...ETCETERA

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

DELIVERABLE D3.1

Report on Validated Alternative Technological Solutions

Authors: Steven J Savage, Malek Khan, Riitta Räty, Camilla Trané (FOI)

November 2013

Dissemination Level: PU

1 Introduction

The collaborative FP7 project “Evaluation of critical and emerging technologies for the elaboration of a security research agenda” (ETCETERA) had two main objectives:

1. To deliver several qualified lists concerning Critical and Emerging Technologies and balanced research plans to deal with current and future needs
2. To develop and apply novel approaches and methods for the evaluation of Critical and Emerging Technologies and for strategic security research planning

The approach is illustrated schematically in Figure 1 below.

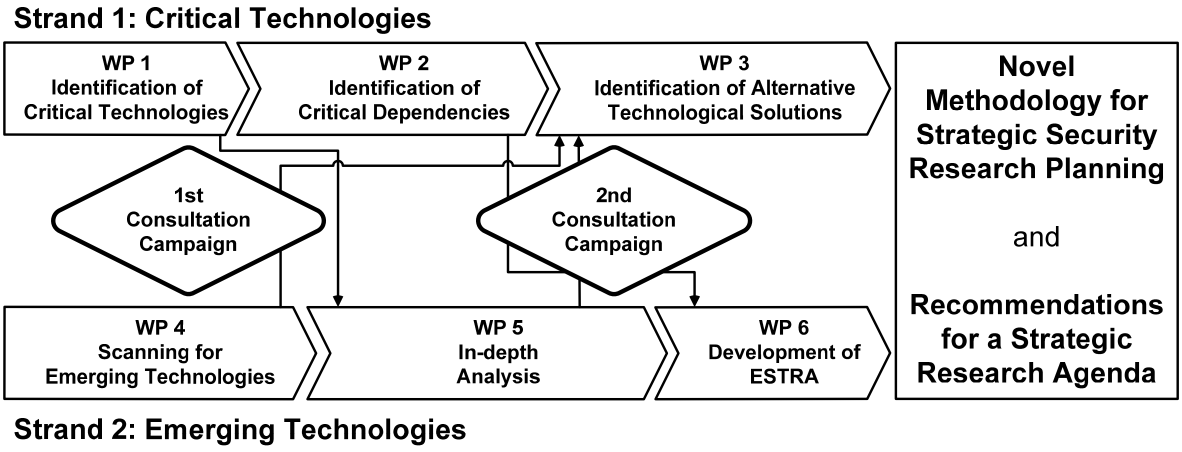
Strand 1: Critical Technologies
WP 1 Identification of Critical Technologies
WP 2 Identification of Critical Dependencies
WP 3 Identification of Alternative Technological Solutions
1st Consultation Campaign
2nd Consultation Campaign
WP 4 Scanning for Emerging Technologies
WP 5 In-depth Analysis
WP 6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

Figure 1 showing the position of WP3 in the flow chart of ETCETERA work packages

This report documents the methods used in and the results obtained from WP3.
The objective of this WP is to identify and wherever possible verify alternatives to security technologies which have been shown in WP2 to suffer from critical dependencies. It was expected that the input from WP2 would be a relatively long list of critical technologies with critical dependencies, but in fact the list was not as extensive as expected and so it was possible to analyse all the critical technologies with critical dependencies, with four technologies in particular selected for in-depth analysis. This means that the original TEPID-OIL[1] filtering method planned to reduce the number of critical technologies was not absolutely necessary. However it may still be useful in the future to filter larger numbers of critical technologies, so the TEPID-OIL method was investigated as regards its usefulness for this purpose.

While the emphasis has been on method development and application of different methods to find ways to eliminate critical dependencies, some attention has been paid to ethical issues which might arise from implementation of the alternative solutions.

[1] TEPID-OIL = Training, Equipment, Personnel, Infrastructure, Doctrine & concepts, Organisation, Information & Logistics

2 Input to the integration

2.1 The ITIPOLITRE[2] method

The TEPID-OIL method (or a similar method) was to be used to filter a list of critical technologies, separating those dependencies which could be eliminated by alternative technological solutions from those which could be eliminated by non-technological solutions. In the event filtering was not necessary as the list of critical technologies with critical dependencies was shorter than expected (13 technologies in all, from WP2 and Task 3.2) and it was practicable to analyse them all.

However, the general approach is considered valid and this being the case the applicability of the TEPID-OIL method was studied. The method was originally developed for military technologies and situations, but for civilian security situations the needs are somewhat different as the range of possible situations is much wider and less well defined. The TEPID-OIL method was therefore extended by including the additional parameters: *Incitement/psychology* and *Economy/market mechanisms*. These parameters are not included in TEPID-OIL, but are now included in the extended method abbreviated as ITIPOLITRE.

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

The results of Task 3.1 are documented in WD3.1.[3]

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

The WBAT[4] method was developed by Fraunhofer INT, originally to investigate the potential of a large number of industrial chemicals for risks that they might be used as improvised chemical weapons by terrorists.

WBAT had never been used in the present context (to identify critical dependencies), but the method is flexible and in WP2 Task 2.2 it was adapted to compare different security technologies from the point of view of stakeholders (end-users) with widely varying backgrounds and needs. Below (Figure 2) is shown an example of the WBAT-CD matrix as developed in WP2 (Task 2.4) and applied in the WBAT-workshop in WP3 (Task 3.2). The details of the 2nd Consultation Campaign and how the WBAT-CD was applied are reported separately.[5]

[2] ITIPOLITRE = Incitements/Psychology, Technology/Equipment. Information/Information systems, Personnel, Organization, Logistics, Infrastructure/Facilities, Training/Education, Rules, Economy/Finance

[3] WD3.1 ITIPOLITRE – a method to identify a wide range of alternative security technologies. R. Räty, C. Trané, M. Khan & S. Savage (FOI-S--4418--SE, October 2013).

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

[5] WD3.2 – Report on the Evaluation of the 2nd Consultation Campaign. J. Burbiel & R. Schietke, Nov. 2013

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

Figure 2 showing a section of the WBAM matrix as used in the workshop (WP3 Task 3.2)

WP2, Task 2.4 modified the WBAT and developed it into WBAT-CD (Weighted Bit Assessment Table – Critical Dependencies) and used it to compare different security technologies for any possible dependencies. A workshop was arranged in Task 3.2 where a number of experts and stakeholders participated and applied the WBAT-CD method. Results from this workshop were compared with DTAG[6] and other workshops in WP2 and results from the 2nd Consultation Campaign.[7] This resulted in a short list of 13 prioritised critical dependencies and a reserve list of 30 less relevant technologies where the dependency was not entirely clear. The prioritised 13 technologies with critical dependencies were analysed for alternatives in Task 3.3.

We conclude that the modified WBAT-CD is a relevant method which can be combined with SETAG to identify critical dependencies. However in several cases the result was unclear and care should be used in applying the results.

2.3 Identification & in-depth analysis of alternative solutions including verification of the findings

Tasks 3.3 & 3.4 were the most challenging in WP3. The “shortlist” of 13 prioritised critical technologies with critical dependencies was examined and overlapping technologies eliminated. For instance it was concluded that from a technology viewpoint jamming and anti-jamming technologies were highly related, despite having different applications from the end-user viewpoint, and in a security context both can be used by legally authorised bodies or for illegal/antagonistic activities. The reduced short list contained 10 critical technologies with critical dependencies, as listed in Table 1 below.

Table 1. Critical technologies with critical dependencies investigated in WP 3

Code[8]	Name
110-1	Neutron detection technologies
110-3	Gamma technologies
113-10	Jamming technologies
113-10	Anti-jamming technologies
117	Information security – Secure communication
121-5	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants
200-4/ 210-2	Explosives detection sensors/equipment
112-2	Digital signal processing technology
101-13	Smart textiles
504B-2	Simulation for decision making (real time simulation)

[6] DTAG = Disruptive Technology Assessment Game, originally developed for defence applications. The DTAG was adapted to the present project with security focus and re-named SETAG (Security Emerging Technology Assessment Game).

[7] WD3.2 Report on the Evaluation of the 2nd Consultation Campaign. J. Burbiel & R. Schietke, Fraunhofer-INT, October 2013.

[8] The numbers refer to the STACCATO taxonomy.

The technologies on this list were investigated in a process illustrated in the figure below.

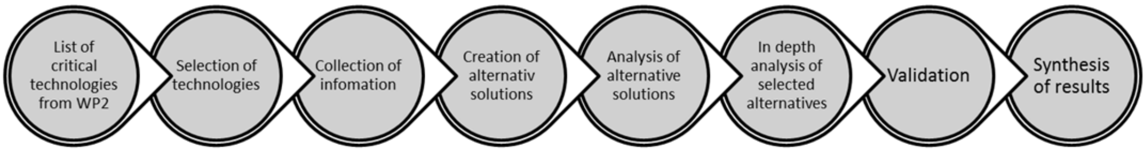
List of critical technologies from WP2
Selection of technologies
Collection of infomation
Creation of alternativ solutions
Analysis of alternative solutions
In depth analysis of selected alternatives
Validation
Synthesis of results

Figure 3 showing the sequence used in the study to identify alternative solutions to critical technologies with critical dependencies.

Important steps in the process were to gather more detailed information about the nature of the critical dependency (information about this from WP2 was necessarily imprecise). This was done by consultation with selected subject matter experts, i.e. scientists well aware of the technology, its nature and security applications. The consultation was done by telephone interviews and written surveys/responses. We chose as the time horizon about 10 years although this was not a hard boundary and longer time horizons were permitted.

Four emerging technologies were also selected for additional in-depth analysis where separate reports were written on the technology. These are included in WP5. The selection was made on the basis of relevance (a broad range of end-users), difficulty (where there is no really satisfactory technical solution available at present) simplicity (where a critical dependency could perhaps be eliminated by simple substitution) and rate of development (i.e. an emerging technology area driven primarily by none-security related applications and civilian market forces). These four in-depth analyses included:

- smart textiles
- detection material replacement for ^{3}He in neutron detectors
- new detection materials combining neutron and gamma detection
- small local mobile standard technologies for explosive detection

A wide range of alternative solutions were generated, as documented in WD3.3.[9] These solutions were however generated mainly from input from a number of scientists and technical experts, many of whom lack direct “hands-on” experience of using the technology in a live situation. To validate the alternative solutions these were presented to and discussed with SSBF[10], considered as representative of typical “broad spectrum” first responders. Each solution was examined from the points of usefulness in likely emergency situations and practicability from the end-user point of view. Comments from the validation were incorporated into the analysis.

A significant and unexpected conclusion was that it is not meaningful to consider technological solutions in isolation from non-technological solutions, as both are essential in real situations. This was not anticipated in the DoW.[11]

This resulted in 16 different alternative solutions, each of which is associated with one or more recommendations for future action. We have been as concrete as possible with our recommendations.

[9] WD 3.3 Identification and in-depth analysis of alternative technological solutions (to critical technologies with critical dependencies. M. Khan, R. Räty, S. Savage & C. Trané. (FOI-S--XXX--SE November 2013)
[10] SSBF = StorStockholms BrandFörsvar, the Greater Stockholm Fire Service
[11] DoW = Description of Work, i.e. Annex 1 of ETCETERA

2.4 Ethical aspects of the technologies

There is considerable public concern about the proliferation of surveillance and monitoring technologies, many of which have been developed quickly due to urgent needs and without regard for the integrity and the privacy of European citizens. It is important that future security technologies take these concerns into account, otherwise there is a risk that none-acceptance will limit the usefulness of the technology. Note that not all security technologies have the same potential to raise integrity issues. The most potent are those technologies using optical camera techniques, especially where images are transmitted or recorded. For this reason it is highly desirable to avoid image-based security technologies wherever possible.

For this reason experts in ethics and integrity have been partners in ETCETERA, and have been consulted in developing the alternative solutions to critical dependencies. Each alternative solution has been assessed for ethical impact (using a 4-level scale) by the subject matter technical experts consulted. These are of course not necessarily experts in ethics, so additional expertise from the partner CSSC has been included[12].

Two of the alternative technologies analysed in-depth were presented and discussed in an ethics workshop[13], which also served to disseminate information about ETCETERA to a wider audience.

3 General conclusions and recommendations

- The initial list of critical technologies (STACCATO) provided a structure and initial overview of technologies that could be relevant, but its structure and contents also led to difficulties. The list contains a mixture of rather narrow single technologies and very broad technology categories. The STACCATO list also contains several items where the same technology may appear under different topics. *Recommendation: if the STACCATO taxonomy is to be used in a similar way in the future is should be re-examined, overlapping technologies clarified by creating sub-categories and duplicated technologies eliminated.*

- The nature of the critical dependency for a specific technology identified in WP 2 is often rather general, which makes identification of a specific solution to resolve the dependence difficult. However “generic“ solutions are likely to be at least as useful initially, bearing in mind the large number of different situations in which the same critical technology may be used. *Recommendation: it is frequently the intended use of the technology which determines if it is critical or not, so the actual uses of the technologies should be emphasised more. This should make easier identification of alternative technologies in particular use-cases and situations.*

- It is very rare that a critical technology with a critical dependency can simply be replaced by a critical technology without any dependency. One example of this direct substitution is replacement of ^{3}He. This does however demand development of new detector technology, where other dependencies might occur. It is however useful to be aware of the dependencies as they are one aspect that influences the “security” of a technology.

[12] CSSC = Centre for Science, Society and Citizenship, Italy.

[13] Report on the Dissemination Workshop Ethics, Governance, and Societal Implications of Emerging Security Technologies. E. Mordini. (CSSC, September 2013)

- It is misleading to assume that there is a direct link between a critical dependency and a potential solution. Most technologies used in security applications have many different ways to be used in different situations. It is possible (or likely) there may be more than one technology that can be used in a specific situation. However, in doing an analysis both the technology and situation have to be specified, as we have tried to do here. In some cases it is an economic factor which determines the technology chosen.
- There may be differences in finding alternative solutions for critical dependencies if the threat is accidental (e.g. natural disaster) or antagonistic (e.g. sabotage or attack). However, this aspect was not studied in this WP. *Recommendation: consider more carefully the nature of the threat which the critical technology is used to mitigate.*
- Most of the technologies studied related to reaction to antagonistic action, others related to proactive (preventative) action.
- In the main, potential solutions are developments of current technologies. To identify additional innovative solutions more creative settings need to be used. Foremost this means setting up creative settings and taking more time for the dialogues. Both a workshop and a group interview could be useful but we believe it to be vital that several different kinds of expertise are involved. However, the ETCETERA project has for the selected technologies pointed to areas that could contribute to the development of a European security research agenda.
- In our analysis all technologies have equal weight. We have also not removed any alternative solutions and as a consequence some technologies (e.g. jamming) may appear predominant. This reflects however the ease with which it was to generate alternative solutions, and not necessarily the quality of the solutions. *Recommendation: we believe it is important that the possibility for the occurrence of threats should be a factor in prioritizing the alternative solutions.*
- Ethical implications should also be considered for the alternative solutions. This was a factor which raised several concerns, and ethical implications are most pronounced in the areas relating to surveillance technology, secure communications and real-time simulation.

4 Prioritisation and specific recommendations

For each of the prioritised critical technologies with critical dependencies we have developed a series of recommendations. These are given in full in WD3.3, and are only briefly summarised here. The code number refers to the STACCATO taxonomy[14].

<table>
<tr><td>110-1</td><td><b>Neutron detection technologies</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Detection of radioactive materials</b></td></tr>
<tr><td colspan="2">There is a need to improve current neutron and gamma radiation detectors, in part to alleviate the growing shortage of ^{3}He and in part to develop combined and portable neutron and gamma radiation detectors in the same instrument.
<i>Recommendation: Recommendation: (i) initiate studies into the possibility of using new neutron detector materials such as ^{6}Li and ^{10}Be, (ii) initiate studies into ways to combine neutron and gamma radiation detection in the same instrument. Emphasis should be placed on techniques which allow identification and discrimination between different gamma sources to eliminate false positives from innocuous materials. The primary end-user group includes border control agencies, operators of at-risk facilities and large shipping/transfer facilities.</i></td></tr>
</table>

<table>
<tr><td>113-10</td><td><b>Jamming technologies/ Anti-jamming technologies</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Protective jamming and tracking technology</b></td></tr>
<tr><td colspan="2">There is a need to develop technology for protective jamming in order to prevent wireless communication, e.g. to prevent remote triggering of explosive devices or to legally prevent communication under special circumstances. There is also a need to develop technology to enable tracking the source of jamming signals.
<i>Recommendation: initiate actions to (i) develop technology for small, portable and low(er) energy devices for local jamming. If this can also be made directional there is a potential application in police operations to safely stop non-cooperative vehicles, (ii) develop technology to enable source tracing/tracking of (antagonistic) jamming signals. The primary end-user groups include special security agencies and the police.</i></td></tr>
</table>

<table>
<tr><td>113-10</td><td><b>Jamming technologies/ Anti-jamming technologies</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Forum for dialogue</b></td></tr>
<tr><td colspan="2">There is a need for improved information exchange and dialogue between developers, manufacturers and end-users in the field of jamming/anti-jamming and in the field of explosives detection.
<i>Recommendation: create a forum or fora for dialogue in jamming/anti-jamming and in explosives detection. The target group should include developers, manufacturers and end-users of the technologies</i></td></tr>
</table>

[14] STACCATO = Stakeholders Platform for Supply chain Mapping Market condition Analysis and Technologies Opportunities, developed by the Aerospace and Defence Industries Association of Europe. 2007 (http://cordis.europa.eu/fp7/security/pasr-project-leaflets_en.html)

<table>
<tr><td>117</td><td><b>Information security – Secure communication</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Secure communications</b></td></tr>
<tr><td colspan="2">There is a need to improve security in all forms of electronic communication. The technology in modern cell phones and internet-based communication is developed for speed and convenience, not security. There are multiple ways to improve security.
<i>Recommendation: (i) develop methods and technology to allow users to make security related choices, e.g. to decide the route of communication (i.e. to select which nodes the communication is allowed – or not allowed – to pass), (ii) improve the speed of communication protocols and algorithms and if possible include functionality to automatically adjust the security level according to the information, (iii) study the possibilities to encode security measures in the communication itself, i.e. object-based security. The primary end-user group includes software and hardware developers and end-users. For (iii) it is likely that basic research organisations must be engaged.</i></td></tr>
</table>

<table>
<tr><td>117</td><td><b>Information security – Secure communication</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Authentication</b></td></tr>
<tr><td colspan="2">There is a need to authenticate the communicating parties, to reduce the risk of insecure business transactions and manipulation of information.
<i>Recommendation: develop a system of authentication, perhaps using digital certificates/keys to and improved protocols to identify the corresponding parties. The primary target group includes software developers, system operators and a wide variety of end-users not limited to the security field.</i></td></tr>
</table>

<table>
<tr><td>117</td><td><b>Information security – Secure communication</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Ad-hoc communication systems</b></td></tr>
<tr><td colspan="2">These systems are currently under development and appear to have significant potential for future robust communication, e.g. in crisis management when parts of the normal infrastructure are disabled.
<i>Recommendation: initiate actions to study integration of security features at the design stage, prior to production and implementation. Research is specifically needed on how to obtain secure communication without compromising robustness and usability. The primary target group includes software developers and crisis management/infrastructure end-users.</i></td></tr>
</table>

<table>
<tr><td>121-5</td><td><b>Rapid analysis of biological agents and of human susceptibility to diseases and toxicants</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Risk awareness and biological threats</b></td></tr>
<tr><td colspan="2">First responders are not trained in managing incidents involving biological agents and normally do not even consider the possibility of exposure to B-agents. Crisis managers are not aware of the risks of B-agents.
<i>Recommendation: (i) initiate actions to increase awareness of the risk of incidents involving B-agents. The primary target group is crisis managers, (ii) initiate actions to evaluate the feasibility of developing and implementing automatic B-agent (and possibly C-agent) sample „dosimeter-like“ collectors and the usefulness of such devices. The primary target group is developers and first responder end-users.</i></td></tr>
</table>

<table>
<tr><td>121-5</td><td><b>Rapid analysis of biological agents and of human susceptibility to diseases and toxicants</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Early detection of exposure to and transmission of B-agents</b></td></tr>
<tr><td colspan="2">There is a need to develop better capacity to identify exposure to and transmission patterns for B-agents. Since B-agents have an incubation time of hours to days, there is time for exposed/contaminated persons to travel and spread the agent. This also makes it difficult to detect and identify the disease since it may take some time before it is recognised that a B-agent has been released, and it is always difficult to locate the source of the agent.
<i>Recommendation: initiate actions to develop procedures for sharing, distribution and analysis of information regarding early detection and transmission of B- (and to a lesser extent C-) agents. The primary target group is national and international crisis management agencies.</i></td></tr>
</table>

<table>
<tr><td>121-5</td><td><b>Rapid analysis of biological agents and of human susceptibility to diseases and toxicants</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Sampling, detection and identification of biological agents</b></td></tr>
<tr><td colspan="2">There is a need to efficiently and automatically collect samples when emergency responders attend an incident. The collection should not impose additional workload on the first responder. There is also a need to rapidly identify a wider range of B-agents than can easily be done at present. There is a potential synergy with technologies for long-term monitoring exposure of first responders to chemical toxicants.
<i>Recommendation: (i) initiate actions to develop an automatic sampling device which can be attached to/integrated with the first responder protective equipment (e.g. clothing or breathing apparatus), (ii) initiate actions to develop rapid and robust technologies able to identify multiple biological agents. The equipment is preferably small and portable and should not require specialist knowledge to operate. The primary target group includes developers and first-responder end-users.</i></td></tr>
</table>

<table>
<tr><td>200-4/ 210-2</td><td><b>Explosives detection sensors/equipment</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Explosives detectors</b></td></tr>
<tr><td colspan="2">There is a need to rapidly and unobtrusively scan large public areas for the presence of explosive materials, and to rapidly and accurately detect and identify explosive materials at close range. The former equipment may be relatively large and permanent; the latter is preferably small and portable.
<i>Recommendation: initiate actions to (i) further develop existing large area scanning techniques (which may be based e.g. on optical techniques such as lasers, or chemical techniques based on air or water sampling), (ii) initiate actions to develop new, close range techniques for detection and identification of explosive materials, for instance based on spectroscopy. The primary end-user groups include operators of large transport facilities and developers.</i></td></tr>
</table>

<table>
<tr><td>112-2</td><td><b>Digital signal processing technology</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Autonomous large area surveillance</b></td></tr>
<tr><td colspan="2">There is a need to improve current technology for autonomous and large area surveillance to improve detection of anomalous behaviour and relieve human operators from tedious tasks. It is important that the technology preserves integrity of the individual, for which reason non-visual technologies are preferred. It is likely that no single technology is sufficiently robust under all circumstances, so that multiple sensor systems should be integrated in the same system.
<i>Recommendation: continue current activities in the field of autonomous anomaly detection and emphasise integration with non-visual and privacy preserving sensor technologies. The primary target group includes operators of large public facilities, municipal authorities and system developers.</i></td></tr>
</table>

<table>
<tr><td>111-13</td><td><b>Smart textiles</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Smart textiles</b></td></tr>
<tr><td colspan="2">Smart textiles are under development for civilian applications in sports and medicine, but security is not seen as a priority application. There is significant opportunity for synergy to develop smart textiles for security applications in parallel with on-going activities. Useful areas for joint development include small, lightweight and robust energy supplies for integrated sensors, and for development of integrated antennae for short range communication. There is also potential for smart textiles in non-clothing security applications including floor coverings, curtains and geotextiles.
<i>Recommendation: (i) initiate activities to develop small scale and robust power supplies suitable for powering integrated sensors and communication devices, (ii) initiate activities to develop integrated antennae for short range communication, (iii) initiate activities to identify novel security applications for smart textiles. The primary target group includes developers and first responder end-users.</i></td></tr>
</table>

<table>
<tr><td>504B-2</td><td><b>Simulation for decision making (real time simulation)</b></td></tr>
<tr><td>Alternative solution needed for</td><td><b>Real-time simulation tools</b></td></tr>
<tr><td colspan="2">There is a need for better and widely applicable real-time simulation tools to support (mainly) crisis management and emergency responder commanders in their different roles and to help coordinate and prioritize their operations. The need is e.g. to select the optimum route to/from an operation, hospital or other facility, to re-direct traffic in extraordinary situations, etc. and to assist local commanders in prioritising their actions. An example of the latter is to prioritise actions to protect objects/installations with special cultural, monetary, strategic or environmental significance or value.
<i>Recommendation: initiate actions to develop a range of simulation-based decision support tools that help different decision makers according to their specific needs and conditions. The tools need to have a wide applicability and should not be tailor-made for a particular situation. The tools must be flexible and adaptable to different situations. The primary target groups include software developers and a wide variety of end-users.</i></td></tr>
</table>

As previously noted, the STACCATO taxonomy was not originally intended to be used as it has been in this project and in addition to the above critical technologies which can be directly related to the STACCATO taxonomy, the ECTETERA study has identified additional needs and recommendations which are tabulated below.

N/a	**Standards**
Alternative solution needed for	**Standards**

There is a need to establish international standards for many technologies in security applications. Standards are essential to stimulate product development and to allow access to wider markets for manufacturers. Specifically, standards are needed in the following areas: standards for security in communication, standards for security in industrial control and information systems, standards in security against jamming electronic devices and systems, as well as standards applicable to explosives detection.

Recommendation: (i) initiate activities to identify where standards are needed, (ii) initiate activities to establish international standards for technologies in industrial control and information systems, secure wireless communication including future ad-hoc wireless systems, anti-jamming technologies and explosives detection.

N/a	**Security rating**
Alternative solution needed for	**Security rating**

There is need to easily and clearly show how secure a technology, system or instrument is, in a similar way to the energy declarations commonly found on electrical appliances. This would reduce the need for expert knowledge on the part of the operator of any security-related device or system. Concomitantly it would raise the public level of awareness of the need for security in the evermore complex systems in modern society.

Recommendation: initiate an action, e.g. a working group or similar to study the feasibility of posting a security declaration on a wide range of industrial and consumer devices and systems. The primary initial target group includes national and international security organisations but this must later be greatly extended to a wide range of manufacturers.

(Partially) 113-10	**Risk awareness and the cost of security (against jamming)**
Alternative solution needed for	**Hightened risk awareness versus cost of security**

It is clear that risk awareness among managers and operators of wireless systems and some industrial control and information systems is poor. It is also clear that functionality, convenience of use and high speed is often prioritised in wireless devices and systems and that this affects security negatively. Legacy systems may lack security against new threats, and even the vulnerability of modern systems to accidental or antagonistic jamming is poorly known. Public awareness of the risks of jamming even low technology systems (e.g. car locks, home alarms) is low. The technology of anti-jamming which is implemented today is insufficient to protect against threats from organised crime and antagonistic action.

Recommendation: (i) initiate actions to increase knowledge in risk awareness and in the risk-cost balance. The primary target group includes managers in industry, (ii) initiate actions to study and quantify the vulnerability of legacy and modern industrial control and information systems. The primary target group includes developers, suppliers and end-users, (ii) initiate actions to develop anti-jamming technology for wireless systems and industrial control and information systems. The primary target group includes managers and operators, with developers in a secondary group.

5 Acknowledgements

Many people have contributed to this work. We would especially like to thank all the subject matter experts who contributed. We also would like to especially thank Tomas Strandman (SSBF), Beatrix Wepner (AIT), Joachim Burbiel (Fraunhofer INT) and Carlo Dambra (Ansaldo STS) for valuable comments and suggestions. We would like to thank Anders E Eriksson (FOI) and Christian Carling (FOI) for valuable discussion and constructive comments. Any remaining errors and inconsistencies are the responsibility of the authors.