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 D1.3

Documentation of methods and workshops

Authors: Malek Khan (FOI), Steven Savage (FOI)

October 2012

Dissemination Level: PU

1 Introduction

This report documents the methods and processes used to generate the Critical Technology List (Deliverable 1.2).

Briefly, the process has been to search the open literature and analyse this from the point of view of security (drawing, where possible, a distinction between applications for security and applications for defence). The STACCATO[1] taxonomy was used as a starting point. A series of workshops was organised, using the world café method. Five workshops were organised, in Spain, Germany, Italy, Sweden and France. Each workshop was held in the national language, to enhance communication. Participants in the workshops were selected to represent end-users, companies, scientists and others. The intention was to create an atmosphere representing a typical cross-section of society, not necessarily conscious of security at all. An analysis of the output of these workshops is given below.

The Critical Technology List has been primarily developed by FOI and validated through exchange with and input from (mainly) Tecnalia, AIT and CEA. At several points additional literature searching has been done to verify (or deny) some point of security technology, using the definition below.

There is no commonly accepted definition of a "Critical Technology". The ETCETERA project has therefore created a definition using the project's online communication tool "Cowiki INT" as a discussion forum.

The ETCETERA Description of Work stated:
"A Critical Technology is broadly defined as a technology that is currently available or expected to be available in the near future and that is indispensible [sic] for European security"

However, this is not a workable definition, so following discussions a new and improved definition has been developed, viz:

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

While this definition is still not perfect and open to interpretation, it does include less tangible aspects such as skills, services and software. Hence any "technology" fulfilling the above definition is to be considered as a Critical Technology. In the final list (Deliverable 1.2) all such technologies have been included; even such ubiquitous technologies as for example cement production. In WP 2 each Critical Technology will be analysed to determine if a Critical Dependency exists. For a further "definition of dependency" we refer to Deliverable 2.1 "Intermediate Report on Critical Dependencies".

[1] STACCATO = Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities, an earlier PASR project

2 STACCATO taxonomy

The major advantage of the STACCATO taxonomy is its broadness. It includes a very wide range of technologies, and other less concrete topics such as capabilities and policy. The STACCATO[2] taxonomy is derived from the earlier (PASR) project SeNTRE[3] and was originally intended as a support to a "*Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities*" (sic). It was not therefore intended primarily as a list of security technologies, although it was created by ASD (Aerospace & Defence Industries of Europe). However in view of the broadness of the taxonomy it is a suitable starting point for the ETCETERA Critical Technology List (CTL). Alternative starting points considered (and rejected) include various "critical technology" documents from the USA and the UK. These were rejected as they were primarily directed towards technologies critical for defence, not security.
The structure of STACCATO is presented in the diagram below.

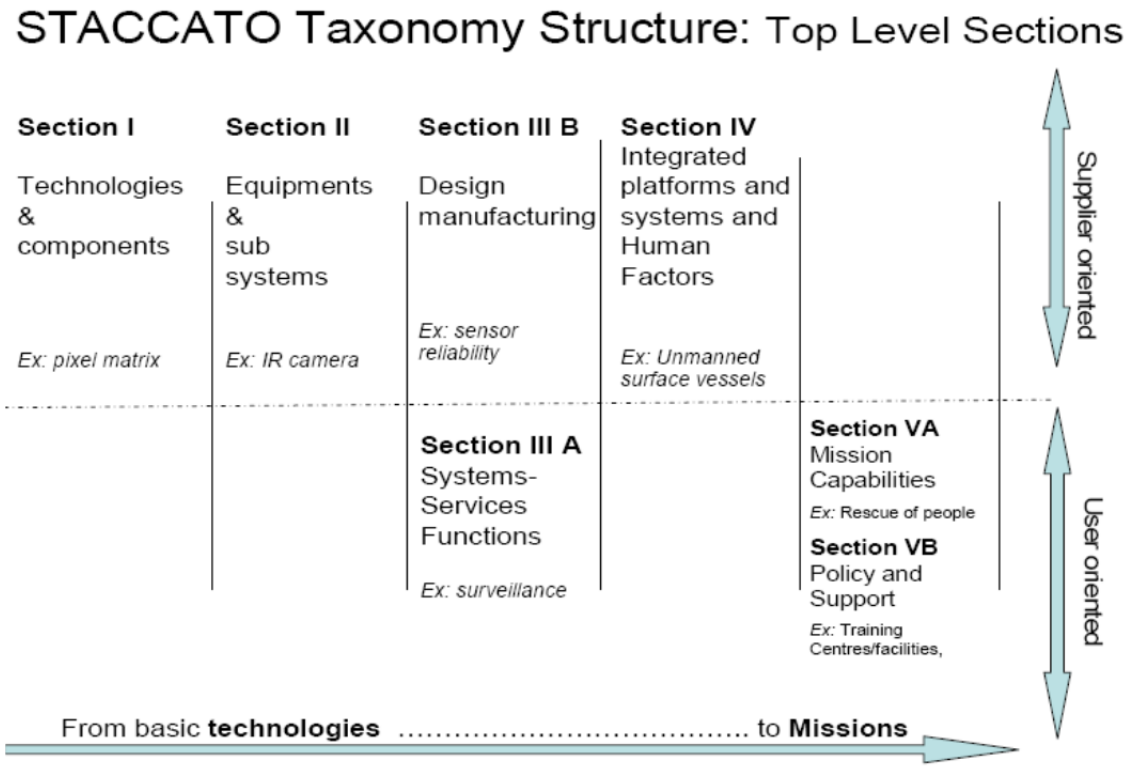

Figure 1. The STACCATO structure (STACCATO D1.2.2 January 2007)

[2] More information regarding STACCATO can be found here: http://sta.jrc.it/pdf/staccato.pdf, http://www.iai.it/pdf/Economia_difesa/STACCATO_Final-Report-Executive-Summary.pdf
[3] More information about SeNTRE can be found here: http://www.frstrategie.org/specifique/activitesEuropeennes/SeNTRE.pdf

A drawback of STACCATO is the overlap and duplication in several areas, for example: 100-3 *Composite materials technology* contains topics: 100-2 *Ceramic composites* and 100-6 *organic composites* and 100-8 *carbone-carbone (sic) composites* and 100-15 *metallic composites*. In this example it would be more logical to define the topic as:

- Composite materials technology including:
    - Ceramic matrix composites
    - Polymer matrix composites
    - Metal matrix composites
    - Carbon-carbon composites

Some topics are indirectly related to a threat, e.g. 104 – Survivability and hardening, but the actual threat is not specified, and is not a particularly useful approach as only a few threats are included. It would be better to relate the topics to the actual security technology, such as (in this case) protection against electromagnetic radiation. It would also be useful to specify what is to be protected. In the STACCATO list it can be assumed that infrastructure and electrical/electronic equipment is to be protected, but not humans, so the topic is incomplete.

In several cases the topic as listed is very vague, such as: 100-16 New concretes. How is new defined, and what are the (potential) applications? In a similar manner 121-1 Biological technologies is undefined, and needs to be qualified so as to relate to an application (or field of application), e.g. biological technologies for soil remediation.

STACCATO is a broad and non-prioritized taxonomy. It aims to include all technologies relevant to security, which is both a strength and a weakness. The STACCATO strength lies in its breadth, and its weakness in the lack of prioritization or context. In some ways STACCATO can be considered as unfinished work. In order to make STACCATO more useful for the ETCETERA-type of analysis the following improvement is suggested. STACCATO should be further analysed (or filtered) from the point of view of the user, where the following broad categories of users are suitable:

- First responders (emergency personnel, ambulance and paramedical personnel, firefighters, etc)
- Security personnel (including police, customs & excise, lifeguards, security guards, etc)
- Essential services, further subdivided into:
    - Water and sewage services
    - Electricity services
    - Transport infrastructure (road, rail, air, water)
    - Medical services (hospitals)
    - Communications (electronic, telephone network, TV, radio including the necessary infrastructure)

A possible method which could be applied for this filtering is illustrated in the figure below, derived from the EDTID project (Addressing key European Defence Technical and Industrial Dependences).

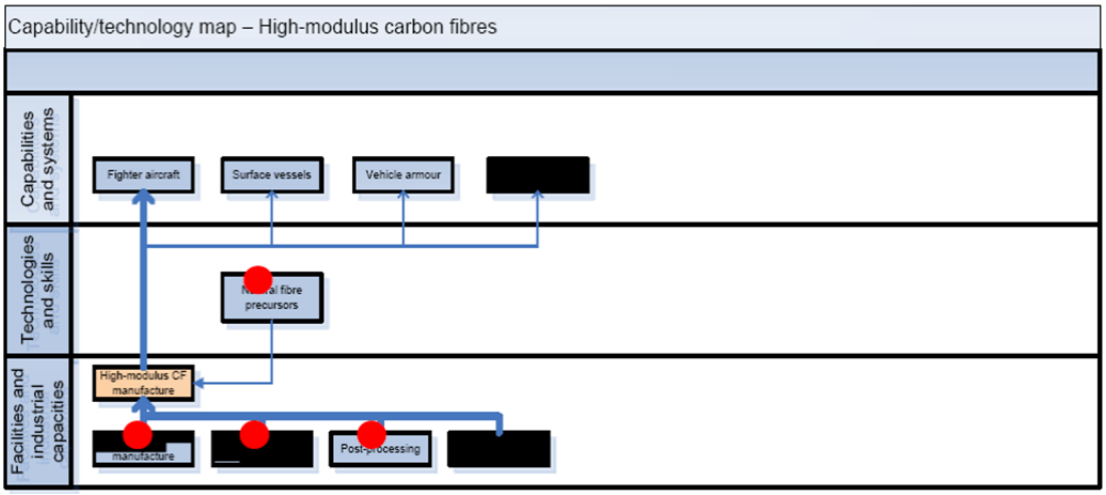

Figure 2. Taken from EDTID Final report (with permission) illustrating the relationships between capabilities, technologies and facilities/industrial capacities

The advantage of this method is that it can be applied freely from any starting point, e.g. from a needed capability downwards to derive the essential industry and assets, from an industry to derive the enabled capabilities (upwards) or essential assets (downwards) or from the bottom showing what capabilities are enabled using available assets. The model can also be used to elucidate what capabilities are affected if a particular industry is unavailable. This latter point is particularly relevant to ETCETERA due to the current trend towards a global manufacturing base where economic factors dominate the choice of location. In the current climate this is leading to re-location of much manufacturing (and some services) from bases in Europe to locations in Asia and India. While supply lines are open this is not a disadvantage, but long supply lines are clearly at greater risk of interruption by political and natural forces than shorter lines. This is a risk which is generally discounted by industry.

3 Generation of the Critical Technology List

The STACCATO taxonomy is large, containing several hundred items all in some way related to security as defined by the authors of the original STACCATO taxonomy. The task of ETCETERA was to distil from this list those technologies *essential* for security (as distinct to simply *related* to security). A tool used for this process was the definition given in Section 1 of this report. An additional task was to complement the STACCATO taxonomy with any missing items.

The process used was to manually evaluate each item in the STACCATO taxonomy to decide if the technology was critical or not. Obviously non-critical items were removed. Other items which were removed were those technologies with purely military applications (weapons systems and the like). This was motivated on the ground that ETCETERA is a civilian project, although it could be argued that military technologies used for defence are also essential for security. However, this argument was discounted as being invalid. In some cases the situation was unclear. Rather than eliminate a technology possibly critical for security at too early a stage in the process, some items were retained and colour coded as possibly critical. This list was retained as WD1.3 Enriched Critical technology List and made available to the other ETCETERA partners.

Following the first distillation, which was done by lead partner FOI, the Critical Technology List (CTL) was circulated, discussed, posted on the project wiki, and input from other WP1 partners invited. During this period additional research on the retained items was performed, mainly by more detailed literature searches, consultation with internal colleagues and other informed sources familiar with both technologies and security applications of the same. Most of this work was done by telephone contact supported in some cases by email exchange. Incidental information gathered at this stage was documented simply for possible future use by other partners in WP2, and incorporated in WD1.3. A particular effort at this stage was to clarify the status of the *possibly* critical technologies. On the basis of this, some items were removed, others retained.

It worthy to note that it is difficult, not to say impossible to define exactly where the boundary between purely military and civilian security technologies lies. In many cases the distinction can only be made on the basis of the application. To give one simple example, a sensor to detect the presence of intruders in a secure area may be civilian if the area guarded is an airport or a government building, but military if the secure area is one where active military operations are taking place. In such dual use cases the technology was retained as being critical for security. The distillation process is visualised in figure 3, taken from the DoW, and includes the first two “funnels” or stages in the development of the Validated Critical Technology List.

It was originally envisaged that the first version of the CTL would be used during the five parallel workshops. This objective was not achieved due to several reasons including:

- incorrect timing – the CTL was not available in time for the majority of the workshops
- the questions used during the workshops were predefined at an early stage and not easily related to the CTL in more than very general terms

- the participants at the workshops would have been very unlikely to understand the vast majority of the critical technologies and thus would have been unable to either validate or discount the technology
- the workshop format (the world café method) would not have allowed enough time to discuss more than a very few technologies

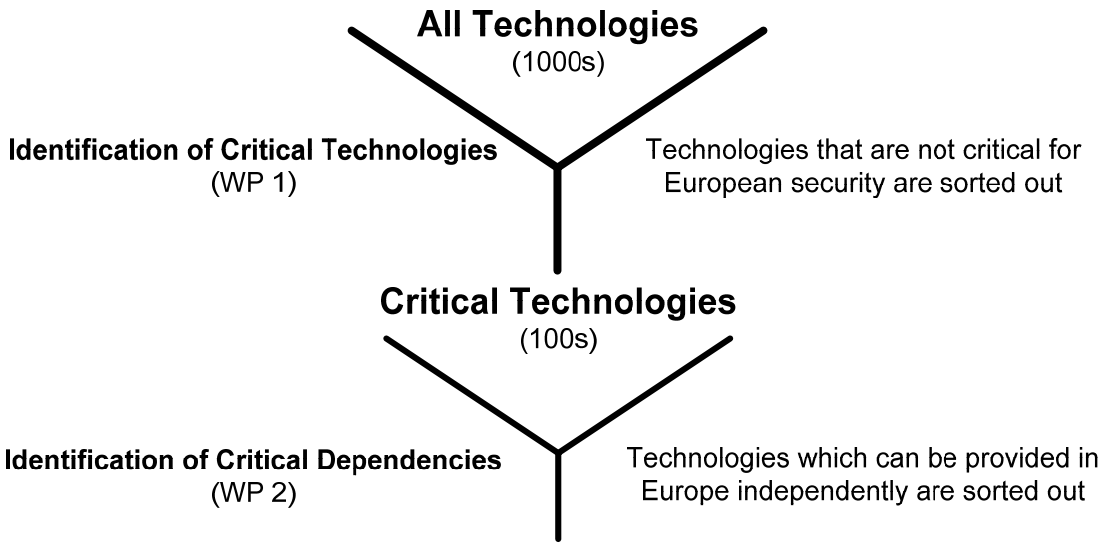

Figure 3. Taken from the description of work

Following the first coarse distillation, circulation of the CTL and receiving further input from WP1 partners and external sources (literature, internet searching, personal contacts, etc) the CTL was examined for any missing technologies. At this stage all partners were very familiar with the STACCATO taxonomy and its advantages and disadvantages. It was fairly easy to determine that due to the very broad nature of STACCATO, especially at the lower levels (Section I, Technologies and components and Section II, Equipment and subsystems) that STACCATO was all-encompassing and no missing items could be added to the list.

At this stage, and following removal of some of the previously retained items (colour coded as possibly critical) the CTL was considered as having been validated.

4 Parallel workshops

To involve industry and end-users in the process of creating a Critical Technology List (CTL), a series of five parallel workshops was organised. The reports from the workshops are gathered in Deliverable 1.1 “Stakeholder Workshops”. In this method paper we document our experience from the structure of the workshops. We also perform an analysis of the workshop report, looking for similarities and differences, and draw some general conclusions. This analysis was used to validate the CTL, deliverable D1.2.

4.1 Structure of the workshops

In order to streamline the five workshops a training exercise (run as a meta-workshop) was held on 30 January 2012 in Bonn (Germany) to ensure that each workshop had approximately the same structure (using the World Café method) and that the output from the workshops was in a common format. The five workshops involved 72 participants as shown in Table 1. Each workshop had a mix of end-users, scientists, industry representatives and individuals from other parts of society. The workshops were held at sites relevant to the security area, to provide added relevance to the workshop and to create additional value to the participating end-users, who are normally primarily engaged in using a particular technology rather than designing, developing or evaluating technologies. A part of each workshop involved a tour of the site, from a security point of view and with the intention of improving cross-mission awareness. The actual sites of each workshop can be found in Table 1.

Table 1. Statistics from the workshops. The numbers for Spain do not indicate the number of people but the number of participating organisations. The “sum” is the total number of participants.

	Site	Enduser	Industry	Scientist	Other	Sum
Spain	Santiago Bernabéu football stadium	5	4	2	1	20
Germany	Building site for the Cologne Underground	2	2	6	2	12
Italy	NH Vittorio Veneto	2	2	5	-	9
Sweden	Emergency Service command centre, Stockholm	3	6	5	2	16
France	Gare de Lyon, Paris	4	4	6	1	15
Sum		16	18	19	6	72

4.2 The workshop questions

Getting the focus question for a workshop right is very important. The focus question will drive the whole workshop. It triggers the brainstorming activities and provides a guide for the clustering and naming. It’s important to create questions that both focus the topic and elicit lateral thinking.

The following two questions were used at all five parallel workshops.

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

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

The two questions were developed during the meta-workshop for which the primary goal was to spread the world café method to the people who were then to host the five parallel workshops. The meta-workshop had the same structure as the parallel workshops and the first question discussed was “How can we pose the questions to our stakeholders so that we can get the most information about “critical” and “emerging” technologies?”

After the workshop procedure of brainstorming, grouping and voting two major trends materialized - one for critical technologies and the other for emerging technologies, see Figure 4. From these two trends, two questions were formulated at the meta-workshops:

- “What would be your worst nightmare if technology fails?”
- “Dream that you are an inventor – no limits – what technology would you create?”

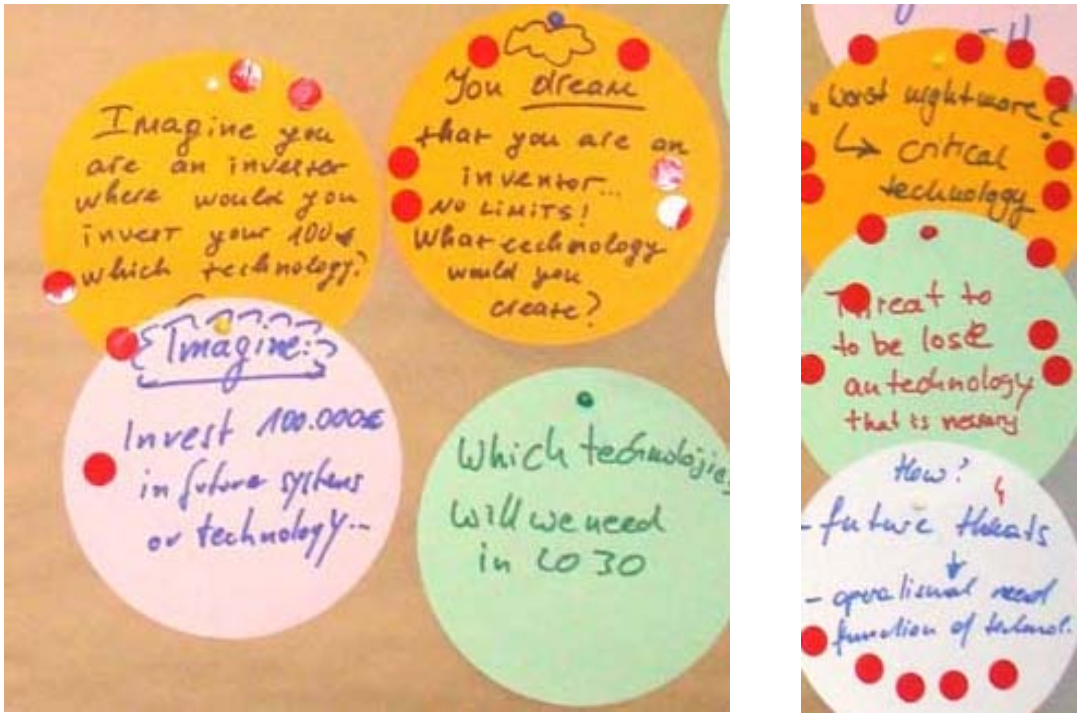

Figure 4. The two groups of ideas with the most votes, as found when answering "How can we pose the questions to our stakeholders so that we can get the most information about “critical” and “emerging” technologies?" at the meta-workshop. The left group is connected to emerging technologies while the right group is related to critical technologies.

When further developing the focus questions for the parallel workshops there was focus on keeping the questions open, clear, simple and abstract (which in this case meant to avoid using the technical terms “critical technology” and “emerging technology” in the question). Due to the limited time given for the parallel workshops there was a design decision to be made about how open the questions could be while still giving relevant answers in the time at hand, i.e. a compromise had to be made between openness and focus.

Other thoughts that came up during the meta-workshop was that lateral thinking and creativity should be encouraged and that it is important to find questions that express the challenges that end-users face. Furthermore it was decided to keep the questions for the World Café secret from the participants before entering the workshops. It is important that the discussion must be kept open and informal in order to obtain free, creative answers made at the moment and by the group (i.e. there should be no “official” answers).

4.3 Analysis of the workshops

The discussions that followed from the first focus question were broad and ranged across all levels of the STACCATO classification from components up to mission areas. The five workshops pointed out a few broad areas as important from a security point of view (Table 2).

Table 2. Important areas for the security arena.
These were developed when discussing question 1 at the workshops

Important areas for security
1. Critical infrastructure including:
a. Energy and electricity (incl. the distribution grid)
b. Communications (virtual and real) and transport
c. Sewage treatment, water & air quality
d. Logistics & production
2. Emergency systems – command & control, warning systems
3. Cyber security – data protection, communication, financial systems
4. Crowd management
5. Trustworthy identification (RFID, biometrics, image analysis)
Important non-technological topics
6. Human behaviour – false security, imagined risk, security awareness
7. Intellectual property
8. Social development
9. Privacy – data protection

Question 1 also allowed for discussions around solutions to the missing vital equipment and the following themes were frequently mentioned: organisation and methods, decentralisation, flexibility, training, maintaining low-tech capabilities, promoting societal awareness and also other general societal aspects as e.g. education, equality and belongingness.

It is interesting to note that the solution space arising from question 1 mainly revolves around soft or human factors. One of the workshops also attempted to define a technology as “critical” when a human cannot replace it. In general it seems that focus drifted from technologies to human factors (culture, organisation, methods).

Focus question 2 was more focused on solution space and also was forward looking towards non-existing technologies. The question explicitly encouraged the participants to think freely, unorthodoxly and without restrictions. In table 3 a list of future technologies "invented" at the workshops is presented. Again the list ranges from broad themes to specific technologies.

Table 3. Futuristic solutions for the security arena.
These were developed when discussing question 2 at the workshops. Some mind-bending suggestions are excluded, as e.g. machines to translate cultures and invoke peace

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)**

Emerging technologies are clearly oriented to human needs and human protection. Societal aspects played a large role in the discussions as well as the right compromise between Security and Liberty of the citizen in particular when discussing surveillance, detection of anomalous behaviour and tracking of people. Issues that were raised were that:

- The security control has to be discrete and non invasive (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 products

4.4 Summary of workshop conclusions

The main conclusions that can be drawn from the five workshops are that:

- Specific organisation and methods need to be available in order to manage crises (multiple actors, responsibility)
- Energy, information technology and communications are essential and their potential vulnerabilities should be understood
- Security technology should serve people and enhance working conditions, be available for end-users and be evaluated regarding their influence (negative and positive) on society
- Security has to be treated in a societal and human context
- Novel security measures should be less intrusive and more efficient
- There is an overlap between the “inventions” of the workshop and the emerging technologies found by consortium analysis

4.5 Observations concerning the world café method

In the process of a workshop ideas are first generated, then structured and hopefully converge to a few dominant ideas. The world café method stimulates the participants to be active and opinioned. The method is fun and inspiring but it is rather hard to draw conclusions from the results obtained. The method is useful to reach a consensus opinion in the group.

For the first question the method was relevant and identified important areas and technologies. One sign of this is that the different workshops reached similar consensus results (identifying energy and communication as important and pointing to robust methods and organisation as important to ensure security). To be critical, the first question did not give any new insight but confirmed what we already know, which in part was the point of the exercise: The end-users validated what is a critical technology.

The second focus question was maybe a little too open with “feel free to bend the laws of physics”, especially since most of the workshops did not use a voting procedure for the second focus question. The discussions around question 2 were at times unfocused and it was hard to synthetize these discussions into something simple. This said, emerging technologies are by definition not well defined.

The ideal size of a world café working group is a compromise between, on the one hand the need to have a large group with much input and a broad base for the consensus arrived at and on the other hand the ambition that every participant can be heard and actively contribute. With the amount of time given approximately 25 participants per workshop would have been ideal. From a practical point of view all workshops had problems with too few participants. The composition of the group influences the direction the discussions take and fewer participants introduce a larger bias. Another interesting observation is that the choice of site actually influenced the results somewhat, e.g. the workshop at a railway station emphasised crowd control and the workshop at an emergency service command centre emphasised command and information tools. This difficulty to control the influence of the exercise composition and settings is somewhat offset by holding multiple workshops.

5 Conclusions

The STACCATO taxonomy can be improved by additional analysis taking as the starting point a particular category of user. This will focus the technologies towards a particular context instead of the current taxonomy which is simply an un-prioritized list with no particular direction. Suitable user categories are:

- First responders (emergency personnel, ambulance and paramedical personnel, firefighters)
- Security personnel (including police, customs & excise, lifeguards, security guards)
- Essential services, further subdivided into:
    - Water and sewage services
    - Electricity services
    - Transport infrastructure (road, rail, air, water)
    - Medical services (hospitals)
    - Communications (electronic, telephone network, TV, radio, including the necessary infrastructure)

The world café method is a suitable and efficient method of obtaining input and building consensus from a range of sources. The workshops held, although in some cases falling short of the ideal size, did all confirm the need for energy and communication as essential, and pointed to robust methods and organisations as fundamental needs to ensure security. The second question was perhaps somewhat too broad to give conclusive results, but it is in the nature of emerging technologies that these are difficult to evaluate in advance.

6 References

The following literature sources have been used in development of the Critical Technology List. The list is not prioritized.

- ASD (Aerospace and Defence Industries Association of Europe). *Technological & Industrial non-Dependence ASD study and way forward*. Presentation 2012-04-25.
- M. Bengisu and R. Nekhili. *Forecasting emerging technologies with the aid of science and technology databases.* Technol. Forecasting & Social Change, 73 (2006) 835-844
- Commerce Control List Suppl. No. 1 to part 774
- European Space Agency/European Defence Agency. *Critical Space technologies for European Strategic Non-Dependence.* List of urgent actions 2010/2011 rev. 21/12/09
- European Space Agency/European Defence Agency. *Critical Space technologies for European Strategic Non-Dependence.* Draft list of urgent actions for 2012/2013 Draft for Commenting by National Delegations and Industry V.2.0
- A.D. James. *Defence and security R&R in Europe SANDERA background paper. One part of deliverable 2.1.* 15th Dec. 2009. [SANDERA = Security and Defence in the European Research Area]
- F. Wising, B. Foucher, B. Candaele (eds.) *DISCOTECH WP2: Forecast of COTS developments.* 25/09/2008. [DISCOTECH = Disruptive COTS Technologies in the IT Area]
- B. Foucher and B. Candaele (eds.) *WP3 – Identification of areas where COTS technologies and components will not be sufficient for the needs of the military user. Final report.* 22/12/2008
- B. Candaele (ed.) *Establishment of roadmaps for European investments in component development for the military user. Progress report.* 25/05/2009
- B. Canle, B. Fodaeucher, M. Levin. *DISCOTECH presentation of final results.* June 2009
- T. Durand. *Twelve lessons from "Key Technologies 2005": The French Technology Foresight Exercise.* J. Forecast. 22 (2003) 161-177
- A. Dwivedi. *Critical technology gaps and potential solutions for mobile free space optical networking.* Military Communications Conference, 2006. MILCOM 2006. IEEE DOI: 10.1109/MILCOM.2006.302330
- European Commission (ed.) *Emerging technologies in the context of "security": Issued in the Framework of Science and Technology Foresight.* 2011. ISBN-10: 3843326630
- ESRAB European Security Advisory Board (ed.) *Meeting the challenge: the European Security Research Agenda.* Sept. 2006
- European security research & innovation forum (ESRIF). *Final report.* Dec. 2009
- Defence R&T Committee of ASD. *ETnD in the 2020 future R&D European policy – inputs from the Defence sector.* V23 Dec. 2011 – Final
- ESTP (European Space Technology Platform). Strategic research agenda V1.0 22.6.2006. Available from http://www.estp-space.eu
- N.S. Gluck, H.R. Last. *Military and Potential Homeland Security Applications for Microelectromechanical Systems (MEMS).* Institute for Defence Analysis IDA document D-3067. Nov. 2004

- Committee on Optical Science & Engineering, National Research Council (ed.). Harnessing Light: Optical Science & Engineering for the 21st Century. ISBN: 0-309-53884-X. Available from: http://www.nap.edu/catalog/5954.html
- G.P. Hatch. *Critical rare earths. Global supply and demand projections and the leading contenders for new sources of supply.* TMR (Technology Metals Research). Aug. 2011. Available at: www.CriticalRareEarthsReport.com
- R.A. van Atta, D.L. Gandle, J.F. Cauley. *Integrating the Critical Technologies Approach into the Defense Export Control Process.* Jan. 1981. ADA103497
- ITAR (International Traffic in Arms Regulations) incl. Part 121-The United states Munitions List. Available from: http://www.fas.org/spp/starwars/offdocs/itar/p121.htm#ITAR
- ITRS (International technology roadmap for semiconductors) 2007 ed. Executive summary.
- M.C. Kemp, P.F. Taday, B.E. Cole, J.A. Cluff, W.R. Tribe. *Security applications of terahertz technology.* Terahertz for Military and Security Applications. R.J. Hwu, D.L. Woolard (eds.). Proc. SPIE 5070 (2003) 44-52.
- R.N. Kostoff, R. Boylan, G.R. Simons. *Disruptive technology roadmaps.* Technol. Forecast. & Soc. Change 71 (2004) 141-159
- N. Lombardo, C. Knudson, R. Ozanich, F. Rutz, S. Singh, M. Tardiff. *A next-generation countermeasure architecture to prevent explosives attacks at large public events.* Technologies for Homeland Security, 2009. HST '09. IEEE. DOI: 10.1109/THS.2009.5168043
- A.R. Metke, R.L. Ekl. *Smart grid security technology.* Conf. On Innovative Smart Grid Technologies (ISGT), 19-21 Jan. 2010. Pp. 1-7
- MONA (Merging Optics and Nanotechnologies). A European roadmap for photonics and nanotechnologies. March 2008. Available from: http://www.ist-mona.org/home.asp
- nanoRoad Nanomaterial Roadmap 2015. *Overview on promising nanomaterials for industrial applications.* http://www.ist-world.org/ProjectDetails.aspx?ProjectId=44b7c13e872c4a0e86a08ba70ceb0cb8&SourceDatabaseId=7cff9226e582440894200b751bab883f
- Technology Strategy Board (ed.) *Nanoscale technologies Strategy 2009-12.* Available from www.innovateuk.org
- HK Government (ed.) *UK Nanotechnologies Strategy: Small technologies, Great opportunities.* March 2010
- Materials UK (Materials transfer network). *Nanotechnology: A UK Industry View. 2010.* Available from: www.matuk.co.uk
- National Institute of Justice. *Guide for the selection of chemical and biological decomtamination equipment for emergency first responders.* NIJ Guide 103-00. Oct. 2001
- C. Kiparissides (ed.) NMP Expert Advisory Group (EAG) *Position paper on future RTD activities of NMP for the period 2010-2015.* EUR24179 EN. Nov 2009.
- Federation of American Scientists. *Nuclear weapons effects technology (Section VI).* Available from: http://www.fas.org/irp/threat/mctl98-2/p2sec06.pdf
- National Research Council of the National Academies, Committee on Harnessing Light: Capitalizing on Optical Science Trends and Challenges for Future Research. *Optics and Photonics: Essential technologies for our nation.* 2012. Available from www.nap.edu
- Photonics 21 Second strategic research agenda in photonics. 2012. Available from: http://www.photonics21.org/

- J. Price, Nevada Bureau of Mines & Geology. Energy critical elements – securing materials for emerging technologies. Presentation 2011. Available from: http://dnr.alaska.gov/commis/priorities/Slides/JonanthanPrice.pdf
- S. Rawal. *Metal-matrix composites for space applications*. JOM 53 (2001) 14-17
- J.R. Richardson (ed.) *Proc. workshop on Combatting Fissile Materials Smuggling Workshop #5.* 30-07-1997. Lawrence Livermore National Laboratory UCRL-JC-13426
- K. Sage & S. Young. Security applications of computer vision. IEEE AES Systems Magazine April 1999 pp. 19-24
- G.M. Scott. *Critical technology management issues of new product development in high-tech companies.* J. Prod. Innov. Manag. 17 (2000) 57-77
- N. Spencer, P. Uggowitzer, P. Smith, K. Feldman. *Unique label for identification or security system.* US Patent. 7,963,563 B2. June 21, 2011
- G. Martini. *STACCATO.* Presentation SCR08, 29-30 Sept. 2008
- G. Martini. *STACCATO – Main conclusions and recommendations on the European Security Equipment Market (ESEM).* Sept. 2008. Available here: http://www.iai.it/pdf/Economia_difesa/STACCATO_Final-Report-Executive-Summary.pdf
- ASD (Aerospace and Defence Industries Association of Europe). STACCATO (Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities). *Deliverable D1.2.2 STACCATO Final Taxonomy.* 15 Jan. 2007
- *Study on How to measure Strengths and Weaknesses of the DTIB in Europe.* EDA ref. 07-I&M-002 (available to EDA pMS governments).
- *Japan-EU workshop on substitution of Critical Raw Materials.* Final report. Nov. 2011
- T. Ueno, M. Hasegawa, M. Yoshimura, H. Okada, T. Nishioka, K. Teraoka, A. Fujii, S. Nakayama. *Development of ZnS lenses for FIR cameras.* SEI Technical Review No. 69 October 2009 pp 48-53
- UK MoD Defence Technology Strategy for the demands of the 21st century. 2006 Available from www.science.mod.uk
- UK MoD National security through technology: technology, equipment and support for UK defence and security. Feb. 2012. Available from: www.tsoshop.co.uk
- Joint U.S. Defence Science Board and UK Defense Scientific Advisory Council. *Task force on Defence Critical Technologies.* March 2006.
- C.M. Stickley. *Uses of DARPA materials sciency and technology in DoD systems.* Final report May 1996. ADA311508
- C.S. Wagner and S.W. Popper. *Identifying critical technologies in the Unites States: A review of the Federal Effort.* J. Forecast. 22 (2003) 113-128
- Swedish ICT – verksamhetsråd Security (Advisory committee) - “VR dokument” 2008 (in Swedish).
- EDTID Final report EDA Contract 10-R&T-OP-33 May 2012.