduce false positive results; Automatic identification routines to deal with mixed sources.
Jamming devices require quite a lot of power. The electromagnetic radiation from the devices is legally restricted.	**Develop the current solution:** Further develop devices for protective jamming to increase the usability. **Other measures:** Provide the public with information regarding risks related to wireless solutions and jamming.
In communication speed and functionality are favoured over security. The technology is not widely used today.	**Develop the current solution:** Develop devices that can locate the jamming signal; Develop Protection of critical infrastructure against electromagne- tic radiation; Develop protection to jamming by accessibility (protection by considering distance and location) **Other measures:** Investigate the vulnerabilities in electronics and where they are used and potential consequences of jamming. Political issue to establish standards/legalisation for the design of systems (especially the next generation mobile phone network standard and next generation of mobile communication systems used in crisis management). **Reduce the dependency:** Facilitate common European development of technology and standards.
Function (availability, speed etc.) is favoured rather than security. Few built in security measures e.g. authentication or choice of security level. Industrial control- and information systems can lack in security due to outdated security measures.	**Develop the current solution:** Develop measures to secure the information rather than the wire or transmission medium (Object based security); Develop a digital identification system for authentication; Develop new protocols for communication with better authentication; Develop ways that allowing the users to decide the route of communication; Develop protocols that allow the user to choose the security level or that the system adjusts the security level according to the information; **Other measures:** Facilitate a political discussion concerning legal demands on secure communication, e.g. the balance between privacy and need to intercept potentially criminal communication; Implement new and more secure standards for industrial control- and information systems. Develop a standard/notation that rates the security of a system as a decision aid; Heightened risk awareness in the field of industrial control- and information systems.
The traditional analysis methods are often slow and expensive. The methods often suffer from false positive results.	**Introduce novel solution:** Develop better capacity to identify exposure and transmission patterns; Investigate possibility of simple C/B collectors attached as a permanent part of first responders uniform for automatic collection of samples that when needed can be sent in for analysis; With the same principle as above develop simple C detectors that monitor the long term exposure to hazardous substances. **Other measures:** Implement measures to raise awareness among higher management levels for biological threats. **Develop the current solution:** Develop devices/chips that allow for analysis of many different agents/substances at the same time.
Detection is still challenging (many false positives and negatives, difficulties in differentiation between explosives). Tracking the origin of explosives in forensic analysis is difficult today. Use of animals restricted by time and cost of training animals and lack of quantitative information.	**Reduce the dependency:** Development of common EU standards for explosives detection. Facilitate common European development. **Develop the current solution:** Develop devices that can detect explosives at a distance. This requires new procedures, legalization and techniques. Develop small local mobile standard technologies that are more specific, sensitive and produce less false negatives.
The systems produce large amounts of data. Integrity issues.	**Introduce novel solution:** Investigate possibilities of e.g. pressure sensitive carpets (smart floors) or other non-visual technologies that track people's motion to find anomalies. **Develop the current solution:** Develop systems with reliable and automatic detection of security threatening behaviour which simultaneously protect privacy. For this image processing algorithms need to be developed (e.g. to discriminate between foreground and background, or to detect anomalous behaviour)
The technology is currently being developed to make the power sources and antennas sufficiently small. There might be ethical issues involved in monitoring firemen's health.	Develop the current solution: Investigate possibilities to monitor hazardous substances by integrating smart textiles in geotextiles, curtains or e.g. furniture. Investigate possibilities to coat textile materials so that e.g. exposure to hazardous substances can be more easily detected or decontaminated. Further develop heat regulating materials.
Today parts of simulation tools are used but not an entire system. Most tools are custom made at a high cost to be accurate enough.	**Develop the current solution:** evelop the numeric simulation systems to be used for handling whole systems and important aspects in environment, especially work on better algorithms.

3.2 Strand 2 "Emerging Technologies"

3.2.1 Scanning for Emerging Technologies with security implications

3.2.1.1 Scanning methods

As described in section 2.3, one of the two research strands of the ETCETERA project dealt with chances that Emerging Technologies offer for civil security and security industry. The scanning and prioritisation process within this research strand involved several research institutions and different foresight methods. It resulted in a list of Emerging Technologies, likely to become relevant for civil security issues in the time frame of 2020 to 2030.

This list of Emerging Technologies was based on the experience of technology foresight and technology experts. Three scanning methods were employed in parallel:

- AIT used a method based on bibliometrics for the survey,
- Fraunhofer INT exploited its broad technological knowhow gained from activities like the Overall Technology Forecast and the Defence Technology Forecast, and
- Isdefe applied its proprietary technique based on an in-house core team of technology experts supported by external researchers.

The methods to identify relevant technologies were compared and assessed to improve future strategic research planning.[22]

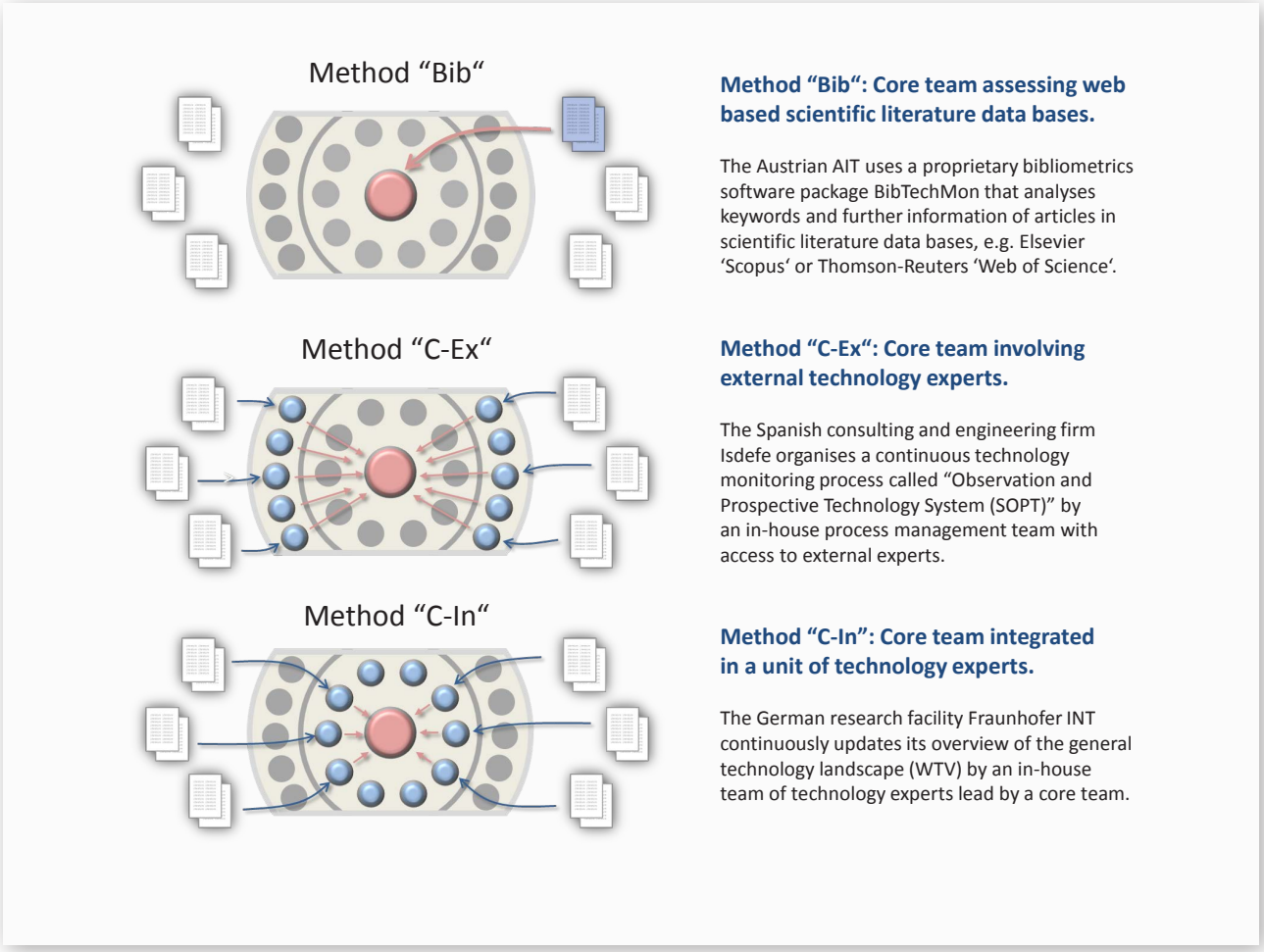


Figure 4: Schematic depiction of the technology scanning methods applied

22 Beatrix Wepner (AIT), Guido Huppertz (Fraunhofer INT), "Report on the comparative analysis of three methods to assess emerging technologies", ETCETERA Deliverable 4.2, November 2013

	TA1: Biometrics	SecRel	Time	Market	Appl	Ethics
	TA2: Communication Technology	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
1	Homomorphic Encryption	6	6	3	3	4
2	Post-Quantum Cryptography	6	1.5	3	3	3
3	Quantum Cryptography	6	3	-1	3	2
4	Chaos based Cryptography	5	3	1	3	4
5	Identity-based Encryption	4	0	-1	3	2
6	Clean-Slate Future Internet	3	0	-1	1	4
7	Artificial Immune Systems	2	3	1	1	4
8	V2X-Communication	1	3	3	-1	0
9	Cognitive Radio	1	3	-1	-1	6
	TA3: CBRN Identification	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
	TA4: Energy Technology	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
10	Smart Power Grid	4	0	3	3	0
11	Hydrogen Production and Storage Technologies	3	3	3	1	6
12	Small-scale Energy Harvesting	2	6	3	3	4
13	Electrochemical Energy Storage Materials	2	3	3	3	6
14	UUV/USV – Energy Storage and Propulsion	2	3	-1	1	6
15	Biomass-to Liquid Biofuel / Fischer–Tropsch Synthesis	1	0	3	-1	6
	TA5: Environmental Security	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
16	Earthquake Prediction	6	1.5	-3	3	6
17	Climate Engineering	3	1.5	3	0	6
18	Carbon Sequestration	1.5	6	3	0	6
19	Nanocomposites for Oil Removal	1.5	6	1.5	0	3
	TA6: Human Machine Interface	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
	TA7: Human Science	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
20	Automated Human Behaviour Analysis	5	3	3	3	0
21	Dark Web Terrorism Research	5	0	-3	3	0
22	Broad-Spectrum Antiviral Therapeutics	4.5	6	3	3	6
23	Reality mining - Machine Perception and Learning	1	3	3	-3	0
24	Agent based Modelling	1	3	1	-1	4
	TA8: ICT and Electronics	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
25	Quantum Computers	3	3	-1	1	4
26	Nanocomputers	1	0	1	-3	6
	TA9: Mobile Platform Technologies	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
27	Semantic 3D Scene Interpretation	6	3	1	3	0
28	Exo-Sceletons	5	3	1	1	2
29	Small Satellites	5	6	1	3	2
30	Stratospheric Platforms	5	6	-1	3	0
31	Autonomous Passenger Cars	4	3	3	1	4
32	Kinodynamic Motion Planning	4	4	3	-3	6
33	Active Protection Systems	4	6	-1	1	4
34	Indoor Navigation	3	3	3	1	0
35	E-Enabled Aircraft	2	3	3	3	6
36	Walking Machines	2	0	1	1	4
37	Chemical Robots – ChemBots	2	3	-1	1	0
38	Space Debris Removal	2	3	-1	-3	6
39	Biomimetic UUVs	2	6	-1	3	4

40	UUV/USV – Collision and obstacle avoidance technologies	2	3	-1	1	4
41	Ducted Fan Air Vehicles	1	6	3	1	2
42	Personal Air Vehicles / Flying Cars	1	0	-1	3	4
43	UUV/USV – Advanced Algorithms for Classification	1	3	-3	-1	6
	TA10: New and Smart Materials	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
44	Smart Textiles	5	3	3	3	2
45	Meta materials	4	3	1	1	2
46	Reinforced Light Alloys	3	0	3	1	4
47	SHM Systems	3	3	1	3	6
48	Liquid Armour	3	3	-1	3	6
49	Nanostructured Ceramics	2	3	3	-1	4
50	Polymeric Nanocomposites	2	0	3	1	4
51	Graphene	2	6	1	1	4
52	Fuzzy Fibres – CFK modified by CNTs	1	3	1	1	4
53	Smart Materials	1	0	1	-1	4
	TA11: Non-lethal Means	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
54	Non-Lethal Means to Preclude non Authorized Access	4	0	1	3	2
	TA12: Sensor Technologies	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
55	Terahertz (Imaging and Substance Identification)	6	3	1	3	2
56	Carbon Nanotube Sensors	5	6	3	3	6
57	Nano Particle Sensors	5	3	3	3	6
58	Through the Wall Radar	5	3	-1	3	0
59	Explosive Traces Integrated Sensors	5	0	-1	3	6
60	Muon Tomography	5	0	-1	3	4
61	Medical Tricorder	4	6	3	3	0
62	Cantilever-based Nanosensors	4	6	3	3	6
63	Sensors on Unconventional Flexible Substrates	4	6	3	3	6
64	OTFT Sensors (Organic Thin-Film Transistors)	4	3	3	3	6
65	Hyper spectral Sensors and Signal Processing	4	0	-3	3	6
66	Femto-Photography	2	6	1	3	2
67	Electrical Impedance Tomography	1	0	-1	-1	4
	TA13: Cross Sectional Themes	**SecRel**	**Time**	**Market**	**Appl**	**Ethics**
68	Power System Security	6	6	3	3	3
69	Effective Water Resources Management	6	6	3	0	3
70	(Trust in) Online Business	4.5	1.5	3	0	0

Table 6: Complete prioritised list of Emerging Technologies with security implications in time frame years 2020 to 2030

3.2.1.2 Results of scanning and prioritisation of technologies

The entire process of scanning and prioritization identified a total number of 127 technologies, arranged in 13 technology areas.

Expert opinion on the security relevance, the expected time to market, the market potential, the application potential, and possible ethical implications of all technologies identified was collected in a Weighted-Bit Assessment Table (comparable to the WBAT-CD described in section 3.1.3.6).

Table 6 shows those technologies out of the 127 identified technologies fulfilling the following basic criteria:

- rating of value "Security Relevance" ≥ 1
- rating of value "Time Frame" ≥ 0
- rating of value "Ethical Rating" ≥ 0

Application of these criteria eliminated all Emerging Technology found in certain technology areas (TA). Those areas are listed here for comprehensiveness but have no entries.[23]

However, the list of identified and prioritised Emerging Technologies is the result of an effort limited in time and personnel budget and represents a time dependent vision on future issues. The dynamics of technology development as well as the comprehension of the term "security" or "security implications" will be subject to changes in time. The content of this list will consequently be different if this activity is repeated in the future. It is thus recommended to repeat the Emerging Technology identification process described here in regular intervals.

For further details of the process and results (e. g. alternative rankings) please refer to Deliverable 4.1 and Working Document 4.1.[24,25]

3.2.1.3 Observations concerning methodologies

The main goal of the scanning process described in this section was to identify and prioritise Emerging Technologies. As a consequence, the methods initially described were carried out in a pragmatic manner, e.g. results of bibliometrics were checked by in-house technology experts at AIT. All methodological reflections must thus take into consideration that the methods applied in this part of the ETCETERA project were not carried out under "ideal" or "laboratory" conditions.

A first, rather surprising, observation made was that of the 127 initial items, only five were identified by more than one method. The hypothesis that the three methods applied would lead to more or less overlapping results was not confirmed.

In a next step "validity" was assessed. A technological item was considered to be valid if it met both criteria of

- being (potentially) relevant for security, and
- being likely to be implemented between 2020 and 2030.

Of the 127 original items, 94 were judged to be "valid". The rate of "valid" items in comparison to all items identified was significantly higher for the methods based on expert consultations (approx. 80%) than for the bibliometrics approach (approx. 30%). Further analysis revealed that judging technology maturity seems to be harder than judging the relevance of technology for security.

Concerning "completeness" another interesting observation was made: While the expert-based methods concentrated on pure technologies (as required), bibliometrics produced results beyond the technological scope. These "cross-sectional themes", relating e.g. to food security or economic conditions, opened a broader horizon, even though no technologies for further processing within ETCETERA were identified.

A cursory analysis concerning efficiency adumbrated that the expert-based methods were significantly more efficient in detecting valid Emerging Technologies than the bibliometrics method (as "technologies identified per budget"). However, this assessment neglects the fact that prior technology scanning experience of the experts involved was not remunerated within the project.

Further details regarding the methods used for the technology scanning process and lessons learned are documented in Deliverable 4.2.[22]

3.2.1.4 Ideas for a novel method for Emerging Technology identification

Following the methodological assessment, an idea for the synthesis of a novel 3-step approach was developed:[26]

- Step 1 "Search Phase": Collection and bibliometrics analysis of scientific literature based on pre-defined search terms
  - Delivery of a widespread and unbiased overview of a topic (backcast)

23 The technology areas concernd are TA1, TA3 and TA6.

24 Beatrix Wepner (AIT), Guido Huppertz (Fraunhofer INT), Jesús López Pino (Isdefe), "List of emerging technologies with security implications", ETCETERA Deliverable 4.1, July 2012

25 Beatrix Wepner (AIT), Guido Huppertz (Fraunhofer INT), Jesús López Pino (Isdefe), "Report on the scanning for emerging technologies with three different methods, including a provisional list of emerging technologies for security purposes", ETCETERA Working Document 4.1, undated

26 Beatrix Wepner (AIT), Guido Huppertz (Fraunhofer INT), "Ideas for a novel method for emerging technology identification", ETCETERA Deliverable 4.3, November 2013

- Identification of emerging "hot spots" and visualisation of their interconnectedness

- Step 2 "Analysis Phase": Assessment of materials by technology foresight specialists in their respective domains (desk research)
  - Identification of relevant developments in a technology field
  - Analysis of application potential, complementary, and concurrent developments
  - Assessment of future developments (forecast)
  - Formulation of recommendations for specific stakeholders
- Step 3 "Validation Phase": Bibliometry, based on refined search terms, and WBAM supported verification of results
  - Bibliometry:
    - Verification of completeness regarding publications, research groups and institutions
    - Verification of the temporal assessment of the experts (retrospective validation)
    - Visualisation of scientific cooperation and temporal dynamics
  - WBAM:
    - Verification of expert assessment of future developments through consultation of additional experts (forecast validation)

In practice, this 3-step approach will probably be carried out in several internal cycles, especially concerning steps 1 and 2, as expert assessment will contribute to the refinement of bibliometric search terms. The refined bibliometrics might in turn provide new ideas for expert analysis.

3.2.1.5 Results of the parallel workshops concerning Emerging Technologies

As described in Section 3.1.2.2, five "parallel" workshops were conducted in order to broaden the scope of the initial research. These workshops were held in five European countries (Spain, Germany, Italy, Sweden, and France) in the five corresponding national languages, all applying the World Café method. This method is based on informal discussion in small groups (four to six participants). The composition of the groups was altered several times during the workshop. To further encourage discussion, the workshops included visits to locations with a special connection to security, e.g. a large football stadium, an emergency response centre, and the building site of an underground train system.

While the first question dealt with aimed at identifying Critical Technologies, the second was more focused on solution space and futuristic technologies. In the following future technologies (ranging from broad themes to specific technologies) "invented" at the workshops are listed:

- Broad Areas
  - Develop and implement methods for organisational capacity
  - Self-critical development, cultural understanding and behavioural patterns
  - Alternative and distributed (localised) energy (electricity) production
  - Novel (data) communication and information handling systems
  - Advanced sensors, both medical and electromagnetic
  - Enhance working conditions
  - Improve living conditions
  - Decrease of false alarm rate by analysis and coupling of sensors with identification of the person and of the potential threat
- Existing technologies that could be applicable after further development
  - Robots für remote detection CBRN hazards
  - Mobile mass spectrometers
  - Comfortable chemical protective clothing including respiratory protection
  - Visual aids integrated into helmets (e.g. infrared cameras)
  - More ergonomically designed devices and prodedures
- Futuristic technologies
  - A „disease scanner" (for rapid medical diagnosis)
  - A (vehicles mounted) siren that is directed at only those that need to be alarmed
  - Biological remote detection with low false alarm rates
  - Indicator strips for air and water (that show green if everything is okay and red if there is a chemical or biological hazard)
  - „X-ray cameras" to look through walls
  - Reliable simulation tool for power failures (including cascading effects)

The Emerging Technologies named by workshop participants are clearly oriented towards human needs and human protection. Societal aspects played a large role in the discussions. An adequate compromise between security and liberty of the citizen

was discussed intensively, in particular in respect to surveillance, detection of anomalous behaviour and tracking of people. Issues raised were:

- Security control has to be discrete and non-invasive (e.g. contactless sensor) and limited to the control of pre-identified "dangerous" people.
- Both societal and environmental responsibility should be shown.
- Ethics has to be "built in" to all security products.

3.2.2 In-depth analysis of Emerging Technologies

3.2.2.1 Technologies selected for further analysis

Taking into account the prioritisation presented in Table 6 and the technical proficiency of project partners, eight Emerging Technologies and one technology area were selected for in-depth studies:[27,28]

- Indoor navigation (CEA)
- Smart textiles (FOI)
- Small-scale energy harvesting (FOI)
- Homomorphic encryption (Fraunhofer INT)
- Explosive traces integrated sensors (Isdefe)
- Sensors on unconventional flexible substrates (Tecnalia)
- Cognitive radio (Tecnalia)
- Terahertz (imaging and substance identification; Morpho)
- Technology Area: CBRN-Identification (Morpho)

3.2.2.2 Selected results of the in-depth analyses

The in-depth analyses confirmed that the selection process had been successful: All nine items studied were found to be highly relevant for future security applications. The timeframe of 2020 to 2030 was also largely confirmed for the areas studied, although it was found that most items represented various technologies, some of which are already on the market (e.g. solar cells for energy harvesting), while others might never become commercially available (e.g. full homomorphic encryption).

Improved **indoor navigation** was found to be highly relevant for search and rescue operations in areas were no satellite navigation is available. Furthermore, it is essential for the operation of unmanned systems in shielded areas. Numerous technologies are currently considered for indoor navigation, e.g. micro electromechanical systems (MEMS; incl. inertial sensors), visual odometry, and radio wave-based methods. Although many technologies are already available, adaption to specific security scenarios (troubled with e.g. smoke, heat or water) requires further development. There are only few ethical concerns related to this technology, which mainly deal with privacy issues.

Smart textiles are a large group of technologies concerning fabrics with enhanced functions. These include body sensors that measure heart function, pulse, breathing frequency, sweat or dehydration. Furthermore, fabrics could incorporate conductive materials that either serve as antennas or distribute

27 Steven Savage, Anna Pohl, Britta Levin, Malek Khan (FOI), Dominique Noguet, Géraud Canet (CEA), Javier Herrera Lotero (Tecnalia), Jesús López Pino (Isdefe), Stéphane Revelin (Morpho), Matteo Bonfanti (CSSC), Klaus Ruhlig, Guido Huppertz (Fraunhofer INT), "Intermediate Report on Emerging Technologies", ETCETERA Deliverable 5.1, November 2013

28 The short names of the Consortium Parties that have conducted the individual analyses are given in brackets.

electrical power between equipment systems located at different positions of the wearers body. Smart textiles could also provide improved protection to the wearer. Smart textiles will become relevant for security operations as they might allow improved health monitoring both of emergency personnel and victims. Furthermore, they might provide lighter and more comfortable equipment. Although smart textiles could become highly relevant for security applications, it is expected that technology development will be driven by the potential of such products on the profitable sports and outdoor market. Some ethical issues have been identified concerning this group of technologies, mainly concerning the handling of sensitive health data. As smart textiles contain novel and potentially hazardous materials, they might also cause health and environmental problems.

Small-scale energy harvesting is another large group of technologies. These technologies are directed at concentrating energy freely available in the environment (e.g. temperature differences, light, or movement) and converting it to electricity. They can enhance the durability of small distributed systems, e.g. sensors. These technologies might thus be relevant for all security functions connected to surveillance. The technologies will profit from the development of more power efficient electronics and improved secondary batteries. The only ethical concerns are linked to improved possibilities of covert surveillance.

Homomorphic encryption allows computations to be carried out on encrypted data which is not possible using conventional encryption methods. This ensures confidentiality even while data is processed. While encryption schemes that allow some computations are already known, it is not even theoretically clear yet if full homomorphic encryption that allows all kinds of computation is actually possible. Homomorphic encryption is most relevant in the context of cloud computing where it will improve data confidentiality. Although homomorphic encryption is a privacy enhancing technology, it might also offer possibilities to conceal criminal activities.

Explosive traces integrated sensors will improve all security functions aimed at finding and identifying explosives. It is not a new technology in itself but the purposeful combination and integration of existing complementary technologies. The goal is to increase reliability and to lower false alarm rates. While there are little ethical concerns attached to such systems, it seems to be highly important to inform the public comprehensively in order to foster trust and acceptance.

Sensors on unconventional substrates are usually cheap and small and might provide additional information on hazards or health parameters. They might improve all kinds of security functions associated with surveillance and monitoring. Sensors on unconventional substrates are closely related both to smart textiles and small-scale energy harvesting and have a similar ethical rating.

A **cognitive radio** is a system that makes better use of an available frequency spectrum by actively responding to its electromagnetic environment. This may improve communication performance, e.g. by allowing different systems to share a single frequency band, mitigating interferences, and improving network flexibility. This would be especially useful in emergency response situations. Although some useful technologies for cognitive radios are already commercially available, further technology development is still necessary. The successful commercialisation of such systems is highly dependent on legislation. There are few ethical concerns related to this technology.

Some applications of **terahertz technologies** are already commercially available. Nevertheless, this technology promises many further uses for a number of detection and identification applications which are of special interest to transportation security operators. Ethical assessment revealed several privacy issues. Furthermore, long-term health issues require further attention.

With **CBRN identification** a whole technology area has been studied. It encompasses several novel and promising technologies, e.g. Raman spectroscopy, advanced mass spectroscopy, differential mobility spectroscopy, and photofission. Depending on the specific technology, relevant applications might emerge in the short to medium term. Special attention must be paid to technologies that could cause privacy or health issues.

It is worth noting that these findings do not preclude that the other technologies highly prioritised in Work

Package 4 (see section 3.2.1) are less relevant for European security than the ones studied in depth within Work Package 5.

3.2.2.3 Security Emerging Technology Assessment Game (SETAG)

In order to verify the results obtained through desktop research in the first year of the ETCETERA project, two participatory methods with internal and external stakeholders were employed in the 2nd Consultation Campaign: A "serious game", described in this section, and a scenario process, which is discussed in sections 3.2.2.5 and 3.2.2.6.

The Security Emerging Technology Assessment Game (SETAG) is based on the Disruptive Technology Assessment Game (DTAG), which was originally developed to evaluate innovative technologies and systems for defence purposes. The goal of the original game was to identify those technologies that can be "disruptive" to military operations. These technologies could rapidly change the way military operations are conducted and thus influence long-term goals and strategies. The DTAG was developed by task group SAS-062 within the NATO Research and Technology Organization (RTO) framework.

For the ETCETERA project, the military DTAG was modified to assess the relevance of Emerging Technologies for security purposes. In contrast to the DTAG methodology, the ETCETERA game does not focus on the disruptiveness of technologies, but on possibilities future technologies could provide. The name was therefore changed to Security Emerging Technology Assessment Game (SETAG).

The SETAG concept revolves around cards representing future equipment (derived from Emerging Technologies identified in Work Package 4)

Figure 5: Game board of the Security Emerging Technology Assessment Game (SETAG)

and scenarios to which these cards can be applied, pictured on a game board. The game is played by two teams of end-users. Each team has a hand of cards with descriptions of innovative technological concepts described as futuristic systems, called ‚Idea of Systems' (IoS, or in the game as IoS-cards). The game board has fields that represent operational situations (Figure 5). As the teams act on the game board, they move from situation to situation, answering a set of predefined questions related to the use of IoS-cards in the situations encountered. The goal for each team is to optimally apply the available IoS-cards to the situations.[29]

It is up to the teams to:

- determine what operational challenges a situation poses to the response organisations
- describe how the IoS-cards can provide a solution to these operational challenges
- share their ideas with the other team and discuss alternative solutions

Two SETAG workshops were held:

1. In the Netherlands with solely Dutch participants
2. In Spain with solely Spanish participants

3.2.2.4 Results of the SETAG concerning Emerging Technologies

With respect to evaluation of Emerging Technologies, three types of results were gathered from the workshops:

1. Usage frequency of IoS-cards for predefined scenarios
2. Additional scenarios which participants found useful for the given IoS-cards
3. Ranking of IoS-cards based on votes casts for the IoS-cards

At the later stage, based on the voting done by the participants, a distinction seems to arise between a top-3 and the other IoS-cards. When considering the actual use of IoS-cards, albeit in predefined scenarios, there was no similar pattern in the results. Based on the three IoS-cards that got cast most votes, it seems as though the end users had a relatively clear preference for certain issues. Frequently voted solutions improve operational communications and physical safety of responders, or might allow for better intelligence gathering:[30]

When looking at the actual use of IoS-cards, a slightly different rating can be observed:[30]

IoS-cards		Number of votes		
		SETAG-NL	SETAG-ES	Total
5.	Micro radio	4	4	8
11.	Uniforms based on smart textiles	3	5	8
8.	Cloud parallel computing	5	2	7

Table 7: Result of the IoS-cards voting

It should be noted that there was large difference between the Dutch and the Spanish workshop

IoS-cards		Number of scenarios		
		SETAG-NL	SETAG-ES	Total
8.	Cloud parallel computing	4	7	11
5.	Micro radio	3	6	9
2.	Through the wall radar	1	7	8

Table 8: Results of the IoS-card application

concerning the number of IoS-cards used per scenario. Possible explanations for the difference in the number of IoS-cards used per scenario are the different number of participants, the difference in type of participants or changes in the task forms. It thus seems to be adequate to further regulate the use of IoS-cards in future SETAG workshops, in order to allow definitive conclusions based on the actual behaviour during the game, which was not the case for this SETAG.

However, if the findings of the two SETAG workshops are re-aligned with the underlying Emerging Technologies, the following technologies have obtained

29 Sam Besselink, Marcel-Paul Hasberg, Clara Peters, Peter Petiet (TNO), Jesús López Pino, Patricia López Vicente (Isdefe), "Report on the adapted DTA game", ETCETERA Working Document 6.1, May 2013

30 SETAG-NL gives the number for the game conducted in the Netherlands, while SETAG-ES stands for the workshop in Spain.

most attention by workshop participants:[31] Cognitive Radio (IoS-Card "Micro radio")

- Homomorphic Encryption (IoS-Cards "Cloud parallel computing for analysis on large criminal voice databases" and "Cloud password-crack service")
- Smart Textiles (IoS Cards "Uniforms based on smart textiles" and "Self-healing passive protection systems")
- Terahertz Imaging and Substance Identification (IoS-Card "Through the wall radar")
- Explosive Traces Integrated Sensor (IoS-Card "System for tracking explosives traces to their source")

3.2.2.5 Scenarios for the assessment of Emerging Technologies

In addition to the SETAG, a scenario process was conducted for the assessment of the previously selected Emerging Technologies to identify social, political, economic, and environmental factors and to analyse their possible influences on the development of selected technologies.

The scenario technique is a well-known tool to create alternative future scenarios based on quantitative and qualitative data and provides a systematic process. Traditionally scenarios are built for two reasons: exploration and decision support. Scenarios explore the future and identify several future perspectives, thus providing a context in which actors can make decisions. This kind of future scenarios is based on a networked / cross-linked system of influencing factors, with several possible opportunities of development into the future being considered for each factor.[32]

The aim of the scenario process performed was to determine key factors that would foster or hinder the development of selected Emerging Technologies with security implications. The process was composed of four steps:

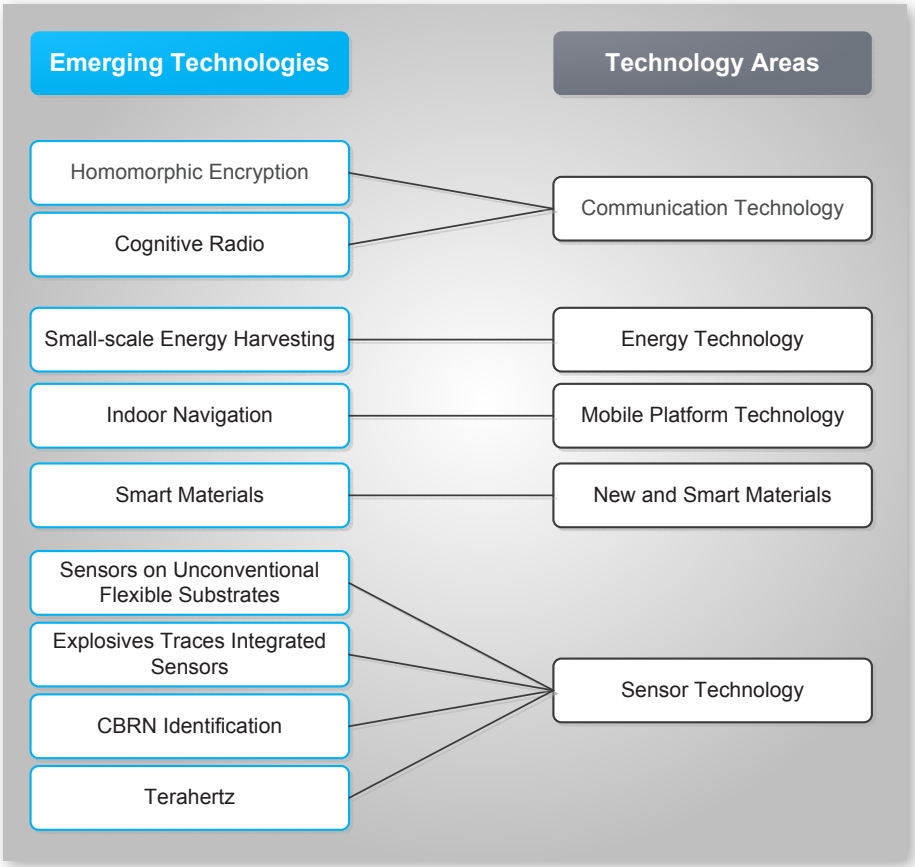


Figure 6: Prioritised selected Emerging Technologies and their technology areas

1. Analysis of social, political, economic and environmental factors that influence the selected technologies (desk research)
2. Selection of key factors and development of future projections (first workshop)
3. Development of the raw scenarios (desk research)
4. Identification of drivers and barriers for specific technologies (second workshop)

Concerning the selection of technologies to assess, the Scenario Workshop team at Fraunhofer ISI followed the selection process performed during the transition between Work Package 4 "Scanning for Emerging Technologies with Security Implications" and Work Package 5 "In-depth Analysis". For details of the selection process of Emerging Technologies with security implications please

31 Joachim Burbiel, Ruth Schietke (Fraunhofer INT), "Report on the Evaluation of the 2nd Consultation Campaign", ETCETERA Working Document 3.2, November 2013

32 Antje Bierwisch, Victoria Kayser, Erduana Shala (Fraunhofer ISI), "Report on the scenario based workshop", ETCETERA Working Document 6.2, August 2013

Factor no.	Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
1	**EU security policy and legal framework**	1A | Human orientation of overarching EU-Security-Policy	1B | National orientation of EU-Security-Policy	1C | Defence-orientated EU-Security-Policy	
2	**General development of EU**	2A | Strong development of Europe and further integration	2B | EU of different nations and different integration levels	2C | Decreasing importance of the EU	2D | European political union with new constitution
3	**EU R&D infrastructure**	3A | Public funding scheme	3B | Shift to private R&D funding	3C | Shift to private funding and research	
4	**Commercialisation strategy of R&D**	4A | EU-Security label & far reaching information providing	4B | No security label, but marketing label &limited public information	4C | No security label & few/less public information	
5	**Design and orientation of R&D**	5A | Resilience-driven R&D	5B | Threat-driven R&D		
6	**Capabilities and capacities in R&D**	6A | European human resources are sufficient	6B | Lack if EU-talents & recruitment outside Europe	6C | Lack of EU-talents & international recruitment failed	
7	**Design and implementation of security technologies**	7A | Orientation on user-needs and convergence	7B | Competition-driven and User-independent		
8	**Security understanding and concerns in society**	8A | High risk awareness	8B | High need for more security		
9	**Cultural influences and social change**	9A | Changing value system and focus in material interests	9B | High meaning of social value system		
10	**Attitude towards technologies in society**	10A | Technology-hype & no scrutinizing of research	10B | Decreasing technology acceptance & scrutinizing	10C | Acceptance depends on user-friendliness & scrutinizing	
11	**Global economic arrangement**	11A | long-term stability & quantitative growth	11B | Instable economic situation, emerging new economies	11C | Long-term financial crisis and global instability	11D | Lon-term stability & qualitative growth
12	**Production and consumption behaviour**	12A | Inefficient and un-sustainable	12B | Efficient and sustainable		
13	**Security industry**	13A | Global leadership of EU by knowledge-based security industry	13B | Big players, focus on market-driven interests	13C | Strong security industry by fragmented market	
14	**Relevance of security in different sectors**	14A | Security economy – fully secure	14B | Security economy – risk acceptance		
15	**Role of intellectual Property Rights (IPR)**	15A | Open knowledge in EU	15B | Agreed upon EU patent	15C | National frameworks & strategic use of patents	
16	**Global shifting powers and balances**	16A | Competing political systems	16B | Few leading countries	16C | Regionalism & de-globalisation	16D | Towards more resilience
17	**Global emergencies and disasters**	17A | Interest-driven interventions	17B | Underinvestment of infrastructure	17C | Overwhelming international system	

Table 9: Overview of the future projections for 17 key factors

refer to Deliverable 4.1[24], Deliverable 4.2[22], Working Document 4.1[25] and Deliverable 5.1.[27]

Six technology areas were considered in the scenario process (depicted on the right in Figure 6). For practical reasons, four technologies within the technology area "Sensor Technology" were treated as one item at the workshops, leading to a total number of six technology items examined:

- Homomorphic Encryption
- Cognitive Radio
- Small-scale Energy Harvesting
- Indoor Navigation
- Smart Materials
- Sensors Technology

Analysis of social, political, economic and environmental factors
As a first step towards the identification of "key factors", areas of influence were specified. For the ETCETERA project, the field of the scenario was divided into six areas of influence:

1. EU-(Security)-Policy
2. R&D and Innovation Characteristics
3. Trends and Drivers in Technology
4. Society
5. Economy
6. Global Stability and Policy

More than 100 studies and reports were analysed to answer the following research questions:

- What are the key factors characterizing and influencing the field of security today and in the future?
- What are the present developments of the key factors?
- What kinds of future projections describe the possible developments of the key factors?

This analysis resulted in more than 40 factors. These factors of influence were the basis for the discussion with experts in the first workshop.

First scenario workshop
During the first workshop, conducted on 11 and 12 December 2012 in Frankfurt a. M. (Germany), the long list of factors was reduced, selecting those factors which have a high impact on issues dealt with in the ETCETERA project. 17 key factors were selected and "future projections" were developed for these factors. A total of 49 future projections were created for the 17 key factors (Table 9).

Development of raw scenarios and second workshop
In order to generate plausible scenarios, an analysis of how well future projections of different key factors fit with each other was performed. As a result of this "consistency analysis" a total of four scenarios were selected for further assessment:

- The green scenario: "2nd Woodstock – a peaceful world of harmony, unison and qualitative progress"
- The orange scenario: "High-tech rules the world"
- The pink scenario: "Buddenbrooks global – instability, social gaps and inequalities"
- The yellow scenario: "The broken pitcher – broken relationships, no harmony, stagnation, retrograde step in social terms"

At a later point in time, short storylines were developed to illustrate the characteristics of the individual scenarios.

During the second scenario workshop, conducted on 13 and 14 February 2013 in Langen (Germany), Drivers and Barriers for the selected Emerging Technologies were identified.

In order to achieve a holistic assessment of these future technologies, they were discussed concerning their technical feasibility, user demands and social aspects, political and framework conditions, industrial systems and infrastructures, the education and research system, and the interrelated dynamics of these elements (Table 10).

		Green scenario	Orange scenario	Pink scenario	Yellow scenario
		2nd Woodstock – a peaceful world	Technology rules the world	Buddenbrooks global	The broken pitcher
Scenario characteristics	Global or in general	• long-term economic stability • absence of great power conflicts in the world • sustainable, efficient consumption and production behaviour • usefulness determines supply & demand for security technologies/ measures • focus on technologies contributing to needs of everyday life	• competing political systems at global level • worldwide economy is stable • greater demand and competition for essential resources • balance of military powers shifts to various regions • could lead to tensions between regions, states and national identities	• instable economic situation • many crises and competition for resources • new global players evolve and assert market interests	• economic and political instability • regionalism, de-globalization process, global powers and balances shift to few regions • conflicts over markets, investment flows and resources • long-term financial crisis • only a few leading countries worldwide benefit from technologies
	European Union	• competitive at global level • strong industrial capability and knowledge base in security field • worldwide leading position in science and research incl. Civil security	• competitive worldwide leading position in science /industry • harmonization far driven – enlagement of European Union/monetary union • 'western' value system remains important • security policy – human security, focus on securitization of life, pushed forward by fragmented, yet strong security economy and industry • civil security technologies widely used	• decreasing political influence • divided into different regions and different integration levels at policy side • the eurozone is minimized • security policy – strong focus on national security, limited interactions with other policies • need for security enforced by the security industry • less regulation/harmonization allows development of industries and is accompanied by more innovation inputs	• reduced power in the worldwide context • stagnating enlargement of European Union • effords for harmonization of legal framework stopped • return to interest of nations and regions - decision making process at EU level stagnates • security policy –emphasis on defence than on trust and cooperation; lobbies have strong influence at the policy level
	R&D activities in science & industry and Security products/ services	• take into account expressed market needs and user integration at early stage • change from fully secure approach to risk management approach	• addresses more technological feasibility than usefulness and societal needs • solutions for current challenges, problems and societal needs mainly expected in technology field	• shift to private R&D funding • defined by profit, efficiency and turnover • R&D applied research, basic research missing • technology driven research • very strong security industry, tailored solutions for society and industry • oriented to market and societal needs than to best solution	• multinational companies and big players which concentrate on markets with few risks • security market dominated by US companies • more effective research required
	People and Society	• show conscious handling of uncertainty and risk • enhanced resilience of the society • traditional and social values still remain important Europe	• technology affinity in society • trust in technology solutions • awareness/ acceptance of risk originating from technologies • for higher security level – reduced claims for citizen's rights • public acceptance for high security standards • technology is solution for different kinds of challenges • new technologies are hyped • research activities not scrutinized	• affinity to technological solution • high technology penetration of everyday life • for higher security levels - citizens accept restriction of individual rights and freedom • growth of social gaps, strict differentiation between social classes • only certain groups of "rich people" can afford security technologies and products	• decreasing technology acceptance • decreasing demand for security technologies • awareness not all risks may be covered by security solutions • not all citizens can afford security measures due to financial/ economic crisis • growth of social gap, strict differentiation between social classes • stronger extreme groups, difficult to control
Selected Emerging Technologies	Homomorphic encryption	+	++	-	-
	Cognitive radio	+(+)	+	+	+
	Small-scale energy harvesting	++	+	0	-
	Indoor navigation	+(+)	++	+	0
	Smart textiles	+(+)	++	0	-
	Sensors	+	+	-	-

Table 10: Assessment of selected Emerging Technologies within different scenario contexts

3.2.2.6 Results and conclusions of the scenario process

Table 10 also summarises the results of the scenario process regarding the assessment of the selected Emerging Technologies. It displays the estimated potential of the Emerging Technologies dependent on the different developed scenario framework conditions.

The future development and application potential of the Emerging Technologies is defined as follows:

++/ +(+)	The scenario supports very well the future development and application potential of the technology.
+	The scenario supports the future development and application potential of the technology.
0	The scenario is neutral for the future development and application potential of the technology.
-	The scenario is hindering for the future development and application potential of the technology.

The scenario-based approach was able to assess the potential of application and development of the selected emerging civil security technologies. With regard to the evaluation on Emerging Technologies, the following types of results were gathered:

- Identification of barriers and drivers
- Identification of key factors in the developed scenarios which have an important influence of technology development and application
- Identification of relevant dimensions that have an influence on the application and development potential for the selected emerging technologies

The identified barriers and drivers were associated to six different dimensions: societal, legal, political, ecological, economic and technological with the societal, technological and economic dimensions being most relevant. However, ecological, political and legal aspects were rarely discussed at the second workshop.

The following key influence factors and their future developments were most significant in the discussion of future application and development potentials for the selected technologies:

- Attitude of society towards technology
- Security understanding and concerns in society
- Global economic arrangements
- Global shifting powers and balances

The global scenario approach showed starting points and hints for different activities within the research and development process of technologies:

- Approaches for innovation policy activities, e.g. research programs
- Influence of society, first-responder, end-user etc., involvement of actor needs in the development process, marketing activities, establishment of transparency
- Necessary knowledge exchange, discussion about required infrastructures and technological pre-conditions
- Consideration of ethical and legal aspects in the whole R&D and innovation process "privacy by design", "ethical by design" or/and "societal impact by design"

Furthermore, the scenario-based evaluation process gave clues for changes in the focus of the technology development process. Technological feasibility did not seem to play an important role, but elements like the attitude of society towards technologies and security understanding and concerns in society were attributed more influence potential than other elements. Therefore, a change can be recognised from a technology driven process to a more basic need or societal need driven technology development approach.

Although the data resulting from the scenario workshops is highly complex as the technologies discussed were embedded in an intricate socio-economic context, some general trends can be abstracted (Table 10):

- "Homomorphic encryption" and "sensors technology" scored well in the technology-oriented scenarios but failed in the less technology oriented scenarios.

- "Small-scale energy harvesting" and "smart textiles" scored (very) well in the technology-oriented scenarios but received little attention in the less technology-oriented scenarios.
- "Indoor navigation" scored (very) well in three scenarios and was only ignored in the yellow scenario.
- "Cognitive radio" was received well in all scenarios.

3.2.3 Development of recommendations for an Emerging Security Technology Research Agenda (ESTRA)

3.2.3.1 Process of developing recommendations

In the last Work Package of Strand 2 "Emerging Technologies", all results previously obtained were taken into account to create recommendations for the development of an Emerging Security Technology Research Agenda (ESTRA). Additionally, existing national and European research strategies were analysed in order to assure the usefulness of the recommendations made. Furthermore, a socio-economic model was developed to assess high risk/ high pay-off Emerging Technologies.[33]

3.2.3.2 Socio-economic considerations regarding Emerging Technologies

Initially it was planned to adapt and apply a mathematical economic model for the assessment of high risk/high pay-off by the Chair of Finance and Banking, University of Duisburg and Essen. It turned out that merging such a mathematical model with the data generated through previous ETCETERA Work Packages proved not feasible in the end. However, this shortcoming was compensated by work of Fraunhofer ISI, the second partner in this task, by the development of a socio-economic model based on the results of the scenario process.

For the development of this model, a multi-criteria decision analysis with several dimensions was conducted. Within the process, qualitative and

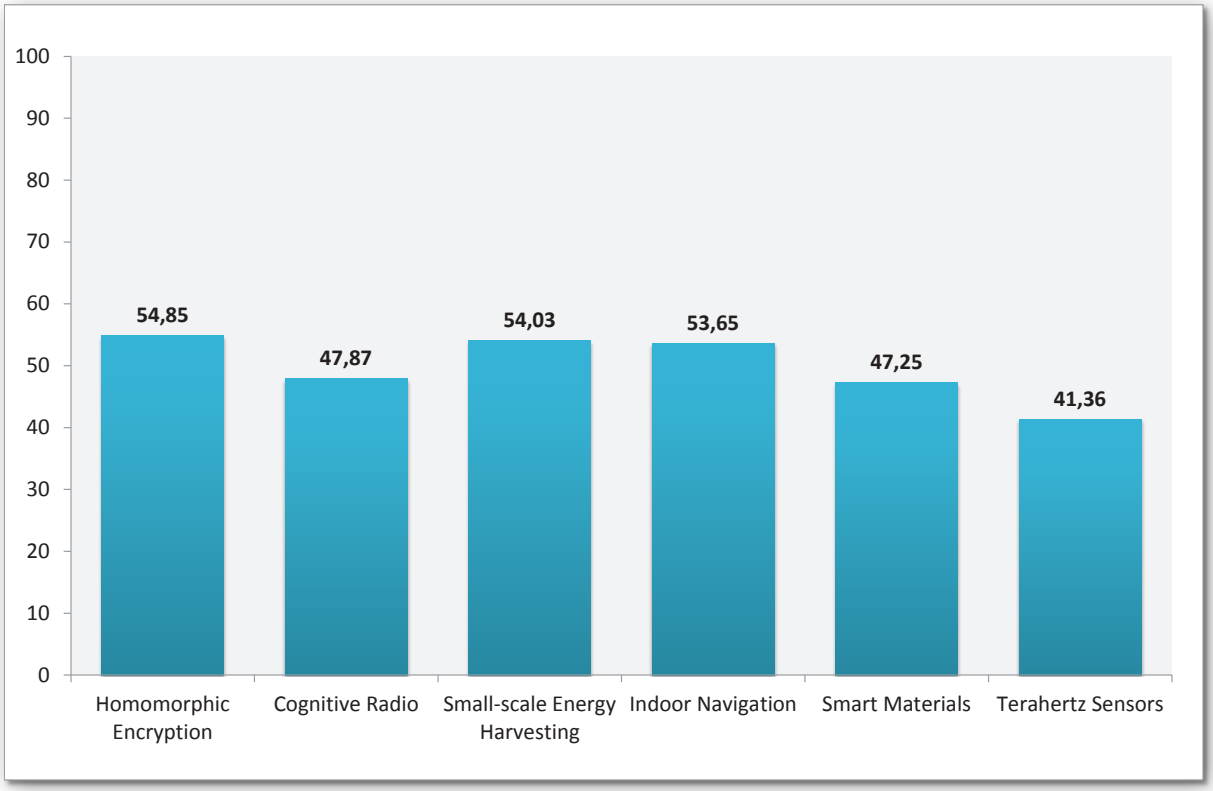


Figure 7: Scores for the selected Emerging Technologies – Ranking of global assessment

33 Joachim Burbiel, Ruth Schietke (Fraunhofer INT), "Recommendations for an Emerging Security Research Agenda (ESTRA)", ETCETERA Deliverable 6.1, November 2013

quantitative data were considered to fulfil the requirements of a holistic assessment approach by integrating expert opinion and quantitative facts.[34]

The assessment approach included qualitative information procurement as well as multi-criteria analysis taking into account specific dimensions such as technological, economic, social, ecologic and legal & political dimensions. Furthermore, the four future scenarios developed in WP 5 were used as an additional dimension, including drivers and barriers which were identified as explicitly relevant.

The combination of results derived from the qualitative and quantitative assessment of the selected Emerging Technologies led to the following ranking:

1. Homomorphic Encryption
2. Small-scale Energy Harvesting
3. Indoor Navigation
4. Cognitive Radio
5. Smart Materials
6. Terahertz Sensors

According to expert opinion and analysis of the quantitative and qualitative assessment data there are three technologies having good innovation potential. These are homomorphic encryption, small-scale energy harvesting and indoor navigation. Less innovation potential was attributed to cognitive radio, smart materials and terahertz sensors.

Remarkably, during this last expert consultation exercise, conducted as a directed online survey, the weighting of ecological, legal and political dimensions for the assessment of the technologies was surprisingly high, which was rather unexpected having in mind the experiences during the second scenario workshop.

For detailed data regarding the qualitative respectively quantitative assessment and its combination results as well as regarding the weighting of the technological, economic, social, and drivers & barriers dimensions please refer to Deliverable 6.2.[34]

3.2.3.3 Recommendations concerning methods

In the course of the ETCETERA project a number of methods were applied to identify and prioritise Critical and Emerging Technologies with security implications:
Desktop research

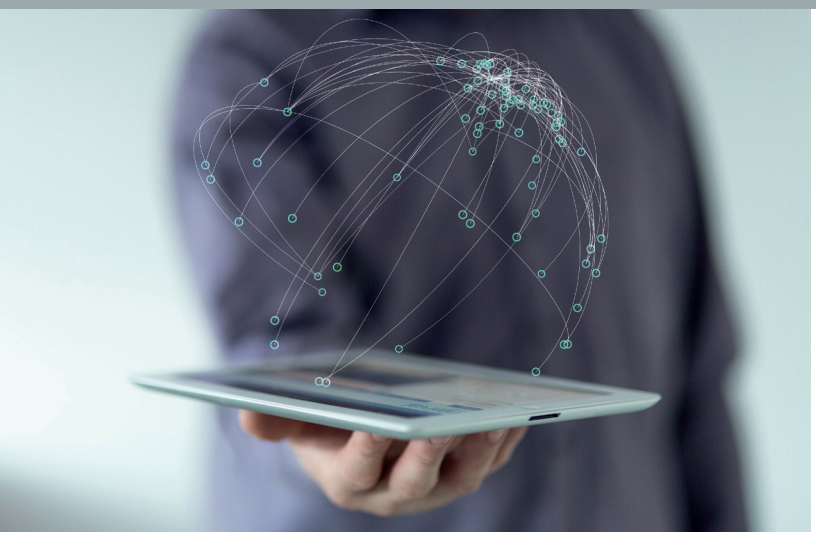
- Direct consultations with external experts
- Scientometrics (e.g. bibliometrics and patentometrics)
- Two Weighted-Bit Assessment Methods to aggregate expert opinion
- Adapted TEPID-OIL filtering methodology – ITIPOLITRE
- Parallel workshops applying the World Café method
- A dedicated Security Emerging Technology Assessment Game (SETAG)
- A complex scenario process
- Multi-criteria decision analysis with several dimensions for economic modelling
- An online survey to get additional information for the socio-economic assessment

Desktop research and in-house expert consultations proved to be a rather efficient way of getting a first picture of the opportunities related to Emerging Technologies. Nevertheless, an assessment based on the opinion of only a few experts might lead to results biased by personal preferences.

> ***Recommendation 1:***
> *Non-participative methods should be used for initial prospective studies on Emerging Technologies. Nevertheless, they need to be supplemented with participative methods to get a solid basis for political decision making.*

Direct consultations with external experts (e.g. through interviews or by asking for written input) can broaden and consolidate the results gained by in-house desktop research. They require a network of experts that can be involved as required. While setting up such a network might be time-consuming, it allows high flexibility when responding to specific requests.

34 Antje Bierwisch, Stephan Grandt, Victoria Kayser (Fraunhofer ISI), "Socio-economic Model for the Assessment of Emerging Security Technologies", ETCETERA Deliverable 6.2, October 2013



Recommendation 2:
Building a network of highly qualified external experts is demanding but may be a good extension of in-house expertise.

Scientometrics have been used at two points of the project: As a method to identify Emerging Technologies and for the assessment of Critical Dependencies. In the context of Emerging Technologies their application has led to a set of results which also identified areas that are usually not taken into consideration in the context of security research (e.g. financial security). On the other hand, these sets of results needed careful evaluation as they contained a high proportion of by-catch which was not conducive for getting to results. Assessing technology maturity proved to be very difficult with scientometrics.

Recommendation 3:
Scientometrics should be applied if large sets of results need to be generated in a "quick and dirty" approach or if a huge solutions space should be explored in a broad manner. Nevertheless, the results should be checked by experts before any conclusions are drawn.

Recommendation 4:
Scientometrics should be used to validate the completeness of expert-based technology assessment.

In the ETCETERA project **Weighted-Bit Assessment Methods** were used at two points to aggregate expert opinion: For prioritising Emerging Technologies for further analysis and for aggregating all information available about Critical Dependencies. In both cases, this relatively simple method proved to be very useful. Nevertheless, the full potential could not be exploited during this project for organisational reasons.

Recommendation 5:
Weighted-Bit Assessment Methods should be used if information of different kinds and sources have to be evaluated. Great care has to be devoted to the design of the "questions".

Recommendation 6:
Weighted-Bit Assessment Methods should be further explored as to their potential as tools to enable interdisciplinary discussion.

The TEPID-OIL method was originally developed for analysis of military alternatives. In order for the method to be applicable to the broader requirements of civilian alternatives the method was modified and extended to include incitement/psychology and economy/markets, hence becoming **ITIPOLITRE**. The applicability of the improved method was demonstrated using alternatives to x-ray technologies applied in airport security as the starting point. ITIPOLITRE was found to work satisfactorily.

Recommendation 7:
ITIPOLITRE should be explored further as a method to prospect for technological and non-technological solutions for security problems.

The goal of conducting **"parallel workshops"** in different languages at different places was to involve

stakeholders that are not willing to travel across Europe to attend a workshop in English. This goal was met, even in the limited sphere of the ETCETERA project: A total of 72 stakeholders took part in the workshops, many of whom had not been involved in European security research before. End-users, representatives of industry, and scientists were equally represented. On the other hand, the effort of organising five "parallel workshops" was significantly higher than for organising just one "central workshop", even though the methodology was only prepared once.

Recommendation 8:
Organising "parallel workshops" at different locations and in different languages is worth the additional effort if grassroots input from European stakeholders is sought.

Applying the **World Café method** at the workshops was very convenient. Three main advantages of this method were identified:

- All participants have a chance to share their views and ideas, which is sometimes difficult in large "conventional" workshops.
- The World Café method is easily scalable: In the ETCETERA project it was applied to groups of 15 to 20 persons, but it can also be carried out with much larger groups.
- The participant response was very positive: Many stakeholders expressed that they had enjoyed the workshops and would be willing to participate in such an exercise again.

The World Café method is especially useful to generate ideas and to get to a common picture. Consequently, it was not straightforward to integrate the results of the parallel workshops to the pre-determined workflow of the two strands of the ETCETERA project.

Recommendation 9:
The World Café method is well suited for stakeholder consultation as it provides exceptional scalability. It is especially useful to generate ideas and to get to a common picture, but should be used with care if concrete answers to specific questions are needed.

The **Security Emerging Technology Assessment Game (SETAG)** proved to be a valuable tool for technology assessment. It was considered interesting by the end-users involved. It was possible to feed some results back into the main work stream of the project, but some valuable observations could not be sufficiently integrated in consecutive work. Nevertheless, the preparation of the game, especially the creation of the Idea-of-System cards, implied great effort and solid foundations for further development were laid.

Recommendation 10:
The Security Emerging Technology Assessment Game (SETAG) developed in the ETCETERA project should be used as a basis for future "serious gaming" in the context of European security research planning.

The complex **scenario process** conducted within the ETCETERA project led to a very broad set of results, not only including drivers and barriers of technologies, but also a multitude of societal perspectives: Emerging Technologies were discussed not only concerning their technical feasibility, but also taking into consideration user demands and social aspects, political and framework conditions, industrial systems and infrastructures, the education and research system, and the interrelated dynamics of these elements. On the one hand, this served as a source of information for the development of a socio-economic model; on the other hand it was difficult to reduce the plethora of results back to plain information about technologies. It should be mentioned that carrying out the scenario process was the most expensive form of external consultation used in the ETCETERA project as the process of preparing, conducting, and evaluating the workshops was very labour-intensive.

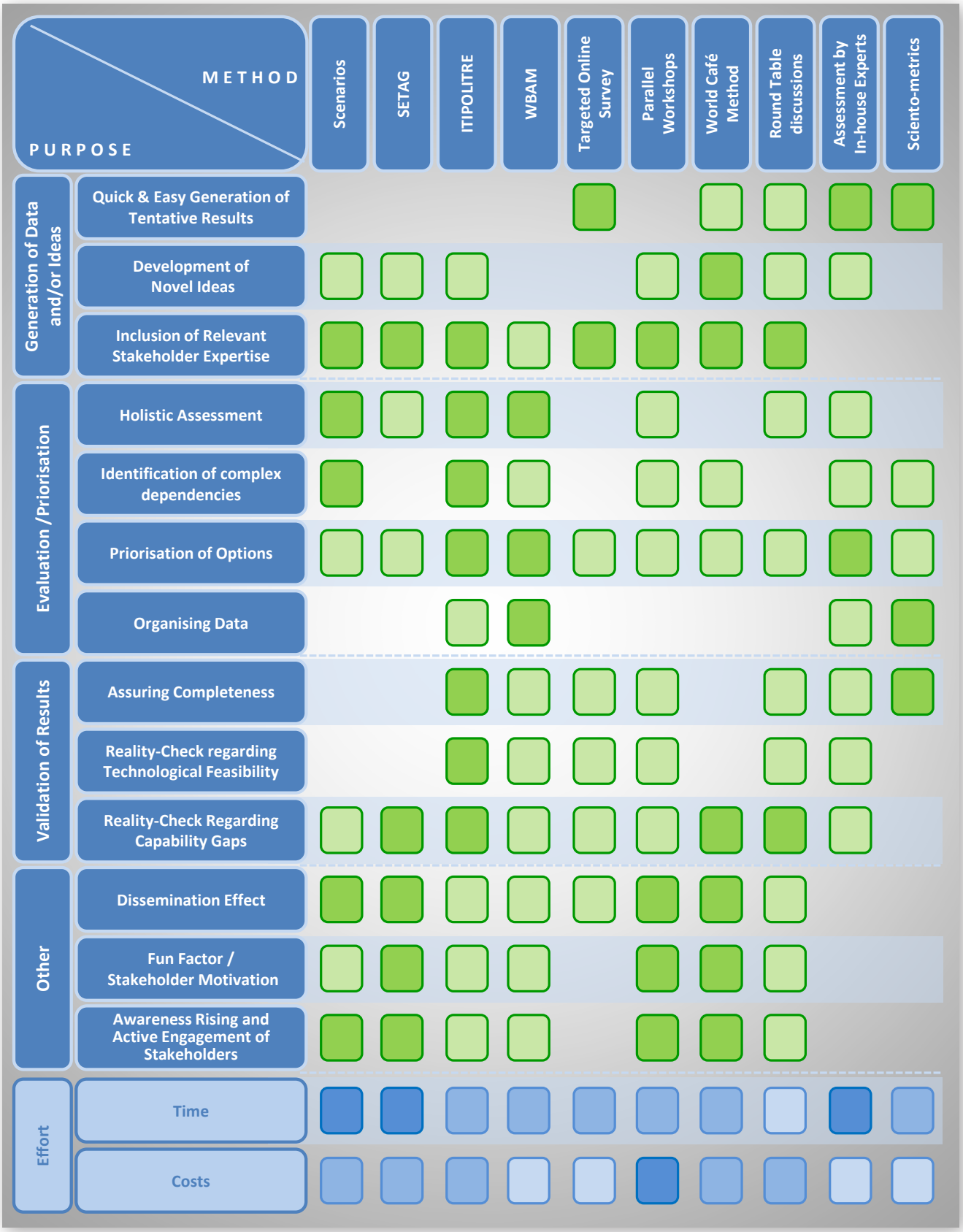


Figure 8: Alignment of methods and purposes. Dark green fields indicate that a method is well suited for a purpose, light green fields indicate that a method is partially suited for a purpose.
Time and cost are assessed as low (light blue), medium (blue), and high (dark blue).

Recommendation 11:
Scenario processes should be used for the assessment of broad conditions of technology development. The complexity of the process should be carefully balanced with the size of the consultation exercise.

Recommendation 12:
A scenario process should be conducted if broad stakeholder involvement is sought and transparency is a key requirement.

Recommendation 13:
A scenario workshop is especially suitable for assessing one specific technology or technology area, as dealing with diverse technologies might overstrain participants.

Online surveys were only used at selected points of the ETCETERA project, as they have the inherent risk of receiving insufficient valid responses. On the other hand, sufficient information was gathered when persons already interested in the project were invited to share their views.

Recommendation 14:
Open online surveys should be used if information on simple matters shall be collected.

Recommendation 15:
If complex information is to be collected through online surveys, invitations to participate need to be very targeted.

It is obvious that the choice of methods used depends on the purposes to be achieved. Figure 8 gives an overview of how well the methods applied within the ETCETERA project align with different goals in research planning. Four groups of purposes have been evaluated:

Generation of data and/or ideas:
- Quick and easy generation of tentative results without much preparative efforts
- Development of novel ideas, e.g. through stimulation of creativity
- Inclusion of relevant stakeholder expertise, always dependent on the size of the effort

Evaluation / priorisation:
- Holistic assessment by looking at one item from a multitude of perspectives
- Identification of complex dependencies
- Priorisation of options
- Organising (complex) data and presenting it in an easily understandable format

Validation of results:
- Assuring completeness: Has anything been overlooked or neglected?
- Reality-check regarding technological feasibility: Is the solution possible from a technical perspective?
- Reality-check regarding capability gaps: Is the solution useful for real-life situations?

Other:
- Dissemination effect: Will anybody take notice of the activity?
- Fun factor / stakeholder (re-)motivation: Will stakeholders participate (again)?
- Awareness raising and active engagement of stakeholders: "Winning hearts and minds"

3.2.3.4 Recommendations concerning Emerging Technologies

While the process within Strand 2 "Emerging Technologies" delivered a wealth of information concerning methodologies for research planning, the results concerning concrete technologies seemed to be somewhat arbitrary.

On the one hand, a large set of results was obtained from the process of Emerging Technology identification. This process was not restrained concerning technological boundaries and gave a list of 127 Emerging Technologies with possible security implications in the future. Efforts to prioritise this list were made, leading to several prioritised lists, depending on the weight attributed to different priorisation factors. Nevertheless, these evaluations were made by a handful of technical experts only and might thus be biased by personal preferences.

On the other hand, several assessments involving a larger number of stakeholders were made. One of these assessments, the Parallel Workshops, were not constrained concerning technologies, but the results seem to be somewhat erratic, which might be connected with the relatively small total number of results. The two other participatory methods applied in the ETCETERA project, the SETAG and the scenario method, were strongly constrained from a technological point of view: For the SETAG 16 technologies were selected from the list of 127 Emerging Technologies with possible security implications and recombined to 14 Idea-of-System cards. For the scenario process the aggregation and selection was even more constricting: Only nine Emerging Technologies were analysed, of which four belong to the sensors technology area. In these cases broad stakeholder involvement was traded off with technological limitations.

Bearing these reservations in mind, some prioritisation can be deduced from the SETAG and the scenario process (Figure 9). The technologies that have obtained most attention by workshop participants at the SETAG were: Cognitive Radio, Homomorphic Encryption, Smart Textiles, Terahertz Imaging and Substance Identification, and Explosive Traces Integrated Sensor.

From the results of the second scenario workshop, the following priorisation can be derived:

- **High:** Cognitive radio & Indoor navigation
- **Medium:** Small-scale energy harvesting & Smart textiles
- **Unclear:** Homomorphic encryption & Sensors technology

For the same set of technologies the combination of results derived from the qualitative and quantitative assessment of the selected Emerging Technologies led to the following ranking (Figure 7):

1. Homomorphic Encryption
2. Small-scale Energy Harvesting
3. Indoor Navigation

Emerging Technologies for in-depth analysis	Technology Area	SETAG	scenarios	socio-economics
Indoor navigation	Mobile Platform Technology		HIGH	HIGH
Smart textiles	New and Smart Materials	HIGH - MEDIUM	MEDIUM	MEDIUM
Small-scale energy harvesting	Energy Technology		MEDIUM	HIGH
Homomorphic encryption	Communication Technology	HIGH	unclear	HIGH
Cognitive radio		HIGH	HIGH	MEDIUM
Explosive traces integrated sensors	Sensor Technology	HIGH		
Sensors on unconventional flexible substrates		MEDIUM - LOW	unclear	
Terahertz		HIGH		LOW
CBRN-Identification		MEDIUM - LOW		

Figure 9: Overview of the prioritisation of selected Emerging Technologies

Non-technological Areas:	
Development Area	**Needs**
Some of the solutions concern the need for sharing information in order to facilitate development in the area - Forum for dialogue	• jamming/anti-jamming field • explosives detection field
Some of the solutions concern raising risk awareness and the need to disseminate information about risks in modern technological systems	• industrial control-and information systems • wireless communications amongst the general public • general awareness of jamming/anti-jamming among users of wireless communications • threat awareness related to biological agents in higher management levels of first responders
Some of the solutions concern the need for further studies	• biological risk area: identification of exposure and transmission patterns to B-threats • vulnerabilities of modern electronic devices and systems regarding jamming, in context of critical infrastructures or in general applications
Technological Areas:	
Development Area	**Needs**
Some solutions concern measures mainly related to detection/monitoring	• radiation detection: new detection materials for neutron detection to overcome possible future shortage of ^{3}He; new technologies and methods with improved capacity for identification of specific substances/mixtures of substances • explosives detection: wide areas scanning/long distance detection devices; mobile devices for detection at close range; improvement of specificity, sensitivity and accuracy of small mobile standard technologies
Some solutions concern technological development mainly aiming towards robust operational tools	• protection against jamming: improved power (battery capacity) for portable protective jamming devices; system for locating/tracking the source of a jamming signal • real-time simulation decision support: a range of simulation-based decision support tools that help different decision makers according to their specific needs and conditions • detection of biological agents: rapid detection devices with multi-substance analyses in one device; simple B and/or C/R collectors as a permanent but removable addition to first responder's uniforms; detector/monitoring devices for long term exposure to hazardous substances, attachable to first responder's uniforms • surveillance technology: systems with automatic detection of security threatening behaviour while simultaneously protecting integrity of the monitored citizens (including image processing, algorithms automatically alarming anomalous behaviour) • smart textiles: coating materials for e. g. shielding, easier decontamination; heat regulating material; monitoring health status; monitoring hazardous substances
Some of the solutions concern the need of common standards and/or rules and legislation	• common EU standards to enhance security in industrial control and information systems, especially in critical infrastructure • joint anti jamming policy for EU member states to be applied in international standards committees • investigation of advantages of common EU or international standards aiming to increase the market driven development of explosive detector instruments • some kind of standardised security analysis to more clearly present security risks for decision makers

Table 11: Recommended fields of activity to reduce selected Critical Dependencies

4. Cognitive Radio
5. Smart Materials
6. Terahertz Sensors

Nevertheless, while these results concerning technologies might be useful building blocks for security research planning, deriving a research agenda from them seemed to be too speculative, as only a small portion of the Emerging Technologies originally identified could be analysed more in depth within the ETCETERA project.

3.2.3.5 Recommendations concerning the reduction of Critical Dependencies

The ETCETERA project also aimed at proposing ways to achieve more European technological independence. In association with the search for alternative solutions for Critical Technologies with Critical Dependencies, additional areas were identified that could foster the development of alternative solutions and thereby reduce Critical Dependencies.

These development areas could provide relevant input when identifying priorities for European civil security research. These areas have a broad scope including information sharing, heightening risk awareness, communication technology, detection technology, robust operational tools for first responders, and common standards for security technology.

The development areas have been categorized as "non-technological" and "technological" areas. However, this is an artificial categorisation and in general any solution to a Critical Technology with Critical Dependence will have both non-technological and technological aspects.

Table 11 summarises the considerations regarding possible research and development areas as well as the respective needs. For details please refer to Working Document 3.3 "Identification and in-depth analysis of alterative technological solutions".[20]

3.2.3.6 Recommendations concerning ethical and fundamental rights issues

Taking into account ethical aspects regarding Critical and Emerging Technologies was a continuous process during all work packages of the ETCETERA project. For this purpose an ethical helpdesk was installed, which was frequently consulted during the entire process.

The results and conclusions regarding ethical considerations were collected and described in detail in the Working Documents 5.1 "Report on Ethical, Political, Legal and Societal aspects concerning Emerging Technologies with Security Implications"[35] and 6.3 "Report on the Evaluation of Ethical Aspects Concerning the Findings on Critical and Emerging Technologies".[36]

Summary of ethical considerations within ETCETERA

Technological innovation is embraced as an unquestionable component of the EU's security policies. From the turn of the century the EU has increasingly promoted the development and employment of "new", "advanced", "next generation" or "emerging" technologies for countering its internal security threats. Consistently with the increasing role assigned to the technological factor in countering such threats, the EU has taken actions in order to acquire the necessary technological tools. It has stimulated the supply of new technologies by supporting relevant research and development (R&D) initiatives at European level and, recently, sustaining the European security industrial sector.

On the regulatory side, the EU has not adopted any framework legislation dealing comprehensively with the category of "Emerging Technologies for security". There are of course different EU legal instruments which are relevant and applicable both at R&D stage and once a concerned emerging technology for security is no longer "emerging" but available and deployable. However, there is no regulation, decision, directive or other EU legal instrument having "Emerging Technologies for security" as main and specific object.

For this reason, recommendations were developed for making emerging security technologies consistent with individual's fundamental rights as stated in the EU Charter of Fundamental Rights (CFREU) and other relevant policy and regulatory documents adopted by the EU. Recommendations for actions to improve the EU governance of emerging technologies for security were developed as well.

35 Emilio Mordini, Matteo E. Bonfanti (CSSC), "Report on Ethical, Political, Legal and Societal aspects concerning Emerging Technologies with Security Implications", ETCETERA Working Document 5.1, February 2013

36 Emilio Mordini, Matteo E. Bonfanti (CSSC), "Report on the Evaluation of Ethical Aspects Concerning the Findings on Critical and Emerging Technologies", ETCETERA Working Document 6.3, June 2013

Nine recommendations for making emerging security technologies consistent with the CFREU

Recommendation 1:
Respect for human dignity should be the leading principle followed in the development and employment of emerging security technologies.

Recommendation 2:
Emerging security technologies should be designed to prevent any unnecessary, arbitrary or not proportional interference with individuals' freedoms, in particular with their right to privacy, right to the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, and freedom of assembly and of association.

Recommendation 3:
Emerging security technologies should – if possible and applicable – enforce the right to privacy and to data protection by design.

Recommendation 4:
Emerging security technologies should be designed and potentially employed in such a way that they do not allow to discriminate among individuals on grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation, cultural, religious or linguistic diversity.

Recommendation 5:
Emerging security technologies should be designed and potentially employed to safeguard the individuals' rights to have ensured a high level of human health.

Recommendation 6:
Emerging security technologies should be designed and potentially employed to ensure a high level of environmental protection.

Recommendation 7:
Only those emerging security technologies should be developed and used that are compatible with the value of a democratic society, i.e. a society that is based on "pluralism", "tolerance", "broadmindedness", "equality", "liberty", "right to fair trial", "freedom of expression, assembly and religion".

Recommendation 8:
Emerging security technologies should only be employed after they have been validated in trials. When involving humans, trials should be carry out in compliance with ethical and legal standards that - among other things - require to obtain the free and informed consent of participating individuals. Trials should demonstrate the capacity of these technologies to achieve fully the intended or expected security effect and perform consistently the required security mission.

Recommendation 9:
Emerging security technologies operating procedures should be subjected to a public and democratic scrutiny

Eight recommendations for improved governance

The following recommendations should be considered by decision and policy makers when defining a governance system of Emerging Technologies for security.

Recommendation 1:
Combine policy guidelines and soft-law (i.e. quasi legal instruments like code of conducts, guidelines) with hard-law to deal with the likely implications generated by the development and future employment of emerging security technologies.

Recommendation 2:
Support and enforce democratic oversight and transparency of programmes aimed at developing and employing emerging security technologies.

Recommendation 3:
Promote ethical, societal, and fundamental rights impact assessments both at R&D stage and after emerging security technologies have been adopted.

Recommendation 4:
Promote and sustain a fundamental rights "by design" approach to the development of emerging security technologies.

Recommendation 5:
Develop and employ those emerging security technologies that show to provide great advantages – in terms of enhanced security and diminished negative ethical, fundamental rights and other societal implications – compared with other possible technological solutions or available technologies.

Recommendation 6:
Establish appropriate systems and procedures for granting the larger part of population may benefit from advantages originating by the development and employment of emerging security technologies.

Recommendation 7:
Promote information and communication campaigns on policies and initiatives on emerging security technologies, and their implications.

Recommendation 8:
Establish adequate regulation, control and licensing regime to prevent emerging security technologies may be "misused" outside a given jurisdiction and contrary to established fundamental rights and etical standards.

4 Conclusion and Outlook

The ETCETERA project provided a plethora of aspects and insights concerning Emerging Technologies and Critical Dependencies in the field of civil security. A special highlight is the large number and variety of methods used within the project. They provide a toolbox for research planning which waits to be opened and used practically.

Besides the application and advancement of the individual methods, the intelligent combination of methods remains a challenge. E.g. the combination of scientometrics and desktop research has been shown to be very fruitful when scanning for Emerging Technologies and deserves further attention.

Another issue that has been raised in the ETCETERA project is in how far additional Critical Dependencies could be overcome by research investments in technologies that are just emerging today. This aspect surely deserves a more dedicated approach.

A further aspect that should not be neglected is the observation that working on the ETCETERA project has brought national actors involved in security research planning closer to each other. The first follow-on projects of subgroups of consortium parties are already on their way.

The two Consultation Campaigns were designed to attract stakeholders beyond the "usual crowd". While the planning and execution of the "parallel workshops" was very complex, the goal of getting persons and organisations involved that had not been in contact with European security research was achieved. The two SETAG workshops are another successful example of how a broader perspective on European security research issues can be obtained.

All in all, the ETCETERA project has contributed to the development of innovative methods for research planning. At the same time it has identified and analysed limitations, especially when dealing with large sets of technology options. We are optimistic that the partners involved, the European Commission, and third parties will find useful building-blocks for further activities in the result of the ETCETERA project.

5 Consortium Parties and Roles

The ETCETERA project was conducted by a consortium of 14 partner organisations. This section gives a brief overview of the organisations and their respective roles.

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)

At present, the Fraunhofer-Gesellschaft maintains more than 80 research units at different locations in Germany. The majority of the 22 000 staff are qualified scientists and engineers, making Fraunhofer Europe's largest application-oriented research organisation.

Two independent institutes of the Fraunhofer-Gesellschaft were part of the ETCETERA consortium: The Fraunhofer Institute for Technological Trend Analysis INT in Euskirchen, and the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe.

Fraunhofer INT has more than 30 years of experience in Technology Forecasting and Planning Support for Research & Development for the German Federal Ministery of Defence. Since about 10 years the focus has been widened to the field of security.

Fraunhofer INT has coordinated and managed the ETCETERA project. Furthermore, it has led the three Work Packages of Strand 2 "Emerging Technologies". This included the execution of one scanning method for Emerging Technologies, one in-depth study, and the compilation of recommendations for an Emerging Security Technology Research Agenda (ESTRA). Additionally, it hosted one of the "parallel workshops" within the 1st Consultation Campaign. Fraunhofer INT also played a major role in Strand 1 "Critical Technologies", providing advice and coordination in Work Packages 1 to 3, including the development and execution of the WBAM process in the 2nd Consultation Campaign.

Fraunhofer ISI is active at the intersection of societal considerations and technology-oriented issues. It is highly networked in security research and since September 2007 has participated in the research policy initiative launched by the French and German governments.

Fraunhofer ISI was mainly active in Strand 2 "Emerging Technologies". It conducted the scenario process and developed the socio-economic model for the evaluation of high risk/high pay-off research.

Totalförsvarets forskningsinstitut (FOI)

FOI is one of Europe's leading research institutes in the areas of defence and security. It has 990 highly skilled employees with various backgrounds. FOI's core activities are research, methodology/ technology development, analyses and studies. FOI is an assignment-based authority under the Swedish Ministry of Defence.

FOI has led Work Packages 1 "Identification of Critical Technologies" and 3 "Identification of Alternative Technological Solutions" within Strand 1 "Critical Technologies". It also developed novel methodology (ITIPOLITRE) and hosted one of the "parallel workshops" within the 1st Consultation Campaign. Within Strand 2 "Emerging Technologies", FOI provided two in-depth studies.

Tecnalia Research & Innovation (Tecnalia)

Tecnalia is an applied research centre committed to the scientific and technological development of the collaborating companies – mainly SMEs –, and society as a whole. Tecnalia was formed by the merger of eight internationally reputed technological centres, resulting the largest private R&D&i entity in Spain and the fifth in Europe, with a staff of over 1,400 employees.

Tecnalia was mainly active in Strand 1 "Critical Technologies", leading Work Package 2 "Identification of Critical Dependencies". It was a key player in developing the format of the "parallel workshops" within the 1st Consultation Campaign and also hosted one of the workshops. Tecnalia provided two in-depth studies in Work Package 5 "In-depth Analysis".

Ingeniería de Sistemas para la Defensa de España (Isdefe)

Isdefe is a state owned company founded in 1985, with the objective of providing technical engineering support and consulting services for advanced technologies in the defence and civil sectors.

Within Strand 1 "Critical Technologies" Isdefe provided an analysis of trade and academic restrictions for knowledge exchanges. In Strand 2 "Emerging

Technologies" it conducted one scanning process for Emerging Technologies, contributed one in-depth study and, together with TNO, developed and tested the SETAG method.

Universität Duisburg-Essen (UDE)

The Chair of Finance & Banking at Universität Duisburg-Essen offers a variety of courses, ranging from introductory courses in finance to advanced courses in corporate finance, capital markets, and banking. The main research areas are risk management and different applications of analysis in corporate finance.

Within the ETCETERA project, UDE provided ideas concerning the development of a socio-economic model for the evaluation of high risk/high pay-off research.

Austrian Institute of Technology (AIT)

The Foresight & Policy Development Department is one of the five departments of the largest Austrian non-university research institution, the AIT Austrian Institute of Technology, and focuses on innovation and sustainability research concerning the grand challenges of the future. Its fifty employees come from different scientific disciplines and are members of numerous international research networks.

AIT was the major provider of scientometrics for the ETCETERA project. It contributed patent analyses to Work Package 2 "Identification of Critical Dependencies". In Work Package 4 "Scanning for Emerging Technologies" it conducted a bibliometrics-based scanning process and was involved in the methodological analysis and exploration process.

Commissariat à l'énergie atomique et aux énergies alternatives (CEA)

CEA is a French state-owned research and technology organisation with nearly 16 000 staff. It is a prominent actor in research, development and innovation in three main areas: energy, health and information technologies, defence and global security.

For the ETCETERA project, CEA provided patent analyses to Work Package 2 "Identification of Critical Dependencies" and one in-depth study to Work Package 5 "In-depth Analysis". Furthermore, it hosted one of the "parallel workshops" within the 1st Consultation Campaign.

Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek (TNO)

TNO is an independent innovation organisation in the Netherlands. TNO's more than 4000 professionals work on practicable knowledge and solutions for the problems of global scarcity. TNO focuses on a safe and secure society by creating innovations for people working in the armed forces, law-enforcement agencies, emergency services and industry.

Together with Isdefe, TNO developed and tested the SETAG method within the 2nd Consultation Campaign of the ETCETERA project.

VDI Technologiezentrum GmbH (VDI-TZ)

The VDI Technologiezentrum GmbH is an associated company of VDI, the Association of Engineers in Germany. Since 1973 VDI Technologiezentrum GmbH has been working on behalf of the German Ministry of Education and Research (BMBF) and for other institutions and enterprises. Its activities aim at increasing the technological efficiency and competence of industry and scientific research. The VDI Technologiezentrum GmbH employs over 200 staff members.

VDI-TZ has contributed to several issues in Strand 2 "Emerging Technologies", leading the analysis of national and European research strategies concerning Emerging Technologies.

Morpho

Morpho, a high-technology company in the Safran group, is one of the world's leading suppliers of identification, detection and e-document solutions. Morpho is specialized in personal rights and flow management applications, in particular based on biometrics, a sector in which it is the world leader, as well as secure terminals and smart cards.

Within ETCTERA, Morpho contributed an industry perspective, especially to the development of a socio-economic model for the evaluation of high risk/high pay-off research. It also conducted two in-depth studies to Work Package 5 "In-depth Analysis".

Ansaldo STS

Ansaldo STS is a leading technology company operating in the global Railway & Mass Transit Transportation Systems business with the provision of traffic management, planning, train control and

signalling systems, security systems and services. It acts as lead contractor and turnkey provider on major projects worldwide. Ansaldo STS is headquartered in Italy, and employs over 4,300 people in 28 different countries.

Ansaldo STS provided an industry perspective to several activities of the ETCETERA project. Furthermore, it hosted one of the "parallel workshops" within the 1st Consultation Campaign.

COMSEC Unternehmensgruppe

For 15 years the COMSEC Group has been successful providing security externally and internally for many companies in various areas of trade and industry. Experienced criminalists, lawyers and latest technology are kept at clients' disposal 24 hours a day, always ready to provide individual solutions for company-specific security problems.

COMSEC provided an SME and end-user perspective to the activities within the ETCETERA project.

Centre for Science, Society and Citizenship (CSSC)

The Centre for Science, Society and Citizenship (CSSC) is an independent research centre specialised in advice on political, ethical and social issues raised by emerging technologies. By taking an interdisciplinary approach, CSSC explores social, cultural and ethical implications of emerging technologies in various fields (e.g., homeland security, biometrics and autoID, smart ambient, ubicomp, cloud computer, disaster preparedness, public health, eInclusion).

CSSC has provided comprehensive ethical and fundamental rights advice to the ETCETERA project. This included contributions to the development of alternative solutions within Work Package 3, the selection and analysis of Emerging Technologies in Work Packages 4 and 5, and support for the development of recommendations for research planning in Work Package 6. CSSC also hosted an ethics workshop, which also served to disseminate information about ETCETERA to a wider audience.

Storstockholms brandförsvar (SSBF)

The Greater Stockholm Fire Brigade operates fire and rescue services in 10 municipalities in central Sweden. It has 850 employees, 15 fire stations and 9 rescue corps that serve 1.1 million people.

SSBF provided an end-user perspective to the ETCETERA project. It was especially active in Work Package 3 "Identification of Alternative Technological Solutions" where it provided a "reality check" to the solutions proposed. It also provided the facilities for one of the "parallel workshops".

The authors thank Mrs Sylvia Scheid for support in design and layout.