FP7 Project ETCETERA - Evaluation of critical and emerging technologies for the elaboration of a security research agenda

Joachim Burbiel, Fraunhofer INT, Germany
Stefanie Goymann, Fraunhofer INT, Germany
Steven Savage, FOI, Sweden
Javier Herrera Lotero, Tecnalia, Spain

Abstract

The ETCETERA project is a contribution to effective and efficient security research planning on a European level. Its aim is three-fold:
1. to develop novel methodologies for future strategic research planning,
2. to identify risks and potential benefits associated with Critical Dependencies and Emerging Technologies with security implications, and
3. to recommend research plans to deal with these risks and potential benefits.

1 Introduction

1.1 Background

"Evaluation of critical and emerging technologies for the elaboration of a security research agenda" (ETCETERA) is the name of a project addressing Topic SEC-2010.7.0-3 "Critical and emerging technologies for security" within the security theme of the 7th Framework Programme. The topic asked for:
1. Identification of technology areas needed for security purposes, specifically those where European industry is dependent from other world regions for these technologies. Alternative technological solutions are then to be sought to allow European produced security equipment to be used / sold / deployed worldwide.
2. Identification of topics within the Emerging Technologies of the future (10-20 years ahead), which are suitable to set out high risk, high pay-off research priorities. The study should

- provide an in-depth analysis of different emerging technology areas,
- identify issues relevant to civil security research, and
- outline recommendations for future research priorities.

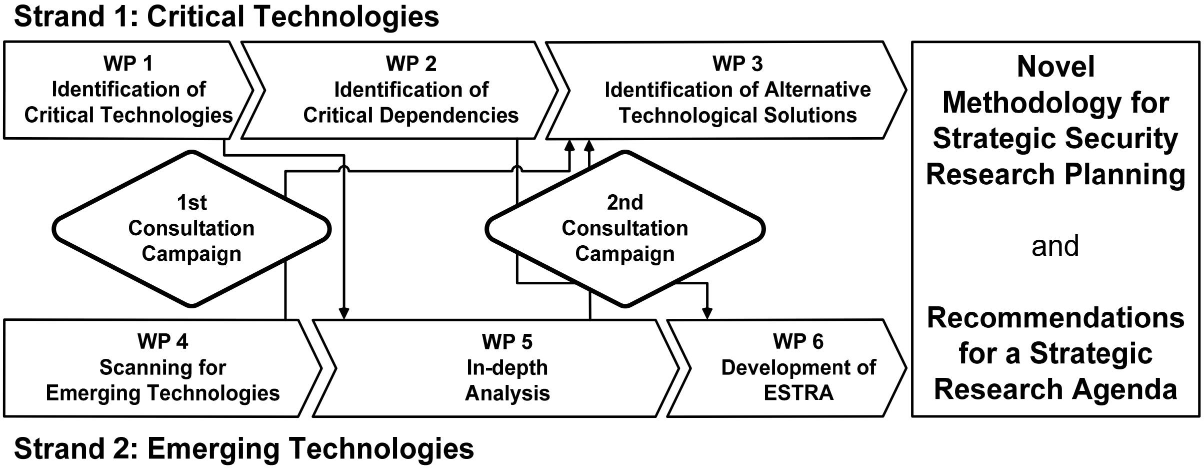

Strand 1: Critical Technologies
WP 1 Identification of Critical Technologies
WP 2 Identification of Critical Dependencies
WP 3 Identification of Alternative Technological Solutions
1st Consultation Campaign
2nd Consultation Campaign
WP 4 Scanning for Emerging Technologies
WP 5 In-depth Analysis
WP 6 Development of ESTRA
Novel Methodology for Strategic Security Research Planning
and
Recommendations for a Strategic Research Agenda
Strand 2: Emerging Technologies

Figure 1 General structure of the project

1.2 Concept

The ETCETERA project takes up the two-fold structure of the topic by dealing with the issues “Critical Technologies” and “Emerging Technologies” in two separate but interrelated research strands (see **Figure 1**). Each strand is further divided into three work packages (WP) that will be carried through in a sequential manner. A further work package deals with project management (WP 7). Two Consultation Campaigns will generate input from technical experts, end-users, and public authorities for both strands.

1.3 Goals

The ETCETERA project is a contribution to effective and efficient security research planning on a European level. Its aim is three-fold:
1. to develop novel methodologies for future strategic research planning (e.g. through synthesis of known methods in WP 4),
2. to identify risks and potential benefits associated with Critical Dependencies and Emerging Technologies with security implications (WP 2 and WP 5), and
3. to recommend a research agenda to deal with these risks and potential benefits (WP 3 and WP 6).

As an example for the development of new methodologies, an approach, similar to the scenario technique, but involving the use of a specifically designed Weighted-bit Assessment Table (WBAM) will be applied in Strand 1 “Critical Technologies” and the 2nd Consultation Campaign. Such a system does not exist yet as an evaluation tool for Critical and Emerging Technologies and thus constitutes a relevant innovation in research planning. Furthermore, the military DTAG method will be adapted to civil security settings. Both methods are aimed to provide a platform for efficient communication between stakeholders of various backgrounds.

Among the methods applied for generating research recommendations, a novel methodology for economical assessment of high risk/high pay-off technologies deserves special notice. It is to be developed by a group of academic and research & technology organisation (RTO) researchers with involvement of industrial specialists that work together for the first time as members of the ETCETERA consortium.

1.4 State of the art

Thematic planning efforts concerning 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 area of the 7th Framework Programme were laid. From September 2007 to September 2009 an even larger programme, the European Security Research and Innovation Forum (ESRIF), aimed at devising a medium- to long-term strategy for European security research.

While these actions were conducted directly by the European Commission (EC), 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), that 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. The Coordination action on Risks, Evolution of threatS and Context assessment by an Enlarged Network for an r&D rOadmap (CRESCENDO) project was granted as part of the first security research call (Work Programme 2008) and ran from July 2009 to July 2011. Its aim was to collate information from a diversity of expert sources into R&D-roadmaps.

The Security Technology Active Watch (STRAW) project was initiated in October 2008. The aim of this project is to collect information from a variety of stakeholders and to transfer it to the public at large, public authorities, and the research community. While STRAW focussed on the positive aspects of new technologies, Foresight of Evolving Security Threats Posed by Emerging Technologies (FESTOS), which runs from March 2009 to October 2011 looks a their “dark” sides. The results of these projects will be taken into consideration when the ETCETERA project is implemented.

Of course, scanning technologies for security implications is not a purely European effort. As an example, the US Department of Homeland Security features a Science & Technology Directorate. Its mission is to improve homeland security by providing to customers state-of-the-art technology that helps them achieve their missions. It has established a Science and Technology Transition Program to define major research and development needs. Furthermore, the Homeland Security Advanced Research Projects Agency (HSARPA) was established in 2002 to foster the development and adaption of new technologies for security applications.

The security implications of new technologies are of concern to military actors, too. One of the international efforts to deal with Disruptive Technologies is the Disruptive Technologies Assessment Game

(DTAG) conducted by NATO-RTO. Several RTOs of the ETCETERA consortium are involved in this activity, and an approach to adapt this method with a military background to civil security settings is part of the ETCETERA project.

1.5 Consortium partners

The ETCETERA project will be carried out by a consortium of 14 partners from seven European countries. A core group is constituted by the Fraunhofer Society, FOI and Tecnalia. Further research and technology organisations (RTO) of the consortium are Isdefe, AIT, CEA, TNO, VDI-TZ, and CSSC. This group of RTO is complemented by two industrial partners (Morpho and Ansaldo STS), a university (UDE) and two end-user organisations (SSBF and ComSec).

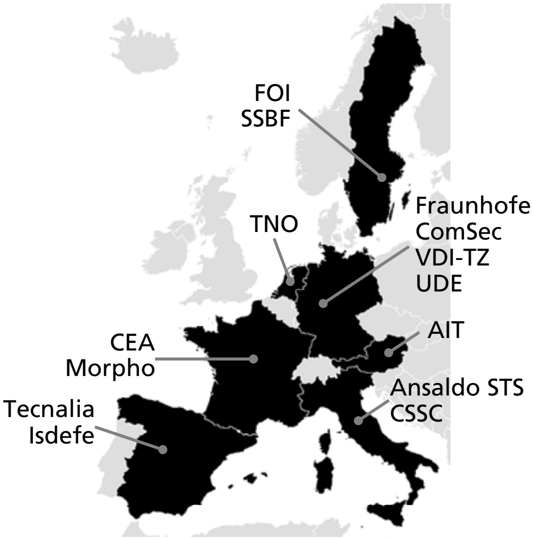


Figure 2 Location of consortium parties

2 Description of Work

2.1 Strand 1: Critical Technologies

The first research strand (Work Packages 1 to 3) can be envisaged as a collating and analysis exercise (see **Figure 3**).

Starting from all possible technologies, all technologies indispensible for European security now and in the near future will be identified in Work Package 1. This will be achieved through extensive consultations within the consortium and with external experts. The list thus obtained will be validated through an iterative mechanism.

In the second work package (WP 2), the validated list of Critical Technologies will be analysed for Critical Dependencies. Critical Dependencies arise if European industry is not non-dependent in providing critical technologies/systems/capabilities to end-users. Those dependencies could be caused by extra-European intellectual property rights (IPR), trade and academic restrictions, restrictions due to high classification in dual-use technologies, and economic challenges (e.g. shifting production sites, lack of specialisation in EU industry, deficient research orientation, hindering or underdeveloped norms and standards, failing business models).

The last work package of Strand 1 (WP 3) will propose and prioritise alternative solutions to alleviate the Critical Dependencies identified. In the case of solutions of technological nature, implementation measures, including appropriate research agendas, will be developed.

Strand 1 is associated with the 1st Consultation Campaign which includes five parallel workshops held at five locations and in six languages. The use of local languages is an effort to incorporate the diversity of European working practices by removing language barriers.

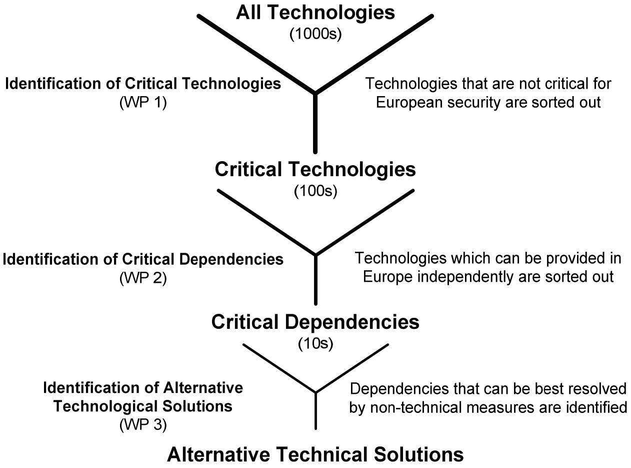

All Technologies
(1000s)
Identification of Critical Technologies
(WP 1)
Technologies that are not critical for European security are sorted out
Critical Technologies
(100s)
Identification of Critical Dependencies
(WP 2)
Technologies which can be provided in Europe independently are sorted out
Critical Dependencies
(10s)
Identification of Alternative Technological Solutions
(WP 3)
Dependencies that can be best resolved by non-technical measures are identified
Alternative Technical Solutions

Figure 3 Outline of Strand 1 “Critical Technologies”

2.2 Strand 2: Emerging Technologies

In the first work package of Strand 2 (WP 4), Emerging Technologies will be scanned for their security implications in 10 to 20 years time. These implications might have the form of high risk/high pay-off opportunities, but also of future threats. Three scanning methods will be performed in a parallel fashion:

- AIT will use bibliometric methods for the survey. A broad range of sources will be electronically exploited to identify relevant information using AIT's BibTechMon approach.
- Fraunhofer INT will exploit its broad technological knowledge base which will be supplemented by additional analyses of relevant studies and expert interviews.
- Isdefe will apply its proprietary systematic approach to prepare a further independent list of Emerging Technologies with security implications.

A comparative analysis of the results of these three methods will then be performed, leading to the explorative task of developing a novel method for this kind of technology scanning.

Emerging Technologies identified to be most relevant will be further analysed in the second work package of this strand (WP 5). These in-depth analyses will mainly be carried out by experts of consortium members, with external specialists engaged for highly specific input. Furthermore, it is endeavoured to adapt the originally military Disruptive Technology Assessment Game (DTAG) to civil scenarios and to set up an evaluative scenario workshop (2nd Consultation Campaign).

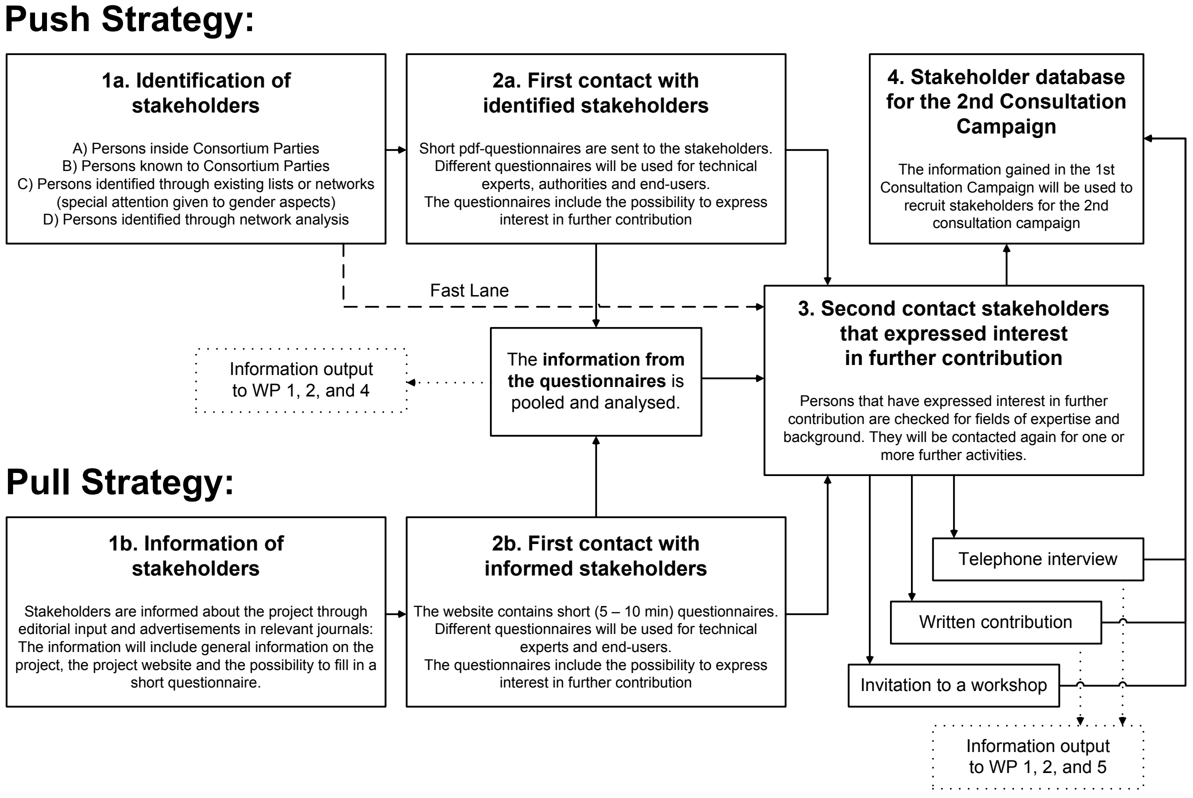
In the last work package of the strand (WP 6) all results on Emerging Technologies will be considered when developing recommendations for an Emerging Security Technology Research Agenda (ESTRA). Measures will be taken to ensure that ESTRA is compatible with existing national and European research strategies. Ethical aspects will also be taken into account.

2.3 Stakeholder recruitment strategy

The 1st Consultation Campaign includes a double stranded, multi-level strategy for the recruitment of stakeholders (technical experts, industrial suppliers, end-users and public authorities; see **Figure 4**):

- The "push" strategy takes advantage of the knowledge already available at the Consortium Parties, information available from previous security R&D activities (both by Consortium Parties and other research organisations), and information gained through network analysis methods. Especially the Research and Technology Organisations (RTO) in the consortium can draw from a large pool of technical experts, which ensures that a sufficient number of experts can be recruited by the "push" strategy. A "Fast Lane" allows inclusion of experts identified by these measures for further consultation without going through the questionnaire step.
- The complementary "pull" strategy is a very open approach, using advertising in journals and over professional organisations, and an open internet platform that might well attract technical experts and end-users that would not be reached by research efforts of the European Union by other means. Furthermore, the advertising campaign can be seen as the basis of broad dissemination of information about the ETCETERA project. On the other side, it is associated with the risk that not enough qualified stakeholders can be recruited.

The combination of "push" and "pull" strategies will deliver a well balanced approach to input from many stakeholders. Some possibilities for stakeholders to get involved are: Approaching consortium parties for inclusion in the “push” strategy, filling out the online questionnaires, and registering with the website. For further information about opportunities for joining the process, please check the project website at http://www.etcetera-project.eu/


Push Strategy:
1a. Identification of stakeholders
2a. First contact with identified stakeholders
4. Stakeholder database for the 2nd Consultation Campaign
Fast Lane
Information output to WP 1, 2, and 4
The information from the questionnaires is pooled and analysed.
3. Second contact stakeholders that expressed interest in further contribution
Pull Strategy:
1b. Information of stakeholders
2b. First contact with informed stakeholders
Telephone interview
Written contribution
Invitation to a workshop
Information output to WP 1, 2, and 5

A) Persons inside Consortium Parties
B) Persons known to Consortium Parties
C) Persons identified through existing lists or networks (special attention given to gender aspects)
D) Persons identified through network analysis

Short pdf-questionnaires are sent to the stakeholders. Different questionnaires will be used for technical experts, authorities and end-users. The questionnaires include the possibility to express interest in further contribution

The information gained in the 1st Consultation Campaign will be used to recruit stakeholders for the 2nd consultation campaign

Persons that have expressed interest in further contribution are checked for fields of expertise and background. They will be contacted again for one or more further activities.

Stakeholders are informed about the project through editorial input and advertisements in relevant journals: The information will include general information on the project, the project website and the possibility to fill in a short questionnaire.

The website contains short (5 – 10 min) questionnaires. Different questionnaires will be used for technical experts and end-users. The questionnaires include the possibility to express interest in further contribution

Figure 4 Stakeholder recruitment strategy

3 Expected Impact

The expected impacts given in the topic addressed are:
"1. A list of critical technologies and a plan to deal with these to allow 'non-dependence' for Europe and
2. a list of emerging technologies and a plan to deal with these to set out high risk, high pay-off research priorities."
In the ETCETERA project the list of critical technologies will be developed in WP 1, while the plan to deal with gaps identified is dealt with in WP 3. The requested list of emerging technologies is created in WP 4 and the plan concerning research opportunities is prepared in WP 6. The high risk/high pay-off aspect is contributed in a quantitative manner.
Other goals given for Activity 10.7 "Security research coordination and structuring" are
• "to utilise limited resources in an effective and efficient manner",
• to "indicate opportunities and constraints for developing and strengthening a European security related market",
• to "contribute to the overall impact of the Security theme by making it more effective and efficient", and
• to "contribute to the design of future Work Programmes of the Security theme."
The ETCETERA project addresses these issues, both by the lists and plans described above, and the methodological progress expected as a result of the work proposed:
• By combining and adapting several known methods for the identification of Critical Technologies (WP 1), Critical Dependencies (WP 2), and alternative technological solution (WP 3) two goals will be achieved: opportunities and constraints for developing and strengthening a European security related market will be identified (e.g. by pointing out technologies to be exploited, or by identifying sectors were market failure is imminent), and a contribution to future Work Programmes will be made (e.g. by pointing out areas were applied research will give desirable results concerning European competitiveness).
• Within Strand 1 "Critical Technologies" the Weighted Bit Assessment Method (WBAM) is adapted to technology planning. This will give a novel method both for organising planning results in a coherent way, and for discussing these results with stakeholders from diverse backgrounds.
• The thorough analysis of the economic, legal and IPR environment of Critical Technologies performed in WP 2 will be fundamental for future planning efforts concerning the building of a competitive European security market.
• In WP 4 an effort is made to develop a truly novel method for the identification of security implications of Emerging Technologies. This effort consists of the parallel execution of three very different methods for technology assessment, a comparative analysis of the methods, and the development of novel ideas. It is expected that significant methodological advance will be made, which will benefit the design of future Work Programmes of the Security theme.
• The in-depth analysis of selected Emerging Technology fields (WP 5) will contribute to the design of future Work Programmes of the Security theme by assessing research opportunities for technologies with a time horizon of 10 - 20 years time.
• This positive impact on future Work Programmes is enhanced by the very comprehensive integration of factors performed in WP 6. The recommendations for an Emerging Security Technology Research Agenda (ESTRA) will be a significant input for future research efforts concerning basic research that will lead to truly innovative security technologies in the middle future.
• The production of an overview of national security research programmes in Europe (WP 6) will also be beneficial to future research planning of the EU.
• Research on the ethical impact of future security technologies will accompany all planning efforts within ETCETERA (WP 3, 5, and 6).
• The economic method to be developed for the economical assessment of high risk/high pay-off technologies (task 6.3) will be adjuvant for distributing limited resources in an effective and efficient manner.

The Final Report will sum up these efforts and results.

References

[1] AeroSpace and Defence Industries Association of Europe/ PASR (2008): STACCATO Final Taxonomy. http://www.asd-eurpe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf, last updated 06.09.2008

[2] ESRIF (2009): ESRIF Final Report (WEB). I527-290. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf, last updated 09.12.2009