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

EVALUATION OF CRITICAL AND EMERGING SECURITY TECHNOLOGIES FOR THE ELABORATION OF A STRATEGIC RESEARCH AGENDA

DELIVERABLE D6.1

Recommendations for an Emerging Security Technology Research Agenda (ESTRA)

Authors: Joachim Burbiel, Ruth Schietke (Fraunhofer INT)

November 2013

Dissemination Level: PU

1 Introduction

1.1 The ETCETERA approach

During the last decade, a number of activities have been carried out in an effort to plan effective security research in Europe. The majority of them had the character of expert consultations.[1] Although expert consultations are of course highly important, there has been little methodological research on how to improve security research planning and evaluation. The ETCETERA project aimed at both advancing the methodology of security research planning on a European level, and providing impulses for the development of specific research agendas.

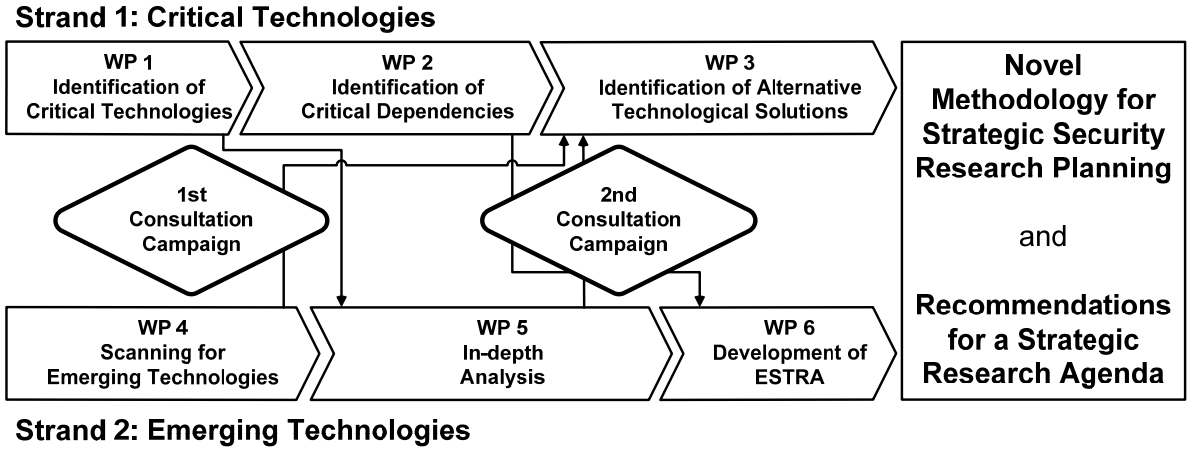

Figure 1: The ETCETERA timeline

The project features two research strands dealing with Critical Technologies and Emerging Technologies, respectively (Figure 1). In the context of the ETCETERA project, Critical Technologies are understood as technologies that are necessary to ensure security in Europe now or in the near future. A number of Critical Technologies were examined for Critical Dependencies. Critical Dependencies arise if European industry is not sufficiently independent from other world regions in providing Critical Technologies to end-users. Critical Dependencies might be rooted in, e. g., insufficient production capacities, IPR issues, raw material dependencies, and trade restrictions.[2]

Emerging Technologies, on the other hand, will only become commonly available in 10 to 15 years time. The ETCETERA project applied three methods of scanning for Emerging Technologies that might have an influence on European security in the future. Several in-depth analyses were conducted to identify opportunities that Emerging Technologies offer for civil security and security industry.[3]

[1] For details see sections 2.1 and 2.2
[2] This issue has recently received heightened attention by the European Commission under the key word “security of supply”, e.g. in its communication “Towards a more competitive and efficient defence and security sector”, Brussels, 24 July 2013, COM(2013) 542
[3] The FP7 project “Foresight of Evolving Security Threats Posed by Emerging Technologies” (FESTOS, March 2009 to October 2011) has dealt with the “dark side” of Emerging Technologies and thus ideally complements the ETCETERA approach of looking at the chances of Emerging Technologies.

This report describes the conclusions drawn from these processes concerning recommendations for the development of an Emerging Security Technology Research Agenda (ESTRA). Such an Emerging Security Technology Research Agenda could be part of the "non-dependency strategy on critical technologies" recently called for by the Committee on Foreign Affairs of the European Parliament, which explicitly encompasses "unlimited access to and availability of civilian and military (dual-use) emerging and key enabling technologies." [4]

1.2 The road to recommendations for an Emerging Security Technology Research Agenda (ESTRA)

The general approach of Strand 2 "Emerging Technologies" (see Figure 1) is to analyse technologies that are now just "emerging" in order to identify opportunities that such technologies might offer for civil security and European security industry.

In order to make sure that the recommendations developed are compatible with existing national and European research strategies, an analysis of relevant activities is documented in section 2.

In the process of generating recommendations for an ESTRA, several methods of technology scanning (WP 4) were combined with thorough in-depth analyses (WP 5). A plethora of methods were combined to ensure both highly validated and relevant results. Experiences from these novel combinations will enhance the design of future strategic research planning projects. The relevant results of WP 4 and WP 5 are discussed in sections 3.1 and 3.2 of this report.

The project also included two "Consultation Campaigns" to generate input from technical experts, end-users, and public authorities. The "Parallel Workshops" within the 1st Consultation Campaign (spring and summer 2012) provided some futuristic ideas for security technologies (section 3.3). Two of the activities within the 2nd Consultations Campaign (winter 2012 and spring 2013) were closely related to the development of this report:

- an adapted Disruptive Technology Assessment Game (DTAG, developed and conducted by TNO and Isdefe) and
- a scenario process (developed and conducted by Fraunhofer ISI).

The results of these consultations are discussed in sections 3.4 and 3.5, respectively.

In addition to this, a novel methodology for economical assessment of high risk/high pay-off technologies was developed by a group of academic and RTO researchers under involvement of industrial specialists (section 3.6).

The results of Strand 1 "Critical Technologies" are briefly reviewed in section 4, as adequate planning of the development of Emerging Technologies can be seen as a way to avoid Critical Dependencies in the future.

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

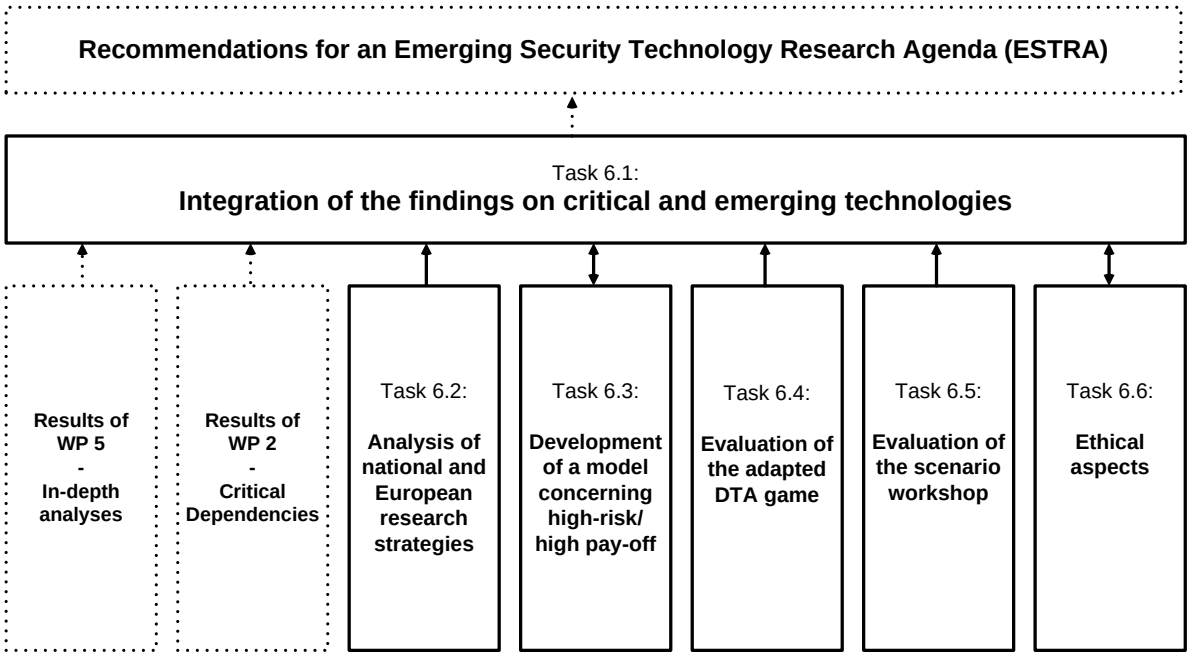

Figure 2: Schematic build-up of WP 6 "Development of ESTRA". Dotted lines indicate reports and other kind of information flows.

In Work Package 6 all prior results on Emerging Technologies were taken into consideration for the development of recommendations for an ESTRA (Figure 2). They mainly consist of methodological recommendations (section 5.1), but some ideas on technology priorisation are also given (section 5.2). Recommendations concerning ethical and fundamental rights issues complete this chapter (section 5.3).

2 Background

2.1 Planning efforts within the European Union regarding Security Research – a brief history

Planning efforts concerning the themes of EU Security Research started with meetings of the *Group of Personalities* (GoP) in 2003 and 2004. As an outcome, the *European Security Research Advisory Board* (ESRAB) was created. In this board, comprising approx. 70 persons and supported by over 300 experts, the foundations of what is now the Security theme of the 7th Framework Programme were laid.

From September 2007 to September 2009 an even larger board, the *European Security Research and Innovation Forum* (ESRIF), aimed at devising a medium- to long-term strategy for European security research.[5]

While the actions previously mentioned were conducted by the European Commission (EC) directly, several advisory projects were carried through in a parallel fashion. These were financed by the EC through research and support grants. The first project in this line of development was the *Security Network for Technological Research in Europe* (SeNTRE, December 2004 to January 2006), which aimed at supporting ESRAB through the provision of expert advice.

From January 2007 to May 2008 the *STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities* (STACCATO) enlarged the efforts of SeNTRE to all 27 member states. It also aimed at creating a network of security technology suppliers and users with the goal of achieving a more integrate European security market. One of the outcomes was the STACCATO Taxonomy, which tried to integrate all security related technologies and capabilities into one systematic framework.[6]

The *Coordination action on Risks, Evolution of threatS and Context assessment by an Enlarged Network for an r&D rOadmap* (CRESCENDO, July 2009 to June 2011) project was granted as part of the first security research call (Work Programme 2008). It was again a Coordination and Support Action (CSA) with the aim to collate information from a diversity of expert sources into R&D-roadmaps.

FORESEC was an FP7 project especially dedicated at the development of scenarios for future European security (February 2008 to November 2009).

Security Technology Active Watch (STRAW) was another CSA (October 2008 to May 2010). The aim of STRAW was to collect information from a variety of stakeholders and to transfer it to the public at large, public authorities, and the research community. Another objective was to revise the STACCATO taxonomy.

Apart from these programmatic efforts, several institutions have contributed to European security research planning. As an example the *Institute for the Protection and Security of the Citizen* (JRC-IPSC, Ispra) issued the Research Strategy Paper "Emerging technologies in the context of 'security'" in September 2005. It includes several ideas that found their way into the security research work programmes of the 7th Framework Programme.

[5] See section 2.2 for some results of this process.
[6] Within the ETCETERA project all research concerning Critical Technologies started from the STACCATO taxonomy (see section 4).

Furthermore, a Security Research Advisory Group (SecAG) was established in 2007 to provide advice to the European Commission concerning goals, strategies and priorities in European security research.

2.2 Cursory analysis of European security research planning concerning Emerging Technologies

In 2005 the **European Security Research Advisory Board (ESRAB)** was set up to draft strategic lines for European security research within the European 7th Research Framework Programme. ESRAB's final report outlined a capability-based approach to security research. [7] This core approach concerned four missions of future security research defined by the EU Commission while ESRAB was still in operation. The four missions were:

- Security of the citizens/protection against terrorism
- Security of infrastructures and utilities
- Intelligent surveillance and border security
- Restoring security and safety in case of crisis

From these missions, ESRAB first derived capabilities, condensed in 11 functional groups, to which technological solutions were assigned:

- risk assessment, modelling and impact reduction
- doctrine and operation
- training and exercises
- detection, identification and authentication
- positioning and localisation
- situation awareness and assessment (surveillance)
- information management
- intervention and neutralisation
- communication
- command and control
- incident response

"Capability Projects" were intended to enhance developments that improve the maturity level of a specific capability or of a group of interrelated capabilities. Technology development at this level should explicitly include new and breakthrough technologies. "Integrated Projects" should develop capabilities, technologies and disciplines at an appropriate state of readiness into innovative combinations. Under "Demonstration Projects", a number of systems were to be combined and integrated into a system of systems.

Within the European 7th Research Framework Programme, the European security research programme was considered as an independent topic for the first time. Over its 7-year duration, the programme concentrated on the above mentioned four missions. Additionally, sector-crossing areas like security systems integration, security and society, and security research coordination and structuring were covered. Projects had to offer suitable solutions or conduct experiments to test the suitability of solution prototypes. Beside a smaller share of basic research including a long-term future perspective, the European security research programme mainly called for applied research and thus particularly addressed the industrial sector. This was also reflected by the fact that the European security research programme within FP7 was associated to DG Enterprise and Industry.

[7] European Security Research Advisory Board (ESRAB): Meeting the challenge: the European Security Research Agenda: A report from the European Security Research Advisory Board, Sep. 2006.

In parallel to the Framework Programme, the European Commission set up the **European Research and Innovation Forum (ESRIF)** in 2007. Up to its conclusion in 2009, ESRIF's tasks were to advise the European Commission on the further development of security research within FP7 and to draw up a long term strategic agenda for future security research activities.[8] This included the development of a roadmap for future security research activities. Table 1 summarises the items of the ESRIF roadmap for which a "long term" perspective is mentioned, as these items are most likely associated to the application of technologies that are now just emerging.

Table 1: Items of the ESRIF roadmap with a "long term" perspective

Purpose	Technology	Timeline	ESRIF running no.[8]
Enabling the public	• Public could be best enabled to actively contribute to such solutions • What the key enablers are • How public should be educated, trained and prepared to be ready to act accordingly when the moment is there.	short to long term (step-by-step approach)	33
Prevention of CBRN incidents by effective multinational counter proliferative organisational measures: • Increased CBRN-security of infrastructure (including knowledge, material, and equipment) involving industry, academia, research institutes, and governmental agencies • Global awareness of dual-use potential • Tools for facilitating implementation and global adherence to CBRN regulations and international conventions	• Ability to prioritise and perform technical assessment within (inter)national networks • Better and more flexible coverage of emerging threats in CBRN-related treaties; better defining general purpose criteria, systems, and having more possibilities and mandates for monitoring • Creating dual-use awareness • Design of toolbox for monitoring and verification of implementation of (new) CBRN treaties • Develop alternatives to replace radioactive sources by non-radioactive means • Develop solutions for safe disposal of radioactive sources • Development of deterring and norm-enforcing tools and methodologies against use of agents as violent means • Down-blending surplus HEU to LEU safely and economically • Safe, quick, and secure process to dismantle obsolete nuclear facilities	short to long term	49
Early warning, monitoring, and surveillance in preparation for or as an immediate response to CBRN incidents: • On-site or remote automated and reliable surveillance and detection for the security of the public • Completely networked warning and situational awareness system that can be used seamlessly by first responders, decision makers, and everyone working in possible CBRN scenarios from all nations • Improved global disease surveillance systems including awareness of rare diseases	• Detection of toxicity and virulence requiring innovative databases for the prediction of toxicity and virulence by molecular and submolecular properties • Detection technology for novel type agents (e.g. bioregulators, peptides, non-lethal weapons, non-traditional agents) • Harmonization of testing and validation procedures for new detection instruments • International harmonisation of threshold values for application of measures • Passive or active detection/imaging technology for the detection of chemical hazards • R&D towards real-time detection of suspicious aerosols. • Stand-off / early warning detection technology including orbit based surveillance means • Technology for equipment with dose-rate meters for • early detection of radioactivity • Technology to mark radioactive sources with a fingerprint • Develop non-invasive methods for pre-symptomatic • detection of disease (alert state dependent)	short to long term	51

[8] European Research and Innovation Forum (ESRIF): ESRIF Final Report, December 2009.

Mitigation: • broad-spectrum treatment of CBRN hazards • Antidotes against broad spectrum of threat agents • specific treatment where necessary	• Development and stockpiling of more effective vaccines, antitoxins and chemotherapeutics with longer shelf lives and safer profiles • Antidote activities on: stabilization, appropriate coating material and fillers, microencapsulation and improved logistic systems • Basic research designed to measure sensitive markers of nerve agent exposure to assure that low-level exposures are not associated with long-term or delayed health effects • Specific know-how and capacity for rare situations, such as treatment of patients with severe radiation injuries	short to long term	55
Satellite comms in System-of-system capability	Satellite Constellations and Formation Flying (FF) in the Networked Environment	mid to long term	62
Space Surveillance in System-of-system capability	Synthetic aperture radar (SAR) systems to the features of image acquisition in all time, all weather conditions and a size of the spatial resolution cell is independent of the distance between target-sensor and of the wavelength for ideal processing. These requests are on one hand the sufficient for detection, recognition and identification, and on the other hand for a broad spectrum of applications, e.g. worldwide reconnaissance, surveillance, catastrophe monitoring, border control, etc.	mid to long term	63
European Security Technological and Industrial Base (STIB)	• Develop or refine the mapping of security stakeholders in all EU-27 Members States. • Identify their capabilities, strengths and weaknesses.	short, mid and long term	80
Education and training	• Develop specific programmes to educate the public on security issues and available solutions • Associate the decision makers , regulators and media to these programmes • Use scenarios to develop training exercises	short, mid and long term	82
Evacuation of population after a catastrophic event	Modelling and simulation tools of residential areas and built infrastructure, for virtual scenarios of evacuation and sheltering.	long term	10
early warning space systems	early warning and ELINT satellite solution (GEO satellites with very large deployable reflectors, mini/micro sat constellations, nanosat disposable constellations)	long term	65
Space Situational Awareness	Ground radar and telescope infrastructure, space weather, survey/tracking and space-imaging solutions through in-orbit demonstration via dedicated missions	long term	68
Space environment and Space Weather	The study and prediction of space weather by integration of data resulting from multiple satellites, detectors and forecasting systems is a key element in this respect.	long term	69
Good governance, referring to the well-ordered flow of information, authority and public resources.	Good governance can be strengthened on the European level by increasing accountability, and seeking new ways to instill it as a norm. As the nature of European governance changes, research should continue to innovate and support experimentation in models of power sharing, coordination and interaction.	long term	88
Ethics and trust, referring to the willingness of European citizens to put their lives and well-being into the hands of others.	• Trust in authorities, systems, and other citizens must be built through education, training and other forms of long-term trust-building interactions. • New forms of communication between public authorities and citizens should be developed and promoted.	long term	93

2.3 National Security Research Strategies

2.3.1 Overview of the strategies and programmes studied

Several European member states have issued national security research strategies or started security research programmes, either before the inclusion of the security theme in FP7 (2007) or as a reaction to this event:

- In **Austria**, the security research programme KIRAS was established in 2005.
- The **German** programme "Forschung für die zivile Sicherheit" was started in 2007 and is now in its second funding phase (2012-2017).
- The **British** security research programme "Global Threats to Security" was initiated in 2008. It has since been renamed "Global Uncertainties: Security for all in a Changing World" and will run until 2018.
- **France** considers security research to be a part of defence research. The key strategies are "Politique et Objectifs Scientifiques (POS)" (issued 2006 and updated frequently) for basic research, and the "Plan stratégique de recherche et technologie (PS R&T)" of 2009 for applied research.
- **The Netherlands** have a strong tradition in strategic security thinking. Its "security research agenda" is constituted by several independent research programmes, e.g. in the fields of forensic sciences, ICT security, and high-tech materials and systems.
- **Sweden** does not yet have an explicit "security research strategy", but preparatory work has become visible, e.g. the "Nationell forsknings- och innovationsagenda - Civil säkerhet" issued in 2011 by the Swedish Security and Defence Industry Association (SOFF)
- **Spain** does not have an explicit "security research strategy". Nevertheless the general "Plan Estatal de Investigación Científica y Técnica y de Innovación" (2013-2016) mentions security research without going into much detail. In contrast, Spain has issued a very detailed "Estrategia de Tecnología e Innovación para la Defensa" in 2010 which highlights research priorities even beyond the purely military sphere. Spain shares the French view that security and defence research are essentially the same thing.

2.3.2 Analysis concerning Emerging Technologies

In order to ensure ESTRA being compatible with existing national security research strategies, analyses of the countries mentioned above were conducted regarding their consideration of Emerging Technologies in security research. The analyses revealed which technology areas of the ETCETERA process are generally covered by national research strategies and programmes at state and institutional level (Table 2).

Table 2: ETCETERA's Emerging Technology Areas and the number of European countries analysed addressing them in the context of security research[9]

ETCETERA Emerging Technology Area	Countries **fully** addressing the technology area	Countries **partly** addressing the technology area
Biometrics	4	2
Communication Technology	6	0
CBRN Identification	3	3
Energy Technology	0	6
Environmental Security	2	4
Human machine Interface	0	4
Human Science	5	1
ICT and Electronics	6	0
Mobile Platform Technologies	2	1
New and Smart Materials	3	2
Less-lethal Means	1	0
Sensor Technology	5	1
Cross Sectional Themes	0	6

Taking into account these findings, three groups of Emerging Technologies can be constructed:

1. Emerging Technology areas that receive **high attention** in national security research programmes:
    a. communication technologies,
    b. ICT,
    c. sensor technologies,
    d. human sciences, and
    e. biometrics.
2. Emerging Technology areas that receive **some attention** in national security research programmes:
    a. CBRN identification,
    b. environmental security,
    c. mobile platform technologies,
    d. energy technologies, and
    e. cross-sectional themes.
3. Emerging Technology areas that receive **little attention** in national security research programmes:
    a. human-machine interface, and
    b. less-lethal means

[9] Spain is not included for technical reasons.

2.4 European research strategy concerning Key Enabling Technologies

In June 2011 the "High-Level Expert Group on Key Enabling Technologies" published a final report on its activities.[10] The six **Key Enabling Technologies (KETs)** prioritised were:

- Nanotechnology
- Micro- and nanoelectronics
- Industrial biotechnology
- Photonics
- Advanced materials
- Advanced manufacturing systems (as a cross-cutting capability)

The group emphasised that especially the combined application of these knowledge- and capital-intensive technologies would lead to highly innovative products and thus to a competitive industrial base.

Concerning research priorities, the high-level group found an over-emphasis on basic research in Europe. The group thus recommended a shift of budgets towards applied research and other measures to overcome the "valley of death" between research and commercialisation.

In its communication "A European strategy for Key Enabling Technologies – A bridge to growth and jobs", the European Commission took up many suggestions from the high-level group.[11] At the inaugural meeting of a new "High Level Group on Key Enabling Technologies" in February 2013, an agreement between the European Commission and the European Investment Bank was signed in order to make KETs a priority when considering about strategic investments.[12]

2.5 European research strategy concerning Critical Space Technologies

The most prominent activity concerning Critical Technologies in Europe is the elaboration of "Critical Space Technologies for European Strategic Non-Dependence". This process is a joint activity of the European Space Agency (ESA), the European Defence Agency (EDA) and the European Commission (EC). The goals of this process include:

- Reduce the dependence on critical technologies and capabilities from outside Europe for future space applications.
- Enhance the technical capabilities and overall competitiveness of European space industry satellite vendors on the worldwide market.
- Open new competition opportunities for European manufacturers by reducing the dependency on export restricted components that are of strategic importance to future European space efforts.
- Enable the European industry to get non-restricted access to high performance components that will allow increasing its competitiveness and expertise in the space domain.
- Improve the overall European space technology landscape and complement the activities of European and national space programmes.

The 25 technologies originally listed in 2008 have little direct relevance for security applications.

[10] High-Level Expert Group on Key Enabling Technologies, "Final Report", June 2011
[11] European Commission, "A European strategy for Key Enabling Technologies – A bridge to growth and jobs", 26 June 2012, COM(2012) 341
[12] European Commission, "Agreement with EIB for breakthrough of Key Enabling Technologies", Press release on 27 February 2013, MEMO/13/150

3 Identification and Prioritization of Emerging Technologies

3.1 Identification of Emerging Technologies with relevance to security

3.1.1 Overview

As described in section 1.2, 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 prioritization 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.

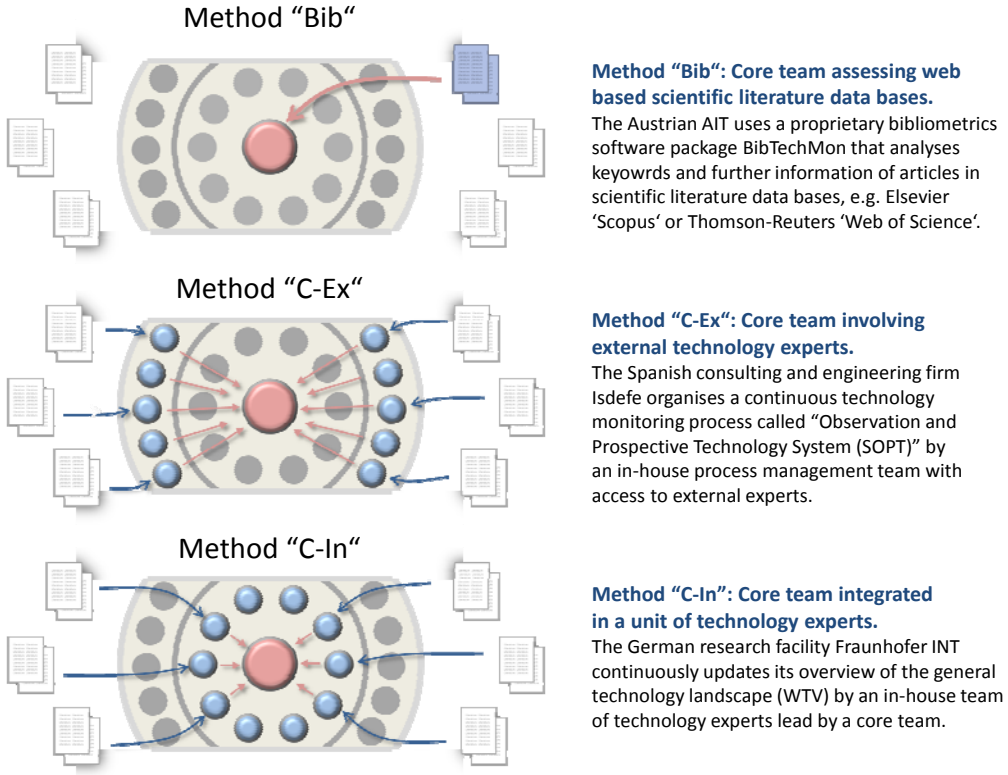

Figure 3: Schematic depiction of the technology scanning methods applied.[17]

3.1.2 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, with the following list of validated Emerging Technologies being the final output.[13]

Table 3: Complete prioritised list of Emerging Technologies with security implications in time frame years 2020 to 2030.[14]

	TA1: Biometrics	no technologies				

	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	no technologies				

	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	no technologies				

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

[14] Note: All technologies within TA1, TA3, and TA6 were either not expected to hit the market within this timeframe or had insufficient security relevance.

	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

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.

For further details of the process and results (e. g. alternative rankings) please refer to Deliverable 4.1[13] and Working Document 4.1.[15]

3.1.3 Results of comparison and assessment of the methods applied

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 expectation that the three methods applied would lead to more or less overlapping results was not met.

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.

[15] 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

Of the 127 original items, 94 were judged to be "valid". Interestingly, 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%). While the hit rate for "security relevance" was comparable for the three methods, the pass rate for "time frame" was markedly different: While the method based on an in-house expert team did very well in assessing technology readiness, probably because the experts were well acquainted with technology foresight exercises, many of the results of the method working with external experts we considered to come to maturity before 2020. In the case of bibliometrics this effect was even more pronounced, with most items initially found being considered to come into the market before 2020 at a later stage. One conclusion that can be drawn from this is that judging technology maturity is harder than judging the relevance of technology for security.

Another important aspect of technology scanning is "completeness": Have all relevant technology areas been investigated or are there blind spots? A first alignment of the "valid" technologies identified with the key enabling technologies (KETs) defined by the European Commission (section 2.4) revealed that all KETs have been addressed.[16] There is little correlation between the items listed in Table 1: Items of the ESRIF roadmap with a "long term" perspective" and the Emerging Technologies with security implications identified in the ETCETERA project. Surprisingly, many of the technologies identified in this project as being emerging (timeframe of 15 to 20 years until broad market availability) show up as "short term priorities" in the ESRIF roadmap. Some examples are New and Smart Materials, Explosives Tracking/Tracing Technologies, New CommunicationTechnologies (e. g. Cognitive Radio). Alignment with the sections of the STACCATO taxonomy also gave the impression that a high level of completeness had been achieved. An analysis of "technologies per technology area" revealed that the three methods had been complementary, which supports the idea of applying several methods in parallel.

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 suggested 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 Deliverables 4.2[17] and 4.3.[18]

[16] Except "advanced manufacturing systems", which is considered to be a "cross-cutting KET".
[17] 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
[18] Beatrix Wepner (AIT), Guido Huppertz (Fraunhofer INT), "Ideas for a novel method for emerging technology identification", ETCETERA Deliverable 4.3, November 2013

3.2 In-depth analyses

3.2.1 Overview

Taking into account the priorisation presented in Table 3 and the technical proficiency of Consortium Parties, eight technologies and one technology area were selected for in-depth studies:[19,20]

- 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)

The analyses comprise around 15 pages each and are subdivided in six sections:

- Technology Description
- Security Relevance
- Time Frame
- Application and Market Potential
- Ethical Consideration
- Technology Profile

3.2.2 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).

This does, nevertheless, not preclude that the other technologies prioritised in Work Package 4 (see section 3.1.2) are less relevant for European security than the ones studied in depth within Work Package 5.

[19] 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

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

3.3 Parallel Workshops

3.3.1 Overview

In order to broaden the scope of the initial research, five workshops were conducted from March to June 2012. These workshops were held in five European countries (Spain, Germany, Italy, Sweden, and France) in the five corresponding national languages, but applying the same method. A total of 72 security research stakeholders attended these workshops. Two rather open questions were discussed with invited experts applying the World Café methodology:[21]

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!

3.3.2 Results concerning futuristic solutions

While the first question aimed at identifying Critical Technologies, the second was more focused on solution space and futuristic technologies. In Table 4 a list of future technologies "invented" at the workshops is presented. The list ranges from broad themes to specific technologies.

Table 4: Futuristic solutions suggested at the Parallel Workshops.

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 for remote detection of 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 procedures
Futuristic technologies • A "disease scanner" (for rapid medical diagnosis) • A (vehicle 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 tools for power failures (including cascading effects)

[21] Malek Khan, Steven Savage (FOI), "Documentation of methods and workshops", ETCETERA Deliverable 1.3, October 2013

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.

3.4 SETAG Workshops

3.4.1 Overview

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 the next chapter.

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) 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 4). 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.[22]

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

[22] 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

Two SETAGs were held:

1. In The Hague (Netherlands) with Dutch participants only
2. In Madrid (Spain) with Spanish participants only

Figure 4: Game board of the Security Emerging Technology Assessment Game (SETAG) within ETCETERA.

3.4.2 Results from 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" for the IoS-cards

At the latter stage, based on the voting done by the participants, a distinction seems to arise between a top-3 and the other IoS-cards (Table 5). When considering the actual use of IoS-cards (Table 6), albeit in predefined scenarios, there was no similar pattern in the results.

Based on the three IoS-cards that got most votes, it seems as though the end users had a relatively clear preference for certain issues. Solutions with most votes improve operational communications and physical safety of responders, or allow for better intelligence gathering:

Table 5: Result of the IoS-cards voting[23]

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

[23] SETAG-NL gives the number for the game conducted in the Netherlands, while SETAG-ES stands for the game in Spain.

When looking at the actual use of IoS-cards, a slightly different picture appears:

Table 6: Results of the IoS-card application[23]

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

It should be noted however, that there was large difference between the SETAG in the Netherlands and the SETAG in Spain in the amount of IoS-cards used per scenario. Therefore, although normally actual behaviour would provide the most direct test of intentions, no definitive conclusions can currently be drawn from these results. Possible explanations for the difference in amount of IoS-cards used per scenario are the difference in number of participants (six end-users in the Netherlands and thirteen in Spain), the difference in type of participants (mix of police and fire brigade in the Netherlands, mainly police in Spain) or the change in task forms.

If the findings of the two SETAG workshops are re-aligned with the underlying Emerging Technologies, the following technologies have obtained **most attention** by workshop participants:[24]

- 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“)

The following technologies have drawn the attention of participants to **a lesser degree**:

- UUV/USV – Collision and obstacle Avoidance Technologies (plus) Advanced Algorithms for Classification (IoS-Card “Mini above water vehicle”)
- Sensors on Unconventional Flexible Substrates (IoS-Cards “Wearable positioning and navigation” and “Smart bandage for wounded personnel”)
- Smart Materials (IoS-Cards “Wearable positioning and navigation”)
- TA3: CBRN Identification (IoS-Card “Stand-off detection of BC agents”)

[24] Joachim Burbiel, Ruth Schietke (Fraunhofer INT), “Report on the Evaluation of the 2nd Consultation Campaign”, ETCETERA Working Document 3.2, November 2013

3.5 Scenario Process

3.5.1 Overview

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 analyse their possible influences on the development of the 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 closely related 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.[25]

During a four-step process, key factors, fostering or hindering the development of the selected Emerging Technologies, were determined and differences were explored:

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 WP 4 “Scanning for Emerging Technologies with Security Implications” and WP 5 “In-depth Analysis”.[26] As a result of this approach, nine Emerging technologies were considered in the scenario process (Figure 5). During the workshops, the four technologies belonging to the “sensor technology” area were investigated as one complex item, while the other technologies were studied individually.

[25] Antje Bierwisch, Victoria Kayser, Erduana Shala, Ewa Dönitz, Stephan Grandt (Fraunhofer ISI), “Report on the scenario based workshop”, ETCETERA Working Document 6.2, November 2013
[26] For details of the selection process of emerging technologies with security implications please refer to Deliverable 4.1 “List of Emerging Technologies with Security Implications” and Working Document 4.1 “Report on the scanning for emerging technologies with three different methods, including a provisional list of emerging technologies for security purposes”.

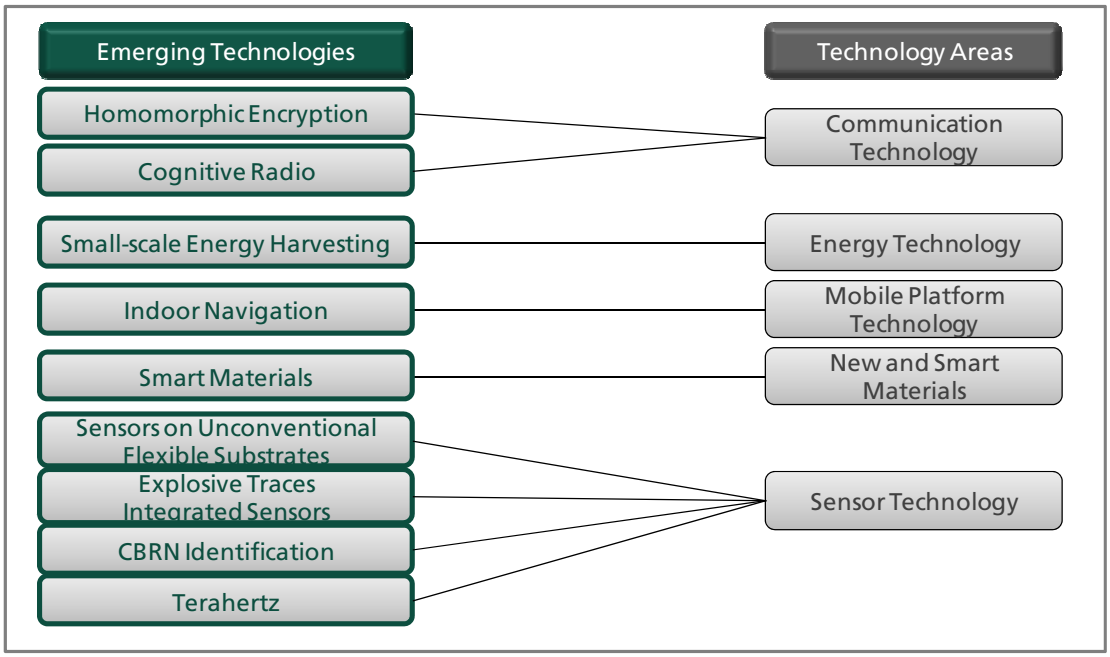

Figure 5: Prioritised selected Emerging Technologies and their technology areas.

3.5.2 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 conceptual 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.

3.5.3 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 that 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:

1. Security understanding and concerns in society
2. General development of EU
3. EU security policy and legal framework
4. Design and implementation of security technologies
5. EU R&D infrastructure
6. Cultural influences and social change
7. Role of intellectual property rights (IPR)
8. Relevance of security in different sectors
9. Attitude towards technologies in society
10. Production and consumption behaviour
11. Design and orientation of R&D
12. Capabilities & capabilities in R&D
13. Commercialisation strategy in R&D
14. Global economic arrangement
15. Global emergencies and disasters
16. Global shifting powers and balances
17. Security industry

The possible future developments of the key factors were described as "future projections". During the elaboration of future projections regarding all relevant key factors more than one alternative assumption were developed for each factor. A total of 49 future projections were created for the 17 key factors.

3.5.4 Development of the scenarios and second scenario 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"

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 7).

Table 7: Assessment of selected Emerging Technologies within different scenario contexts.

		Green scenario 2nd Woodstock – a peaceful world	Orange scenario Technology rules the world	Pink scenario Buddenbrooks global	Yellow scenario 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	+	+	-	-

3.5.5 Results concerning Emerging Technologies

Table 7 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.

3.5.6 Conclusions regarding the development of a research agenda

Basically, it can be stated that 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:

- Identifying barriers and drivers
- Identifying key factors in the developed scenarios which have an important influence of technology development and application
- Identifying relevant dimension that have an influence of 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, the ecological and political/ legal aspects were rarely discussed in this context.

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 7):

- “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 fourth.
- “Cognitive radio” was received well in all scenarios.

3.6 Input from socio-economic considerations

3.6.1 Overview

For further assessment of the selected Emerging Technologies regarding high risk/high pay-off, a socio-economic model was developed. For this, a multi-criteria decision analysis with several dimensions was conducted. Within this model, qualitative and quantitative data were considered to fulfil the requirements of a holistic assessment approach by integrating expert opinion and quantitative facts. The bases of the socio-economic model were the results of the previous work packages as well as the output of the scenario workshops and an online survey executed by the Fraunhofer Institute for Systems and Innovation Research ISI.[27]

The assessment approach includes 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, containing drivers and barriers which were identified as explicitly relevant.

[27] Antje Bierwisch, Stephan Grandt, Victoria Kayser (Fraunhofer ISI), “Socio-economic Model for the Assessment of Emerging Security Technologies”, ETCETERA Deliverable 6.2, October 2013

3.6.2 Global results combining the qualitative and quantitative assessment

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

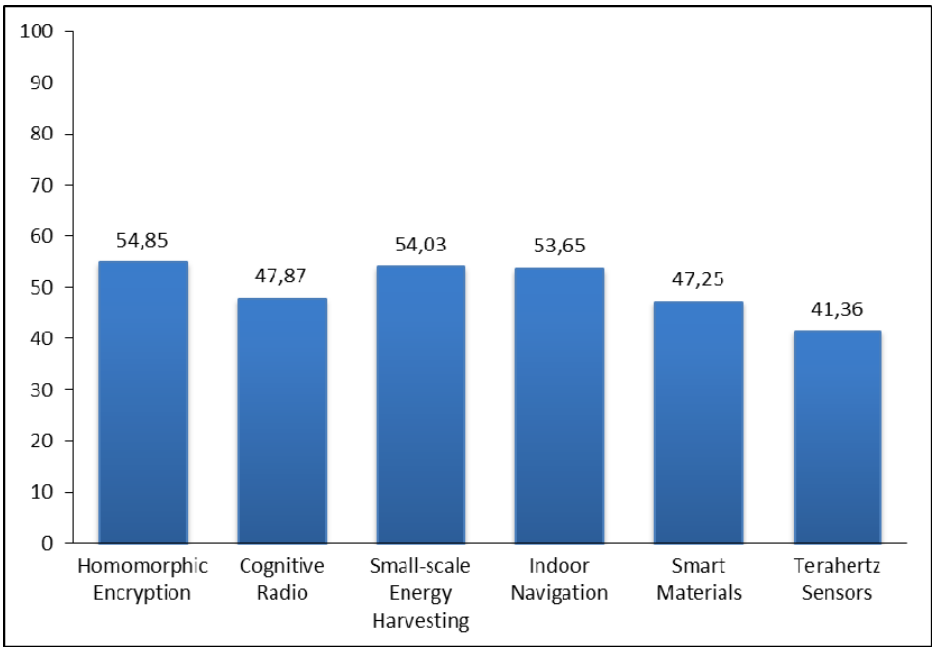

Figure 6: Scores for the selected Emerging Technologies – Ranking of global assessment.

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 a last expert consultation exercise, conducted as an online survey, the weighting of ecological and legal & political dimension 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.[27]

4 Reducing Critical Dependencies

4.1 Introduction

As mentioned in the introduction (section 1.1), the ETCETERA project also aimed at identifying Critical Dependencies and proposing ways to achieve European technological independency. The results of this process are reported in Deliverable 3.1.[28]

Nevertheless, intelligent research planning concerning Emerging Technologies can be considered as a way to avoid future Critical Dependencies. Selected results of the research conducted within Strand 1 of the ETCETERA project are thus presented and discussed in this section in order to delineate clues on Emerging Technology research planning.

4.2 Critical dependencies analysed

The STACCATO taxonomy[29] was used as a starting point to obtain a list of Critical Technologies, i.e. technologies considered to be essential for European security in WP 1 "Identification of Critical Technologies".[30] Within WP 2 "Identification of Critical Dependencies", the technologies on this list were further analysed, searching for cases in which European industry is dependent on extra-European sources or providers.[31]

With the help of the newly developed Weighted-Bit Assessment Table for Critical Dependencies (WBAT-CD),[32] the dependencies to be studied further were prioritised, applying the following criteria:[33]

- Which technology has "a big problem"?
- What is the cause of the Critical Dependency?
- How much do we know about the technology?

The suggestions were sorted into a "Main List" of highly interesting technologies and into a "Reserve List" of slightly less interesting technologies (see Table 8 and Table 9). In some cases, STACCATO categories have been put on the lists, e.g. when further differentiation did not seem to make sense for further analysis.

[28] Steven J Savage, Malek Khan, Riitta Räty, Camilla Trané (FOI), "Report on Validated Alternative Technological Solutions", ETCETERA Deliverable 3.1, November 2013
[29] The STACCATO taxonomy was developed by a previous EC funded PASR project and can be downloaded here: http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf
[30] Malek Khan, Steven Savage, Aziz Ouacha (FOI), "Validated List of Critical Technologies", ETCETERA Deliverable 1.2, September 2012
[31] Antonia Bierwirth, F. Javier Herrera, "Intermediate report on critical dependencies", ETCETERA Deliverable 2.1, July 2013
[32] Joachim Burbiel (Fraunhofer INT), "Report on the adaption of the Weighted-Bit Assessment Method", ETCETERA Working Document 2.8, May 2013
[33] Joachim Burbiel (Fraunhofer INT), "Report on the WBAM-assisted Workshop", ETCETERA Working Document 3.4, May 2013

Table 8: Main list (highly interesting technologies)[34]

STACCATO 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 in L13)
407-3	Secure database management	IPR & market (L13)
504B-2	Simulation for decision making (real time)	Market problems (L13)

Table 9: Reserve list (slightly less interesting technologies)[34]

STACCATO 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
101-7 101-8	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	Analog/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

[34] "L13" refers to inclusion in another list of prioritised Critical Dependencies developed within the ETCETERA project.

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

4.3 Relevance for the development of ESTRA

Within WP 3 "Identification of alternative technological solutions" all Critical Dependencies on the main list (tableTable 8) were analysed.[35] 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).[36] The types of solutions suggested are summarised in Table 10.

Table 10: Types of solutions suggested for overcoming selected Critical Dependencies

		Suggested Solutions		
STACCATO Code	**Short Title**	**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	

[35] The number of items on Table 10 is lower than on Table 8, as some items have been joined.
[36] 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

For developing an Emerging Security Technology Research Agenda (ESTRA) those Critical Dependencies calling for basic research are most relevant:

1. In the case of "Neutron detection technologies" the experts suggested overcoming a possible future shortage of ^{3}He by researching alternative neutron detector materials, e.g. ^{6}Li or ^{10}Be. The fruits of such basic research could be harvested in 10 to 20 years time.
2. The area "Information security – Secure communication" encompasses several technology areas. Some of these could well benefit from research in technologies that are emerging just now. This includes object-based security and technologies like homomorphic encryption.[37]

Additional Critical Dependencies, e.g. the ones on the reserve list (Table 9), might also be overcome through research in Emerging Technologies. Nevertheless, no in-depth studies on these items could be conducted within the scope of the ETCETERA project due to time and budget constraints.

[37] See sections 3.1 and 3.2.

5 Recommendations for an Emerging Security Technology Research Agenda (ESTRA)

5.1 Recommendations concerning methodology

In the course of the ETCETERA project a number of methods were applied to identify and prioritise Emerging Technologies with security implications:[38]

- Desktop research
- Direct consultations with external experts
- Scientometrics (e.g. bibliometry and patentometry)
- A Weighted-Bit Assessment Method to aggregate expert opinion
- 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 expert (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.

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

[38] Additional methods, e.g. the Weighted-Bit Assessment Table for Critical Dependencies (WBAT-CD), were applied in parts of the ETCETERA projects not directly connected to the assessment of Emerging Technologies.

results. Assessing technology maturity proved to be exceptionally 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.

Recommendation 5: Weighted-Bit Assessment Methods should be used if information of different kinds and sources shall 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 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 7: 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 advantage 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 8: 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 were not sufficiently appreciated in the consecutive work. Nevertheless, the preparation of the game, especially the creation of the Idea-of-System cards, implied great effort.

Recommendation 9: 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.

Recommendation 10: 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 11: A scenario process should be conducted if broad stakeholder involvement is sought and transparency is a key requirement.

Recommendation 12: A scenario workshop is especially apt to assessing one specific technology or technology area, as dealing with diverse technologies might overstrain participants.

Online surveys were only used at selected point 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 13: Open online surveys should be used if information on simple matters shall be collected.

Recommendation 14: If complex information is to be collected through online surveys, invitations to participate need to be very targeted.

5.2 Recommendations concerning technologies

While the process described above delivered a wealth of information concerning methodologies for research planning, the results concerning concrete technologies seem to be somewhat arbitrary.

On the one hand, a large set of results was obtained from the process of Emerging Technology identification (section 3.1). 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.[13] 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 (section 3.3). 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.[22] 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.[25] In these cases broad stakeholder involvement was traded off with technological limitations.

Bearing these reservations in mind, some priorisation can be deduced from the SETAG (section 3.4) and the scenario process (section 3.5). 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 (section 3.6):

1. Homomorphic Encryption
2. Small-scale Energy Harvesting
3. Indoor Navigation
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 seems to be too far-fetched.

5.3 Recommendations concerning ethical and fundamental rights issues

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 a 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.[39]

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.[40]

Nine recommendations for making emerging security technologies consistent with the CFREU:

1. Respect for human dignity should be the leading principle followed in the development and employment of emerging security technologies.
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.
3. Emerging security technologies should – if possible and applicable – enforce the right to privacy and to data protection by design.
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.

[39] 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
[40] 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

5. Emerging security technologies should be designed and potentially employed to safeguard the individuals' rights to have ensured a high level of human health.
6. Emerging security technologies should be designed and potentially employed to ensure a high level of environmental protection.
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".
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.
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.

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.
2. Support and enforce democratic oversight and transparency of programmes aimed at developing and employing emerging security technologies.
3. Promote ethical, societal, and fundamental rights impact assessments both at R&D stage and after emerging security technologies have been adopted.
4. Promote and sustain a fundamental rights "by design" approach to the development of emerging security technologies.
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.
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.
7. Promote information and communication campaigns on policies and initiatives on emerging security technologies, and their implications.
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 ethical standards.

6 The Way Forward

The results of the ETCETERA project concerning Emerging Technologies presented in this report highlight several ways towards designing an Emerging Security Technology Research Agenda (ESTRA). They provide a toolbox of diverse methods for research planning which have been discussed concerning their respective advantages and downsides. This toolbox now 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.

All in all, the ETCETERA project has contributed to the development of innovative methods for research planning. At the same time it has identified limitations, especially when dealing with large sets of technology options.

7 Acknowledgements

We would like to acknowledge the intensive work done by the leaders of Work Packages 1, 2, 3, 4, and 5, without whom the results presented here would not have been possible:

- Steven J. Savage of FOI,
- F. Javier Herrera Lotero of Tecnalia, and
- Guido Huppertz of Fraunhofer INT.

Beatrix Wepner led the bibliometric and patentometric analyses of Emerging Technologies at the Austrian Institute of Technologies.

Apart from the persons mentioned above, the following scientists have contributed to the in-depth analyses of Emerging Technologies:

- Anna Pohl, Britta Levin, and Malek Khan of FOI,
- Nieves Murillo and Fernando Seco of Tecnalia,
- Dominique Noguet, Géraud Canet of CEA,
- Jesús López Pino of Isdefe,
- Stéphane Revelin of Morpho, and
- Klaus Ruhlig of Fraunhofer INT.

Apart from these, Riitta Räty and Camilla Trané (both of FOI) have contributed to the analysis of Critical Dependencies and how these could be overcome.

The 2nd Consultation Campaign would not have been possible without the teams that developed, conducted and evaluated the workshops. In the case of SETAG these persons are:

- Sam Besselink, Marcel-Paul Hasberg, Clara Peters, and Peter Petiet of TNO, and
- Jesús López Pino and Patricia López Vicente of Isdefe.

The scenario process was conducted by:

- Antje Bierwisch, Victoria Kayser, Erduana Shala, Ewa Dönitz, and Stephan Grandt of Fraunhofer ISI.

We wish to thank Matteo Bonfanti of CSSC for valuable input on ethical and human rights issues at various point of the project.

Last but not least, the contributions of Antonia Bierwirth of Tecnalia and of Stefanie Goymann of Fraunhofer INT to this project have been manifold and are gratefully acknowledged.