

COMPARATIVE ANALYSIS OF METHODS FOR STRATEGIC SECURITY RESEARCH PLANNING

Joachim Burbiel and Ruth Schietke

etcetera@int.fraunhofer.de

Fraunhofer Institute for Technological Trend Analysis INT,
Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Within the FP7-supported project “Evaluation of critical and emerging technologies for the elaboration of a security research agenda” (ETCETERA, Oct. 2011 to Nov. 2013), technologies that are critical for security functions in Europe were checked for dependencies on extra-European sources. Furthermore, technologies that are now just emerging and will reach maturity in 10 to 15 years were assessed concerning their relevance for European security. In order to achieve these goals, a plethora of methods was employed, including desktop research, scientometrics (e.g., bibliometrics and patentometrics), a Weighted-Bit Assessment Method to aggregate expert opinion, an adapted TEPID-OIL filtering methodology (ITIPOLITRE), parallel workshops applying the World Café method, a dedicated Security Emerging Technology Assessment Game (SETAG) and a complex scenario process. Some of these methods have been specifically developed for the ETCETERA project and/or applied in the context of security research planning for the first time. A comparative analysis of the methods applied was performed, and recommendations for their employment in security research planning were made. This will facilitate better choices concerning methodology in future planning efforts.

Keywords: Research planning, methodology, bibliometrics, scientometrics, scenario process, serious gaming, workshop organization.

1 BACKGROUND

Planning in European security research is traditionally based on a combination of stakeholder consultations organized by the European Commission (e.g., the European Security Research Advisory Board (ESRAB, 2005–06) and the European Security Research and Innovation Forum (ESRIF, 2007–09)) and research projects that contributed additional views to these processes (e.g., “Security Network for Technological Research in Europe” (SeNTRE, 2004–06), “Stakeholders platform for supply chain mapping, market condition analysis and technologies opportunities” (STACCATO, 2007–08) and “Coordination action on risks, evolution of threats and context assessment by an enlarged network for an r&d roadmap” (CRESCENDO, 2009–11).

The FP7-supported project “Evaluation of critical and emerging technologies for the elaboration of a security research agenda” (ETCETERA, Oct. 2011 to Nov. 2013) stands in the tradition of such research projects. Responding to a specific research call, it encompassed two kinds of technology evaluation for research planning:

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

To address these two temporally separated issues, the project was divided into two research strands (Fig. 1). Research agendas were proposed to overcome critical dependencies in the near future and to capitalize on the opportunities offered by emerging technologies. Furthermore, new methodologies were developed and applied. These activities were closely accompanied by work on ethical aspects, as decisions about research funding should take into consideration all possible implications of novel technologies on society [1].

This paper focusses on the methodological findings of the project and presents recommendations concerning the application of the methods applied in (security) research planning.

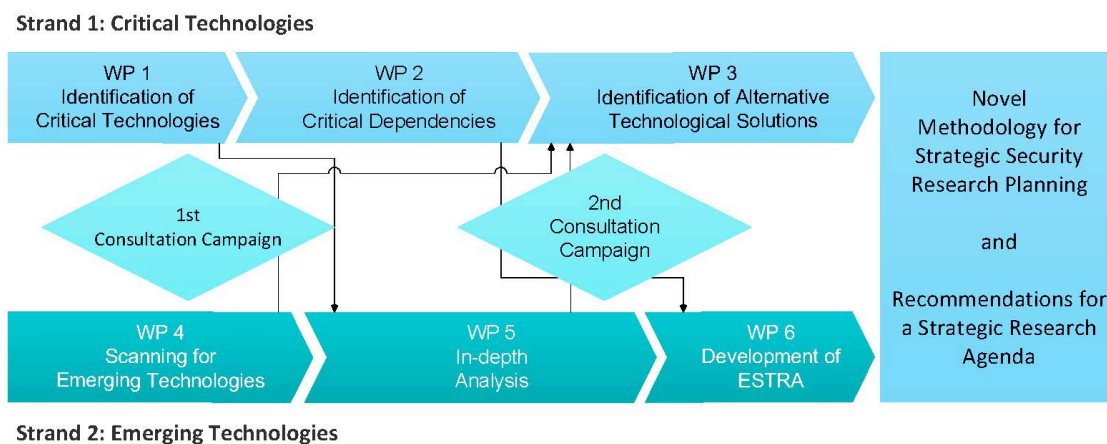


Figure 1: Workflow of the ETCETERA project.

2 METHODOLOGICAL FINDINGS AND RECOMMENDATIONS

In the course of the ETCETERA project, a plethora of methods were applied to identify and prioritize Critical and Emerging Technologies with security implications:

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

In the following, the findings and recommendations concerning these methods are outlined:

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 [2]. 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 future technologies. Nevertheless, they need to be supplemented with participative methods to get a solid basis for political decision making.

Direct consultations with external experts (e.g., through interviews or by asking for written input) can broaden and consolidate the results gained by in-house desktop research. They require a network of experts that can be involved on a case by case basis. While setting up such a network might be time-consuming, it allows high flexibility when responding to specific requests [2].

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 ETCETERA project: as a method to identify Emerging Technologies (mainly bibliometrics, [2]) and for the assessment of Critical Dependencies (patentometrics, [3]). 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 useful for the completion of the task. Assessing technology maturity proved to be very difficult with scientometrics.

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

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

Weighted-Bit Assessment Methods (WBAM) represent knowledge as a set of yes/no answers to carefully designed questions. If the items to be analyzed are listed vertically and the questions horizontally, a matrix of evaluative answers is formed. These answers can be weighted according to their relevance for certain applications to give “scores” that provide a basis for the discussion of prioritizations [4]. In the ETCETERA project, Weighted-Bit Assessment Methods were used at two points to aggregate expert opinion: for prioritizing Emerging Technologies for further analysis and for aggregating all information available about Critical Dependencies [5]. In both cases, this relatively simple method proved to be very useful.

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

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

The TEPID-OIL method was originally developed for analysis of military alternatives [6]. In order for the method to be applicable to the broader requirements of the development of alternatives in a civilian context, the method was modified and extended to include incitement/psychology and economy/markets, hence becoming **ITIPOLITRE** [7]. The dimensions of the assessment of ITIPOLITRE are:

- Incitements/psychology – Why is there a threat? Can the causes be addressed?
- Technology/equipment – equipment and technology needed to perform some action
- Information/information systems – information or information systems that can help in solving a task or mission
- Personnel – number, capacity and competence of personnel

- Organization – partners/actors that are involved in completing the task and how they interact
- Logistics – providing the people, personnel and goods needed to perform a task
- Infrastructure facilities – buildings, structures, land etc.
- Training/education – knowledge, training and development of personnel and others
- Rules – laws and regulations
- Economy – finance, economy and market mechanisms

The applicability of the improved method was demonstrated by searching for alternatives to X-ray technologies applied in airport security as the starting point.

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

The goal of conducting “**parallel workshops**” in different languages at different places, but using the same methodology, 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 five workshops, many of whom had not been involved in European security research before. End-users, representatives of industry, and scientists were equally represented [8]. On the other hand, the effort of organizing five “parallel workshops” was significantly higher than for organizing just one “central workshop”, even though the methodology was only prepared once.

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

The **World Café method** is based on free discussion in small and changing groups [9]. Participants are encouraged to document their thoughts by writing and sketching on large pieces of paper placed on group tables [8]. Three main advantages of this method were identified:

- All participants have a chance to share their views and ideas, which is sometimes difficult in large “conventional” workshops.
- The World Café method is easily scalable: In the ETCETERA project, it was applied to groups of 15 to 20 persons, but it can also be carried out with significantly 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, which applied this method, to the pre-determined workflow of the two strands of the ETCETERA project.

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

A **Security Emerging Technology Assessment Game (SETAG)** was developed based on the military Disruptive Technology Assessment Game (DTAG) [10, 11]. Profound changes had to be introduced, e.g., the “red force vs. blue force” approach was replaced by a cooperative approach more suitable for civil security actors. SETAG

proved to be a valuable tool for technology assessment. It was considered interesting by the end-users involved. It was possible to feed some results back into the main work stream of the project, but some valuable observations could not be sufficiently integrated in consecutive work. Nevertheless, the preparation of the game, especially the creation of the Idea-of-System cards, implied great effort, and solid foundations for further development were laid [12].

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

The complex **scenario process** [13] 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 [14]. 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 labor-intensive.

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

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

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

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

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

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

3 ALIGNMENT OF METHODS AND PURPOSES

It is obvious that the choice of methods to be used depends on the purposes to be achieved. Tab. 1 gives an overview of how well the methods applied within the ETCETERA project align with different aspects in research planning [1]. Four groups of purposes have been evaluated:

Generation of data and/or ideas:

- Quick and easy generation of tentative results without much preparative efforts
- Development of novel ideas, e.g., through stimulation of creativity
- Inclusion of relevant stakeholder expertise, scaled to the size of the effort

Evaluation/priorization:

- Holistic assessment by looking at one item from a multitude of perspectives
- Identification of complex dependencies
- Priorization of options
- Organizing (complex) data and presenting it in an easily understandable format

Validation of results:

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

Other:

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

The correlation of this large number and variety of methods used within the ETCETERA project with elements of (security) research planning may be used to support the decision process of which method is best suited for a certain phase or task.

Overall, the ETCETERA project has thus provided valuable information on the organization of security research processes.

METHOD		Scenarios	SETAG	ITIPOLITRE	WBAM	Targeted Online Survey	Parallel Workshops	World Café Method	Round Table discussions	Assessment by In-house Experts	Scientometrics
		PURPOSE									
Generation of Data and/or Ideas	Quick & Easy Generation of Tentative Results					Dark Green		Light Green	Light Green	Light Green	Light Green
	Development of Novel Ideas	Light Green	Light Green	Light Green			Light Green	Light Green	Light Green	Light Green	
	Inclusion of Relevant Stakeholder Expertise	Dark Green	Dark Green	Dark Green	Light Green	Dark Green	Dark Green	Dark Green	Dark Green		
Evaluation / Priorisation	Holistic Assessment	Dark Green	Light Green	Dark Green	Dark Green		Light Green		Light Green	Light Green	
	Identification of complex dependencies	Dark Green		Dark Green	Light Green		Light Green	Light Green		Light Green	Light Green
	Priorisation of Options	Light Green	Light Green	Dark Green	Dark Green	Light Green	Light Green	Light Green	Light Green	Dark Green	Light Green
	Organising Data			Light Green	Dark Green					Light Green	Dark Green
Validation of Results	Assuring Completeness			Dark Green	Light Green	Light Green	Light Green		Light Green	Light Green	Dark Green
	Reality-Check regarding Technological Feasibility			Dark Green	Light Green	Light Green	Light Green		Light Green	Light Green	
	Reality-Check Regarding Capability Gaps	Light Green	Dark Green	Dark Green	Light Green	Light Green	Light Green	Dark Green	Dark Green	Light Green	
Other	Dissemination Effect	Dark Green	Dark Green	Light Green	Light Green	Light Green	Dark Green	Dark Green	Light Green		
	Fun Factor / Stakeholder Motivation	Light Green	Dark Green	Light Green	Light Green		Dark Green	Dark Green	Light Green		
	Awareness Rising and Active Engagement of Stakeholders	Dark Green	Dark Green	Light Green	Light Green		Dark Green	Dark Green	Light Green		
Effort	Time	Dark Blue	Dark Blue	Light Blue	Light Blue	Light Blue	Light Blue	Light Blue	Light Blue	Dark Blue	Light Blue
	Costs	Light Blue	Light Blue	Light Blue	Light Blue	Light Blue	Dark Blue	Light Blue	Light Blue	Light Blue	Light Blue

Table 1: Alignment of methods and purposes. Dark green fields indicate that a method is well-suited for a purpose, light green fields indicate that a method is partially suited for a purpose. Time and cost are assessed as low (light blue), medium (blue), and high (dark blue).

4 ACKNOWLEDGEMENTS

The work of the ETCETERA project was performed by the following partners: Fraunhofer INT (Coordinator; and Fraunhofer ISI, DE), Swedish Defence Research Agency (FOI, SE), Tecnalia (ES), Ingeniería de Sistemas para la Defensa de España (Isdefe, ES), Universität Duisburg-Essen (DE), Austrian Institute of Technology (AIT, AT), Commissariat à l'énergie atomique et aux énergies alternatives (CEA, FR), Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO, NL), VDI Technologiezentrum (vdi-tz, DE), Morpho (FR), Ansaldo STS (IT), COMSEC (DE), Centro per la Scienza la Società a la Cittadinanza (CSSC, IT), Greater Stockholm Fire Brigade (SSBF, SE).

The research leading to the results presented has received funding from the European Union Seventh Framework Programme under grant agreement n° 261512.

REFERENCES

All deliverables can be downloaded from the ETCETERA website:
www.etcetera-project.eu

- [1] Joachim Burbiel, Ruth Schietke (Fraunhofer INT), “Final Report”, ETCETERA Deliverable 7.2, November 2013.
- [2] 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.
- [3] Beatrix Wepner, Manuela Kienegger, Georg Zahradnik (AIT), “Report of the Analysis of the Regional Distribution of Patents”, ETCETERA Working Document 2.2, May 2013.
- [4] Joachim Burbiel, Norbert Engelhard, Sonja Grigoleit, Harald John, Joachim Schulze, “Gefahrenpotentiale von chemischen Kampfstoffen und toxischen Industriechemikalien – das Punktesystem”, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe -BBK-, Bonn: Gefahren und Warnung – Drei Beiträge. Rheinbreitbach: MedienHaus Plump, 2009, pp. 27–58.
- [5] Joachim Burbiel (Fraunhofer INT), “Report on the Adaption of the Weighted-Bit Assessment Method”, ETCETERA Working Document 2.8, May 2013.
- [6] Clive Kerr, Robert Phaal, David Probert, “A Framework for Strategic Military Capabilities in Defense Transformation”, Proceedings of the 11th International Command and Control Research and Technology Symposium, Cambridge 2006.
- [7] Riitta Rätty (FOI), Camilla Trané (FOI), Malek Khan (FOI), Steven Savage (FOI), “ITIPOLITRE – A Method to Identify a Wide Range of Alternative Security Technologies”, ETCETERA Working Document 3.1, October 2013.
- [8] Malek Khan, Steven Savage (FOI), “Documentation of Methods and Workshops”, ETCETERA Deliverable 1.3, October 2012.
- [9] Juanita Brown, David Isaacs, “The World Café. Shaping Our Futures Through Conversations That Matter”, San Francisco, 2005.
- [10] “Assessment of Possible Disruptive Technologies for Defence and Security”, Final Report of Task Group 062, NATO Science and Technology Organization, RTO-TR-SAS-062 AC/323(SAS-062)TP/258, February 2010
- [11] “Disruptive Technology Assessment Game – Evolution and Validation”, Final Report of Task Group 082, NATO Science and Technology Organization, RTO-TR-SAS-082 AC/323(SAS-082)TP/427, April 2012
- [12] 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.
- [13] Falko E.P. Wilms, “Szenarien sind Systeme”. In: Wilms, Falko E.P. (Ed.): Szenariotechnik. Bern/Stuttgart/Wien 2006, pp. 39–60.
- [14] Antje Bierwisch, Victoria Kayser, Erduana Shala (Fraunhofer ISI), “Report on the Scenario Based Workshop”, ETCETERA Working Document 6.2, August 2013.