JRC Scientific and Technical Reports

Final recommendations towards a methodology for technology watch at EU level

STACCATO Deliverable 2.2.1

Elisabeth Mrakotsky-Kolm   **(Arsenal Research)**
Gustav Soderlind   **(JRC)**

JRC
EUROPEAN COMMISSION

ipSc
Institute for the Protection
and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

<table>
<tr><td>

Europe Direct is a service to help you find answers
to your questions about the European Union

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

</td></tr>
</table>

A great deal of additional information on the European Union is available on the Internet.
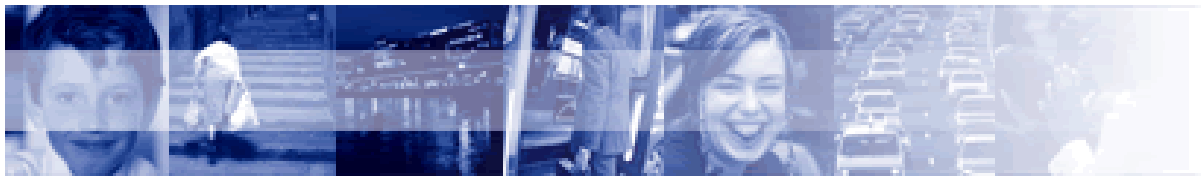It can be accessed through the Europa server http://europa.eu/

Printed in Italy

PASR

**Preparatory Action on the
enhancement of the European industrial
potential in the field of Security research**

SEC6-SA-214200

STACCATO

Stakeholders Platform for Supply chain Mapping,
Market Condition Analysis and Technologies Opportunities

Supporting Activity

**Deliverable 2.2.1
Final recommendations towards a methodology
for technology watch at EU level**

Due date of deliverable: April 28, 2008
Actual submission date: April 28, 2008

Start date of Activity: January 15, 2007   Duration: 16 months

Organisation name of lead beneficiary for this deliverable: Arsenal Research / JRC

Final Version

CLASSIFICATION:	PU

3

Deliverable 2.2.1
Final recommendations towards a methodology
for technology watch at EU level

Table of Contents

1. Introduction

STACCATO co-ordination action under PASR 2006 foresees in WP 2.2. "Methodology for Technological Watch Including Emerging Technologies & Analysis of Importance for Europe", the implementation of a methodology for a global technology watch and monitoring of worldwide trends insecurity-related technology.

WP 2.2 while considering existing mechanisms for technology watch in the European Member States and the US, makes recommendations in order to develop mechanisms for technology outlook and watch in Security Research at EU level.

The term "Technology Watch" is rather generic and can encompass any number of activities for many differing purposes. The meaning used for the STACCATO project is:

"Technology Watch deals with the early detection of emerging technologies and the understanding of what impact these technologies have on specific market applications" and

"Technology Watch for security aims at identifying emerging technologies, assessing their potential relevance to security applications and providing advice on the potential impact of science and technology developments on national and European security and security research policies and strategies."

The present deliverable D2.2.1 indicates final recommendations towards a methodology for technology watch at EU level. Important elements of this deliverable were compiled on the basis of an expert workshop on 'Technology Watch' held in March 2008 in Brussels *(see Annex 1)*. The STACCATO consortium wants to thank the participants of this workshop for their valuable inputs.

2. Executive Summary

The European Union strives to enhance the innovation and competitiveness of its Member States and has in recent years increasingly focused on enhancing the European Security. A European Technology Watch (ETW) would support both these goals, by helping clarify the European Security Industry Structure, and by identifying market growth potentials and deficient industry factors.

The task of an ETW per se would be to observe, track, filter out and assess potential technologies from a very wide field. Life-cycles of new technologies are becoming shorter. As a consequence, the process of introducing them on their way to standardisation must be fast, flexible and practical. In order to cover all thematic fields and lower the risk of missing potentially disruptive technologies, it is suggested to combine 'hard' methods such as literature study with 'soft' methods, such as interviews, expert panels, questionnaires, workshops, etc. The efficiency of ETW will be based on its ability to getting broad input, of varying precision and partiality and reflecting the international bandwidth of innovation.

In order to be truly useful, an ETW must be able to gain the trust and acceptance by all its stakeholders and target groups. Outmost care must be taken to ensure that there is no suspicion of commercial or political bias in its output. The key to this is transparency and impartiality, to meticulously link individual conclusions to their related sources.

Two potential main user groups for a European Technology Watch (ETW)

A crucial step in the creation of an ETW is to clearly define who the users are. The specific user requirements will determine both the form and function of any ETW. There may be large differences between mechanisms required for policy support and those needed for industry support. In order to fill all potential needs this may require several distinct ETWs working in parallel, optimised for differing purposes and using different methods.

Private technology watch mechanisms are already in place by many industry and other market actors, and these may well question or oppose the need for and the conclusions of an ETW. There exist however two target groups that would significantly benefit from an ETW: SMEs and policy makers on the national and European level.

*For the sake of **strengthening** the European **market competitiveness** policy makers* require policy support by ***monitoring developments*** within and beyond the EU to identify important research and innovation areas, offering a comprehensive and realistic picture including the identification of deficient support factors, such as possible regulatory gaps.

Moreover, often the ultimate goal of policy measures is hard to define, as well as which policies will best lead to this goal. For this reason, ***policy impact assessment*** tools and methods for obtaining rapid feedback on the effect of policy measures, and particularly on any unexpected negative side-effects, have a clear value.

Another requirement of policy makers may be the need for ***technology warnings.*** This entails monitoring evolving technologies not only for their economic potential but also for their potential security value or threat, and possibly also their political implications. Technologies that may have negative consequences on society need to be monitored as they appear and mature. Negative effects are here used both denoting a direct threat potential such as e.g. small and effective EMP generators, or more indirect threats, such as disruptive technologies that in themselves are no danger but which when widely introduced may generate new security liabilities unless action is taken early enough to ensure mitigation.

And finally, there is the need to get a ***definition of critical components*** and equipment which could negatively affect European economy and security if internal or external supply was cut off or degraded, i.e. by essential foreign dependencies.

The ***methodology*** of an ETW should not be limited to identifying new potential technologies and services and surveying the current situation, it should also include mechanisms for determining which incentives are most important for stimulating their growth in the European market, which blocking mechanisms there may be in place that would hinder the adoption of the technology, and how to mitigate each blocking mechanism.

The means available for policy makers at the European level to make use of information gathered through ETW and other sources in order to promote innovation and security can range from networking and facilitating partnerships, (i.e. working to bring industry alliances together around common goals and roadmaps, bringing users together around common requirements), to more direct approaches (such as directing research through direct funding, tax incentives, reformulating regulations, promoting the creation and adoption of new standards, and increasing university funding in certain educational topics to increase the human capital available).

Small and Medium-sized Enterprises (SMEs) require more individual support for their respective fields of activity. Mostly, SMEs are lacking the resources to conduct their own competitive technology watch. ETW support would help them keep track of technical developments, find innovative solutions, possibly from outside their primary technical sector, and speed the transfer from R&D to market. They do not only need to know about upcoming technologies but their main interest is technology niches and technology gaps that may offer a chance for their innovative ideas and products.

One specific example of an innovation booster for SMEs can be found in the US Small Business Innovation Research (SBIR) program which provides an opportunity for small, high technology companies and research institutions to participate in Federal Government sponsored research and development efforts in key technology areas.

Special emphasis should be accorded to SMEs coming from the New Accession Countries (NACs). They usually do not work in clusters like Western SMEs do, which makes it harder for them to be integrated and become known market players. Including them in an ETW process would be a way to offer them insight in upcoming developments and make their own competencies visible.

Building a European Technology Watch on existing structures and actors

An ETW should not reinvent the wheel but make use of existing proven methodologies, structures, networks and actors. It is advisable to develop a co-ordinated Technology Watch network with academia, research institutes and other entities, structured according to their technological specializations and with appropriate interactive tools in order to respond quickly to requests for technology feasibility advice, technology performance advice, state of the art, risk assessment, etc.

Additional partners in the network will provide added value by reviewing and assessing the results. In a next step, a steering board should be created in order to coordinate the work and disseminate the results. The steering board could perform meta-analyses, putting together several studies and impact analyses, in order to identify the political implications. As more funding becomes available, studies of all kinds can be commissioned by the steering board, and performed by the ETW partners in collaboration.

Virtually all European countries have for many years conducted Technology Foresight exercises on a national level. The purpose of which has been to determine the expected development of society perhaps 10 years or more into the future as regards health, services, ICT etc, using scenario-drafting and experts consultations. From these estimates it is aimed to develop long range national strategic goals for R&D and other societal important policies. While a Technology Watch for security would have more near term focus, other primary aims, and a different working methodology, the networks established for foresight on a national level could and should be leveraged. They constitute an important link with the national political levels for dissemination of the results, are capable of bringing in a balanced set of regional interest groups as well as constitute a significant labour pool for the day to day activities of the ETW. Coordinating the national efforts will provide advantage to all stakeholders since the combined effort will be able to look wider and yield results not possible on a purely national level without unreasonable effort and expense. Coordination can be achieved by leveraging supranational networks such as the ones formed in ESRIF.

3. General Approach and Rationale

3.1 Policy Support

Policy can significantly accelerate research and innovation by performing an adequate funding scheme for innovative technologies. The right timing and the choice of the right research topics are crucial factors as well as the effective handling of - probably restricted - monetary resources. Thus, policy makers are in need of methods and procedures that allow a structured decision support. Decisions have to be taken with respect to the

- research topics (coping with deficiencies, improving strengths, promoting disruptive technologies, including basic research),

- the level of promotion (e.g. absolute priority for main topics; allow parallel funding in order to achieve rapid progress versus avoiding duplicity and double funding), and

- the optimum timing (early adapting versus benchmark projects).

At this level, it is essential to provide policy makers with knowledge on the **maturity of research topics** in order to allow them a structured approach to the respective decisions.

3.2 Industry Support

If applicable, open market conditions encourage industry to develop innovative technology that can better satisfy existing requirements, strengthen existing markets and give rise to new ones. Particularly in the field of security research these market conditions are not yet established in Europe. As a consequence, on the demand side, buyers have little knowledge about the whole range of available products and capabilities already on the market. An exchange of experience and practice is currently only taking place during selected expert conferences or trade fairs. From the suppliers' perspective, there is not a great variety of customers, but a number of individual organisations (authorities, providers of services, etc.) in need of specific products and solutions.

In this situation, a **European platform** that allows a structured comparison of heterogeneous technologies and an evaluation of their respective maturity levels could help to promote the creation of

a security market. One method to approach this goal could be to make use of publicly available international technology lists or technology inventories, like e.g. the military critical technology list (MCTL) of the United States that addresses military technologies related to dual use and security technology. Those international technology lists could be checked for their relevance and applicability for the European market conditions. At the same time, stakeholders from research organisations and companies working in the various security-related fields should be encouraged to take part in this European platform.

However, a main goal of an ETW in this arena will be to **serve as a tool for** particularly **smaller European companies** (SMEs) lacking the resources to conduct their own competitive technology watch. This would help them keep track of technical developments, find innovative solutions, possibly from outside their original technical sector, and speed the transfer from R&D to market.

Special emphasis should be put on supporting **SMEs** coming from the **New Accession Countries (NACs)** in Eastern Europe. They usually do not work in clusters like Western SMEs do, which makes it even harder for them to be integrated and become known market players. Including them in an ETW process would be a way to offer them insight in upcoming developments and make their own competencies visible.

In this context the **STACCATO database** could become a useful supporting tool for technology watch by reflecting the technologies that are currently developed on the European market and clearly showing the gaps in comparison with the international security market.

The **STACCATO database** was developed as an online tool for mapping the European Security Technological Industrial Base (ESTIB). Organisations working on technologies with security applications, such as SMEs, academia, etc, are encouraged to self register their capabilities online according to the multi-level **STACCATO security taxonomy** developed for this purpose (an extension and improvement of the SENTRE project taxonomy). Registered organisations are given the opportunity to do searches on the contents of the database, thus providing them with a networking tool as an incentive to register. Earlier surveys have encountered the difficulty of keeping the information up-to-date. This method however implies that organisations would have interest in keeping their details updated. End-users are also encouraged to register in the database - for this reason the security taxonomy of the STACCATO database has been expanded with a section covering security missions.

Another important source of information in this context could be the '**INNOWATCH' project**. This FP6 project aimed to assess the efficiency and responsiveness of regional innovation policies through the development of a tool based on technology watch methodologies specifically applied to SMEs.[1]

4. Issues, Target Groups and Partners in a 'European Technology Watch' (ETW)

Issues

A European Technology Watch (ETW) in the field of Security can serve both European end-users (SMEs and larger organizations), and technology providers and integrators. It can also be used to alert European companies to possible emerging threats from disruptive technologies, but it should in no way be abused as a tool for competitive intelligence for large-scale industry.

---

[1] "Application of Technology Watch Methodology for Assessment of Regional-Innovation-Policy Impact on SMEs" (2005-2008, http://project.idetra.com/innowatch/project_results.html).

The well-developed area of "Technology Foresight" and its methodology and mechanisms is not deemed to be of major relevance to the "Technology Watch" as defined by STACCATO - although some aspects of their methodologies can be applied. It bears mentioning that there are a large number of "Technology Foresight" and equivalent programmes in action around the world. Their main purpose is the projection of plausible prospective evolution of technologies or even technology markets, 5, 10, 15 years or even further into the future. These future visions are mainly used as support for identifying strategic research directions. Technology watch offers an important complement to these studies.

European Security policies are highly dependent on science and technology (S&T). The technological basis for both defensive and offensive actions is highly dynamic and specialised. Moreover, many disciplines are involved ranging from natural to social sciences, from ICT to nanotechnologies, from human and social factors to policy, from single technology approaches to integration of technologies in complex systems, etc.

In concrete terms, this means that the user community in the security domain has a need of quick and systematic hands on independent technical and technological advice that is trustful and ensures neutrality and transparency. The *main issues* identified are:

1. *Decision support* on where and how to direct research funding:

   - An ETW has to be trustworthy, both in regards to limiting possible biases in its findings, and in the comprehensiveness of its results. Only if those criteria are met can it be expected that it will be used for support when deciding prioritised research topics and research funding allocation. An example of comprehensiveness in this context is if it can offer a full and realistic picture of the situation, such as the state of the industry, or whether there are bottle-necks in the academic education resulting in too few human resources for any particular new technology to be able to take-off.

2. *Threat identification/ Technology warning:*

   - Emerging technologies may pose a potential threat to the European security on more than one level. Disruptive technologies can grow rapidly, replacing less efficient precursors, and can create new services and markets. This is part of innovation and should be encouraged, but the development should also be monitored in order to identify what new weaknesses/security gaps the technology may introduce into society, in order to be able take action as soon as possible to mitigate possible dangers. A more direct threat which could be posed by new technological developments is the usefulness of technology for antagonistic uses against society or its supporting services. Such technological developments need to be identified, and their maturation progress monitored, in order to support a timely counteraction. The risk should preferably be phrased in political terms, and should also contain information on the estimated urgency of action.

3. *Policy feedback:*

   - R&D policy making is not an exact science, various approaches are available such as tax incentives, directed R&D funding etc. A mechanism is needed that can monitor the progress and directly provide feedback on how efficiently policy is working, and if there have been any unexpected negative side-effects. Poorly designed policy might for example have promoted existing technologies in an important area such as power efficiency, when the original goal was to promote the creation of new and innovative technologies.

Target Groups

It is agreed that Technology Watch effort should start with a clearly defined mission and defined target group. After the concept has been proven successful both the mission and target group may be

expanded. As described above it is suggested that the ***primary target group*** be policy makers at national and EU levels with the objective of decision support, later expanding to support for SMEs especially with the aim of enabling technology transfer.

Partners and possible hinders to the establishment of an ETW

An ETW should build upon and expand on existing networks in the European domain. The original idea was coming from **ESRAB** *(European Security Research Advisory Board, group of personalities)*, consequently the initiative should at best be continued by **ESRIF** *(European Security Research and Innovation Forum)* as a steering entity.

However, it should be avoided that the commercial interest of industry can affect the output of an ETW. Neutrality and impartiality will be a main criterion to gain the trust and acceptance of all players and target groups. There may be actors in the marketplace who - for varying reasons - may be opposed to an ETW and might therefore act to weaken or otherwise influence an ETW effort. Possible actors who would fall into this category are commercial consultancies who offer similar services, but for a fee, and therefore have a direct economical stake in counteracting a public/semi-public service; another opposing category could be industrial lobby groups and associations who may have a stake in tailoring research recommendations to suit their member's economic interests.

In fact there are also appearing private collaborative security initiatives in Europe, focused on acting as intermediaries between industry, government, academia and end-users. Some of these could also substantially contribute to the task of coordinating and hosting an ETW.

One of these initiatives is the ***European Organization for Security*** (EOS)[2]. It has for objective to become the European representative for security solution providers. As a result it may be considered as a candidate for being an important European driver of a Security Technology Watch initiative.

During the ETW workshop it was suggested that an ETW be hosted by a ***neutral body*** such as the ***Joint Research Centre (JRC)***, and consist of a core steering group of eight to ten organisations. These would administer lower level theme/technology specific permanent work groups.

Nominations of other important partners in the network were regional clusters on innovation, public regulatory bodies, interest and lobbying organisations, representatives from venture capital, standardization bodies (e.g. CEN/CENELEC), Government subsidizing bodies, and legal institutions.

The essential point is to get a broad input, of varying precision (and partiality) and the key to transparency and impartiality is to meticulously link individual conclusions to their related source.

5. Methodology

In each field of technology, there is a life-cycle covering the steps starting from basic research to – applied research – product development – product procurement to finally reach market saturation. The maturity of technology is growing along these steps. In the course of growing maturity, certain particular steps have to be taken by various actors within the community in order to benefit from technology development.

---

[2] EOS was established in July 2007 by 25 major private European actors from Industry and Research engaged in the civil security domain in order to address the rapidly growing number of initiatives from both national and European administrations in the framework of the creation of a coherent security market in Europe. EOS aims at acting as a privileged interlocutor between its members (suppliers, operators and users), EU Institutions, national administrations, international organisations and advisory bodies such as ESRIF (http://www.eos-eu.com/).

Generally, within the life cycle we have to distinguish between the ***research phase*** and the ***product procurement phase***.

The challenges of promotion in the *research phase* are stimulating the development of the '*right'* technologies, detecting disruptive technologies, gaining a fore-runner position and consequently establishing competitiveness. At the research level, it is also essential not to forget fostering basic research in order to avoid future technology gaps.

The mechanisms to promote the *product procurement phase* are quality assessment processes like certification, interoperability checks in order to enhance scalability and portability and the establishment of a platform for the exchange of experience and practice.

As a matter of fact no organisation under competition will deliberately publish information related to their customers, emerging technologies or products, strategies, fears, etc. For that reason, it will be hard to gain a valid dataset for technology watch, as participation can only be on a voluntary basis. Encouraging participation may be successful if market participants – i.e. researching bodies and suppliers of systems, components or services – can expect a benefit from sharing their information. In particular there are two phases, when a company/institution is willing to share information:

- During the pre-competitive phase: Researching bodies (RTOs as well as industry) are publishing within academia to make their ideas visible and receive feedback and confirmation from their peers; Applicants for research funding are running through a qualification process.

- During the procurement phase: Suppliers are advertising systems, components or services, outlining features, capabilities, quality, etc.

Thus, the following questions can be raised in order to gain the required datasets for Technology Watch:

1. Who is requesting research funding (national/ EU level) on which topics and when?

2. Which products (stand-alone solutions and products in operational chains) are on the market to support which capabilities at which level of maturity and/or quality?

3. Are there pre-existing international or European inventories on technology available in Security or related areas and are they appropriate to be used for the European market?

Monitoring Processes for timely and up-to-date information

The monitoring process on the datasets for Technology Watch should be a permanent one and will cover mainly the three recommended mechanisms or steps below:

- <u>Utilise processes covering life cycle considerations</u>: This allows assessing up-coming research topics, topics where a community is being built, topics where knowledge on feasibility and time-scales is emerging, topics seeing a decline of participants but being seriously taken over by some "few". The respective analysis is performed by processes like e.g. *Gartner's Hype Cycle Analysis[3]*, giving a global view on technology development. Their

---

[3] 'Gartner's Hype Cycle': A Hype Cycle is a graphic representation of the maturity, adoption and business application of specific technologies. Examples to be considered are e.g.:"Hype Cycle for Emerging Technologies", 2003, Strategic Analysis Report, R-20-4160, "Hype Cycle for Transportation", 2005, G00129024. "Hype Cycle for the Oil and Gas Industry", 2005, G00129922; "Key Technology Advances from 2003 to 2012," AV-18-8822.

main objective is to supply information on the maturity of research topics and to serve as starting points for industrial development.

- Utilise processes covering network analysis: For the assessment of emerging and existing networks of participants within the community. As claimed in JRC's Research Strategy Paper on "Emerging Technologies in the Context of Security"4, the field of security is a very complex environment with a large variety of scenarios, missions/tasks, stakeholders and user interests. Science, research and technological development for security are *capability-driven*, undertaken to support and facilitate day-to-day work of people in security-related activities. Thus, there is a strong need for a *permanent interface* between this wide-spread *user community* and the *technology providers*. Although experience from the military domain provides a good starting point in capability-based research, it is necessary to adapt it significantly to address the specificity of the security sector.

- Utilise processes covering a gap analysis: This permits to assess deficiencies and discontinuities in emerging and existing technologies, capabilities or general market conditions. These processes supply information on the *technology readiness level (TRL)* of the supply side. The main players in this analysis could be experienced senior researchers or experienced end users with an excellent overview on technology and human interoperability. Valuable input for gap analysis can be gained from ongoing or completed European studies or supporting activities, especially those running under PASR, like e.g. *STABORSEC (Standards for Border Security Enhancement)*5. WP 2 of this project treats a prioritised list of missions and technologies in the area of border security. Missing standards and their assessment will be developed and described. Results of STABORSEC (D 2.1) will be made available for STACCATO.

Three key features are essential for the information gathered:

- *Timeliness* which includes not only the amount of time required to deliver the product, but also the usefulness of the product to the target group at a given moment.
- The right *scope* of the information which involves the level of detail or comprehensiveness contained and
- The *periodicity* describing the schedule of initiation and generation of the information.

International and National Examples

For the STACCATO "Technology Watch" several ongoing "type" examples have tentatively been identified as having bearing on various aspects on its working methodology and meriting deeper analysis, for the sake of identifying best practise approaches.

1. The Technology Watch effort by the ***International Telecommunications Union (ITU)***, for the purpose of identifying emerging technologies with high potential and initiating standardization work early.
   Web URL: www.itu.int/ITU-T/techwatch/index.phtml

---

[4] „Emerging Technologies in the Context of ‚Security'", Research Strategy Paper issued in the framework of Science and Technology Foresight, EC DG Joint Research Centre, Institute for the Protection and Security of the Citizen, September 2005.
[5] STABORSEC (Standards for Border Security Enhancement, SEC6-SA-210900), is a PASR 2006 supporting activity started in early 2007 in order to create an inventory of technologies for border security, determine interoperability needs and identify existing and missing specification standards. Information sources of STABORSEC are other European studies and projects, capabilities required to fulfil border security defined by ESRAB and the direct contribution of end-users. The taxonomy established by SeNTRE is used as a reference.

2. The *"Technology Warning"* methodology proposed by the *U.S. National Research Council* in response to the request of the Technology Warning Division of the U.S. Defence Intelligence Agency. The purpose is to identify and classify emerging technologies that may have negative impact on pre-defined vital U.S. security (military) capabilities.
Web URL: http://www7.nationalacademies.org/afstb/tiger_home_page.html

3. The *U.S. Navy research* into *"Text Mining".* In part for the ability to use the method for discovering new cross disciplinary solutions to stated problems, identifying key stakeholders/experts in a topic area, but mainly for the ability to use it to survey and map national and regional research directions and accomplishments, for example for identifying regional asymmetries in research.
Web URL: http://www.onr.navy.mil/sci_tech/33/332/techno_watch.asp

4. The *U.S. National Infrastructure Simulation and Analysis Center (NISAC).* NISAC provides advanced modelling and simulation capabilities for analyzing critical infrastructures and their interdependencies, vulnerabilities, and complexities to help protect theses assets. Simulations are provided that produce accurate forecasts/outcomes for potential policy and regulatory decisions made during exercises, and seminars exploring infrastructure vulnerabilities or identifying second and third order effects of attacks or disruption.
Web URL: http://www.sandia.gov/mission/homeland/factsheets/new06/HSD_SMU_9.25.06.pdf

Moreover, on a *national level*, innovation policies were and are still mainly pursued independently through national programmes: Consequently, 27 governmental initiatives with different structures, regulations and types of resources do exist in parallel. Several initiatives could be identified in relation with technology watch including the *mapping of ongoing national research* activities, programmes, projects, studies, etc. or the French initiative of an annual security technology roadmap review process (*technological roadmap)* established in France in 2005. However, France authorities face a difficulty getting users to participate. One of the reasons may be the users' fear that the government will justify creating new laws and regulations based on the finding's output, so they are reluctant to participate.

6. How can we proceed in the building of an 'ETW'?

In order to bundle and harmonise the existing driving forces in technology & innovation an EU level stimulation will be required. The following next steps can be undertaken based on the recommendations from the experts at the Technology Workshop:

- Pre-define the thematic extension of a Technology Watch initiative in the field of Security and select the most important target groups.

- Undertake an awareness campaign with a task force under the 'ESRIF-umbrella' in order to raise awareness and trust, addressing all relevant players.

- Encourage the building of peer-groups, sharing experience, discussing technology issues, building confidence and setting up the necessary conspiracy to drive the system forward - membership is on a deliberate basis ('Club of the Willing'). Supply procedural information and give assistance in the setup-phase.

- Develop from these peer groups the building of a European Platform, including correspondence groups, governmental bodies, industrial and SME suppliers, research think-tanks, universities, trade-associations, etc. This platform can take over leadership and responsibility on certain

Tech Watch-issues. It is necessary to make clear the national and EU role of this platform and to point out the advantages of becoming an active partner.

7. Conclusions and Final Recommendations

This study highlights the critical role that a dedicated and specialized technology watch focused on security issues could have for public and private actors in Europe. Taking advantage of existing initiatives, but providing that technology watch with appropriate resources and recognizing to it a clear institutional role, it can significantly help policy and business decision makers in dealing with the rapidly evolving technologies and the emerging related markets.

The proper development of the European market would mean having the capacity to satisfy the requirements of the local actors, but also increasing the possibility for European companies to be world leaders. All this will have definite positive effects on the protection of our society, and on its competitiveness.

Therefore, this study concludes that a European Technology Watch (ETW) should become a prioritized issue at EU level. It has already been identified by the group of personalities (ESRAB), mainly for its potential to enable a more focused EU funding for targeted R&D. In addition, the current ESRIF *(European Security Research and Innovation Forum)* working groups have identified the understanding of the technological life-cycle as an essential component.

This is a field where common efforts across Europe and among public and private actors appear to be not only advantageous but necessary. Security is characterized by regulations and significant public procurement; security technologies do not generally provide an immediate productivity gain; standards and regulations can create and shape markets; and the knowledge on security capabilities, vulnerabilities and threats has vital implications for end users for its sensitivity. All these elements underscore the benefits of a joint Technology Watch endeavor.

For these reasons, it should be avoided that the commercial interest of a single industry or industrial sector can affect the output of an ETW. Neutrality and impartiality will be a main criterion to gain the trust and acceptance of all players and target groups.

When considering the current situation, it is apparent that the European Security Market is fragmented, trailing the U.S. Consequently, an imperative common goal for initiating a European Technology Watch is to foster innovation, economic growth and security and make Europe gain a leading role in international security research. An ETW could identify growth potentials and enable early adaptation of research and innovation programs. On the other hand, the effects of policies can be monitored and warnings on side-effects or upcoming vulnerabilities can be addressed. This will promote awareness and interest and lead to an increased end-user adoption of security measures.

The life cycles of new technologies are becoming shorter. By the time it ends up in a published research paper a technology may already be "old". ***ETW needs to*** catch it even before this stage and should therefore ***act fast, flexible and practical*** in order to observe, track, filter out and assess technologies from a wide field.

In order to be efficient, ETW requires a very good understanding of market forces and needs to consider the methods of existing TW efforts all over the world. The findings must conform to the highest possible standards of research. It is recommended to ***build*** a European STW ***on existing structures*** and actors who have already experience in technology reporting and who could be connected in a network. The building of peer-groups could be encouraged, a ***'Club of the willing'***, sharing experience, discussing technology issues, building confidence and setting up the necessary conspiracy to drive the system forward - membership is on a deliberate basis.

From these peer groups a ***European platform*** could be developed, including correspondence groups, governmental bodies, industrial and SME suppliers, research think-tanks, universities, trade-associations, etc. It can take over leadership and responsibility on certain technology watch issues, clearly discerning the national and EU role of this platform.

Such a comprehensive approach of a European Technology Watch (ETW) in the Security area will serve all stakeholders: policy makers and regulators, European end-users (SMEs and larger organizations), and also technology providers and integrators.

The specific user requirements will determine the form and function of any European Technology Watch (ETW), with possibly large differences between policy support and industry support. In order to fill all potential needs this may require several distinct ETW working in parallel, optimised for differing purposes and using different methods.

Specific target groups could be ***policy makers*** and ***European SMEs***. The monitoring of new developments, policy impact assessment and technology warnings will support policy makers in their decisions. Methods should not be limited to identifying new potential technologies and services and to surveying the current situation, it should also include determining which incentives are most important for stimulating their growth in the European market, and which blocking mechanisms should be abolished to make room for its expansion.

SMEs require more individual support for their respective fields of activity. Their main interest is technology niches and technology gaps that may offer a chance for their innovative ideas and products. ETW could help them keep track of technical developments, find innovative solutions, possibly from outside their primary technical sector, and speed the transfer from R&D to market.

In any case we must ***start from a clear mission*** based on a European policy context, like e.g. to address the challenges emerging from the development of the 'European Area of Freedom, Security and Justice', and the development of a 'European Global Stability and Security policy'.

The goal will be to detect, at an early stage, and prospectively shape, scientific or technological breakthroughs, trends and events of potential socio-economic importance, which may require action at a European and/or national decision-making level.

The ***means to reach this goal*** are reliable and accepted scientific and technical methods & tools, not only opinions from single experts.

The ***objective*** will be a common understanding of security issues and the promotion of the European security market establishing **'*Europe as a Security Champion*'.**

8. Annex I: Workshop on Technology Watch, March 5, 2008
Final Report

STACCATO WP2

Workshop results

PART I: General Information

Workshop Title: Technology Watch Workshop

Date: Wednesday 5th March 2008, 10:00-16:00

Place: DG JRC, Building SDME, Room 10F,
                       Square de Meeûs 8, 1049 Brussels

Workshop
Coordinator: Elisabeth Mrakotsky, AR

Partners: Gustav Soderlind, JRC
                       Marcelo Masera, JRC

Date of Report: 2nd April 2008, final report

List of participants:

Name	First Name	Affiliation	e-mail
CARLING	Christian	FOI, Swedish Defence Agency, SE	carling@foi.se
CHOE	Young-Han	ITU, International Telecommunication Union, CH	young-han.choe@itu.int
LAURENT	Frédéric	CEA, Commissariat à l'énergie atomique, F	f.laurent@cea.fr
LEVIN	Magnus	European Defence Agency, EU	magnus.levin@eda.europa.eu
LUIIJF	Eric	TNO Defence, Security and Safety, NL	Eric.Luiijf@tno.nl
MARTINI	Gloria	ASD, BE	gloria.martini@asd-europe.org
MASERA	Marcelo	JRC Ispra, IT	marcelo.masera@jrc.it
MONCALVO*	DARIO	Fondazione Rosselli, IT	d.moncalvo@cotec.it
MRAKOTSKY	Elisabeth	arsenal research, AT	elisabeth.mrakotsky@arsenal.ac.at
RAAB	Christoph	COPURA GmbH, DE	info@copura.de
ROUHIAINEN	Veikko	VTT, Technical Research Centre of Finland, FI	veikko.rouhiainen@vtt.fi
SCHULZE	Joachim	Fraunhofer INT, DE	joachim.schulze@int.fraunhofer.de
SODERLIND	Gustav	JRC Ispra, IT	gustav.soderlind@jrc.it
WIEMKEN*	Uwe	Fraunhofer INT, DE	uwe.wiemken@int.fraunhofer.de
WILLEMS*	René	The Hague Centre for Strategic Studies, NL	renewillems@hcss.nl
WILLIAMSON	Clément	DG ENTR, BE	clement.williamson@ec.europa.eu

* Participation cancelled, but volunteered to contribute to report.

PART II: Workshop content overview

Workshop on Technology Watch

Wednesday, 5th March 2007, 10:00-16:30, Building SDME - 10/F (floor 10, room F)
DG Joint Research Centre (DG JRC), Square de Meeûs 8, 1049 Brussels.

AGENDA

10:00	Introduction to Workshop objectives/structure of the day (Elisabeth Mrakotsky, arsenal research)
10:10	STACCATO – objectives of the project (Gloria Martini, ASD)
10:20	Why do we need a 'Technology Watch'? (Gustav Söderlind, JRC)
10:40	Presentations: _'Best practices in Technology Watch'_ Perspectives from VTT (Veikko Rouhiainen, VTT, FI) Activities at Fraunhofer (Joachim Schulze, Fraunhofer, DE) Technology portfolio in global security (Fréderic Laurent, CEA, F)
11:45	Working Session 1: What are the issues of a 'European Technology Watch'?
12:30	_Lunch Break_
13:45	What is needed to create a 'European Technology Watch'? (Marcelo Masera, JRC)
14:15	Presentation: ITU-T Technology watch function, activities since 2005 (Young-Han Choe, ITU, CH)
16:00	Conclusion and closing comments

Presentations overview:

The following presentations were held:

1) Introduction to Workshop objectives/structure of the day
(Elisabeth Mrakotsky, arsenal research, AT)

2) Introduction to STACCATO (Gloria Martini, ASD, BE)

3) Why do we need a 'Technology Watch'? (Gustav Söderlind, JRC, IT)

4) Perspectives from VTT (Veikko Rouhiainen, VTT, FI)

5) Activities at Fraunhofer (Joachim Schulze, Fraunhofer, DE)

6) Technology portfolio in global security (Fréderic Laurent, CEA, F)

7) What is needed to create a 'European Technology Watch'? (Marcelo Masera, JRC, IT)

8) ITU-T Technology watch function, activities since 2005 (Young-Han Choe, International Telecommunications Union - ITU, CH)

Introductory document:

Why do we need a 'European Technology Watch' (for security)?

The rationales are dependent on the intended user/target: industry, end-users, innovators, policy makers.

The user objective will determine the form and function of any European Technology Watch (ETW), with possibly large differences between policy support and industry support. In order to fill all potential needs this may require several distinct ETW working in parallel, optimised for differing purposes and using different methods.

Policy Support

The European Union strives to enhance the innovation and competitiveness of its member states and lately has increasingly focused on enhancing European security. An ETW could help clarify the European Security Industry Structure, and identify market growth potentials and deficient industry factors.

The following is a list with potential purposes for an ETW for policy support.

- Policy support: By monitoring developments within and beyond the EU an ETW provides policy makers with a complementary tool to identify important research and innovation areas; areas where support is needed due to its security or economic importance for Europe. Some aspects:
  - o Focus on security research should not unduly lead to diminished economic growth in other areas.
  - o Monitoring should be continuous
  - o The effect of R&D projects should be maximised.
  - o When choosing amongst available policy instruments policy makers need a firm grasp of technology, the products and applications. This costs not only time but energy, by coordinating such activity through EU national policy-makers may benefit.
  - o Technology watch should identify how to "legitimise" new technology, e.g. how institutions and society need to be adapted to accommodate it.

- Policy Impact Assessment: Setting policy is done with sometimes unclear understanding of the ultimate goal, and the best methods to reach it. Such selected policies can lead to unexpected negative side-effects. An ETW can serve as a monitoring mechanism, providing continuous feedback on the effect of policy

- Technology Warning: Monitoring worldwide developments which could affect European security negatively when used by antagonists, e.g. cheap GPS Jammers, disruptive technologies with inherent security issues which could create new vulnerabilities when adopted for widespread use.

- Critical components: Monitoring the supply of critical components, and equipment which could negatively affect European economy or security negatively if internal or external supply was cut off or degraded. In short : defining essential foreign dependencies

The methods of an ETW should not be limited to identifying new potential technologies and services and surveying the current situation, it should also include determining which incentives are most important for stimulating their growth in the European market, and which blocking mechanisms that should be weakened to make room for its expansion.

The means available for policy makers at the European level to make use of available information can range from networking and facilitating; working to bring industry alliances together around common goals and roadmaps, bringing users together around common requirements, to more direct approaches such as; directing research, tax incentives, reformulating regulations, promoting standards, and increasing university funding in certain educational topics to increase the human capital available etc.

ETW for Industry Support
The purpose of technology watch can be seen as to gather, process and integrate the scientific and technical information that is useful to economic players in the European economic realm.

The European Security Technology Watch (STW) can serve both European end-users (SME's and larger organizations), but also technology providers and integrators.

A goal of an ETW in this arena could be to **serve as a tool for** particularly **smaller European companies** (SME) lacking the resources to conduct their own competitive technology watch. This would help them keep track of technical developments, find innovative solutions, possibly from outside their primary technical sector, and speed the transfer from R&D to market.

It can also be used to alert European companies to possible emerging threats from disruptive technologies.

(Gustav Soderlind, JRC)

PART III: Results Presentation

Draft Executive Summary - Key aspects addressed in the Workshop

Why do we need a European Technology Watch on Security?

The most common goals for initiating a *European Tech Watch (ETW)* are to foster *innovation, economic growth and security*.

An ETW could identify growth potentials and enable early adaptation of research and innovation programs. On the other hand, the effects of policies can be monitored and warnings on side-effects or upcoming vulnerabilities can be addressed.

Basically, ETW may become a prioritised issue at EU level

- Identified by the personalities
- Increased and focused EU funding for targeted R&D (PASR, FP7 etc)

The European Security Market is fragmented, trailing the U.S. An ETW could

- Promote economic growth
- Promote increased adoption of security measures

Who are the main actors and target groups?
(It was not addressed during the workshop but maybe a prioritization may be necessary. Indeed, these actors do not present the same level of interest nor the would they present the same level of involvement in an ETW process), comment Laurent

The following main actors/target groups have been enumerated:

- EU/National/Regional policy makers
- Industry (the supply chain companies with subcontractors)
- SMEs
- Academia (Universities, Institutes)
- Industrial and research networks
- Regional clusters for innovation
- Public bodies (regulatory etc.)
- Interest/lobbying organizations/associations, venture capital
- Standardization bodies (e.g. CEN/CENELEC)
- Government subsidizing bodies
- Institutions: laws, regulations, routines, culture.

Which existing innovation networks and initiatives could serve as an example?

Several examples were presented, like the International Telecommunication Union (ITU), VTT Finland, Fraunhofer Germany, CEA France as well as national examples of threat identification process/technological roadmap (France) or the structure of Finland's national research program.   For further details see the presentations.

How can we raise awareness of necessity and trust?

- Through an "Awareness campaign", e.g. a task force under the "ESRIF" umbrella. For example, do an ETW on Security ("STW") practical demonstration. Create a formal interest group, with brief duration and concrete results. Run an awareness campaign afterwards, targeted at different groups and adapted to each target category.

- Copy methods from the venture capitalists, they know what political/economic levers to pull to facilitate the introduction of new products/services.

- Be clear on who the customer is, have a clear business plan, and make sure there is consensus in the STW group on what it is you are looking for.

- Target the Ministry of Interior

Foster trust by:

- o transparency in claims,
- o transparency in arguments,
- o transparency in evidence
- o cross-checking of results (peer review)
- o consensus building

- Target groups should be made aware at different 'levels' (according to diverse audiences)

- Install a "*Club of the Willing*"

- Set up an "*Informal Interest Group*" – oriented towards producers

What support can policy makers expect from a ETW?

- Security Technologies solving 'Hot Topics'
- Looking beyond Europe:
    - o USA, Japan, Australia, for innovation
    - o China, India, for markets

- Process of TW should be:
    - o quick,
    - o agile,
    - o adaptable,
    - o life-cycle oriented
    - o by the time it ends up in a published research paper a technology may already be "old"; TW needs to catch it even before this stage

- Threats:

- o Industrial lobby(e.g. EOS),
  - o Consultants (to the idea).

- Decision support on how and where to invest:
  - o reliable
  - o offering a full realistic picture incl. industrialisation & training

- Threat identification

- Identification of Regulatory gaps (indirect incentives to private investments)

- Technology warnings

  - o Risk in political terms.

  - o Information on the urgency of the warning.

  Make sure that the message is tailored into political language (risks/benefits) the politicians and bureaucrats can understand and relate to personally.

  Decide on the scope, should we do the political analysis as well? Should we analyze policy options from a technical point of view?

General Notes

- The Tsunami was given as an example: communications technology can contribute to emergency issues (but requires societal acceptance and trust).
- Policy makers have two main issues.
  - o 1. Care and security.
  - o 2. Money.

  If we show that the STW helps generate economic growth or increase the efficiency of funding (by decreasing the amount of misspent funds?), then it has a chance to be supported. Promote "***Europe as a Security Champion***".
- Look at the US, Japan. Make sure that we don't repeat what they already have done years ago. Or perhaps copy it, if it is working.

Who could be the 'carrier institution'of ETW ?

As a 'natural location' for an ETW workshop participants named the Joint Research Centre (JRC) + a Core steering group of 8 to 10 organisations + lower level, theme/technology-specific work groups.

How can we proceed to a European Tech Watch?

We must *start from a clear mission* based on a European policy context, like e.g. to address the challenges emerging from the development of the European area of Freedom, Security and Justice, and the development of a EU Global Stability and Security policy.

Our goal is to detect, at an early stage, and prospectively shape, scientific or technological breakthroughs, trends and events of potential socio-economic importance, which may require action at a European and/or national decision-making level.

The *means to reach this goal* are reliable and accepted scientific and technical methods & tools, not only opinions from single experts.

The *objective* will be a common understanding of security issues.

Be clear about which blocking mechanisms there are:

- What are the general blocking mechanisms?

- EOS[6] – the European Organisation for Security has for objective to become the European representative for security solution providers. As a result it may consider being the ideal driver of any STW initiative. In this respect, it may see a public driven initiative has a threat for its members.

- Which organisations will see a STW as a threat or competitor? Who can launch a negative lobbying campaign? Who already provides TW services for a fee?

- CEA comment: France has launched since 2005 an annual security technology roadmap review process. However, France authorities face a difficulty getting users to participate. One of the reasons may be the users' fear that the government will justify creating new laws and regulations based on the findings output, so they are reluctant to participate.

Critical aspects from best practice

Young-Han Choe, technology-watch expert from the International Telecommunicatons Union, ITU (www.itu.int/ITU-T/techwatch) critically remarked the need for a *collaborative process for the introduction of new technologies* on their way to standardization. ITU-T is open to all interested parties (members and non-members). Moreover, he stressed that ITU-T needs to act *fast, flexible* and *practical*. They are handling *hot topics* which have been pre-selected in general surveys of new technologies and are submitted to the opinion of their membership (via participation to tech watch symposia, access to reports via web site, correspondence groups, etc.). Finally, Tech Watch reports to the *Telecom Standardization Advisory Group (TSAG)* who decides on how to proceed for the new selected technologies.

Here are some of Young-Han Choes conclusions:

- Life cycles of new technologies are becoming shorter
  → *Need accelerated standardization process*
- Standards-development needs to be market driven
  → *Needs flexible mechanism for identifying new topics*

---

[6] EOS was established in July 2007 by 25 major private European actors from Industry and Research engaged in the civil security domain in order to address the rapidly growing number of initiatives from both national and European administrations in the framework of the creation of a coherent security market in Europe. EOS aims at acting as a privileged interlocutor between its members (suppliers, operators and users), EU Institutions, national administrations, international organisations and advisory bodies such as ESRIF. (http://www.eos-eu.com/)

- Bridging the standardisation gap
  → *Needs evaluation of implications of new technologies for developing countries*
- Standards development is collaborative process
  → *Needs partnership with members and non-members*

Joachim Schulze from Fraunhofer emphasised that the inclusion of end users is difficult, because end users are exclusively *thinking in 'existing technologies'*. So, they would not know about innovation and of course they are occupied with their daily business. Moreover, end users are afraid to even admit the existence of technology gaps, because they do not want to be considered to have problems.

Magnus Levin from the European Defense Agency (EDA) recommended that we first of all define what the security market is, i.e. which criteria we apply for deciding whether an organisation is part of the security market or not.

Frédéric Laurent from CEA noted that there was difficulty in France to get end-users to participate in activities, possibly out of fear that the identification by the government of new threats would lead to additional legal/regulatory burdens being imposed on them.

JRC noted: Do not unduly raise political expectations where you can not deliver. Clearly define which policy making you will support, and how you will do this, using clear procedures and metrics.

Security Tech Watch is just as applicable for Defense Tech Watch, and vice versa, i.e. dual use mechanisms, the defense area may also be a customer.

Due to the fast throughput of technology, by the time it ends up in a published paper it is already "old", TW needs to catch it even before this stage.

Fraunhofer comment: The European Commission might currently be focusing too *much on the market pull* and *too little on the technology push*.

Further comments from participants
(The following comments are reflecting written statements from participants.)

Christian Carling, Swedish Defence Research Agency

Tech watch is a sensitive business, both politically and economically.
Industry and other market actors (e.g. venture capitalists) have their own agenda and will sometimes question or oppose the conclusions of a European Security Tech Watch (STW) function.

The Security Technology market is very hard to delineate
This is in contrast to Tech Watch functions in more precisely defined markets, e.g. telecom.
This means that you will need to observe, track, filter out and assess potential technologies from a very wide field. The filtering is probably the hardest task, but possibly also the highest added value a European STW can provide.

Market factors determine when (or if ever) a technology is mature
Today it is not a steady process of incremental R&D efforts that defines how far a particular technology is from market entry. Some mature technologies fail in the marketplace, e.g. because they lose out in a game of competing standards, others can be a market success while clearly less technologically evolved. The conclusion is that STW requires a very good understanding of market forces.

Do as the Japanese: copy, copy, copy!
Don't invent everything from scratch, copy and adapt. Learn how successful corporations, institutions and nations do TW. And learn how not to do it. Look into how the Japanese Ministry of Trade and Industry (MITI) does this.

Keep a broad, multidisciplinary approach
The findings from a European STW must of course conform to the highest possible standards of research. Also, in order to cover a large ground and lower the risk that you miss some inconspicuous but potentially disruptive technology, you must combine "hard" methods such as literature study etc, with "soft" methods, such as interviews, expert panels, questionnaires, workshops etc. The point is to get a broad input, of varying precision (and partiality) and the key to transparency and impartiality is to meticulously link individual conclusions to their related sources.

Build a European STW on existing structures and actors
To create interest and build confidence in a European STW, you must have something to show from the start. The only way to do that is to build upon and leverage the work already being done by existing institutions.

Start by connecting existing groups doing relevant technology studies into a network of equal partners. Initially, the responsibility for producing STW reports lies on the individual partners.
That way, each partner puts its good name behind the work. The rest of the network provides added value by reviewing the work done.

In a next step, create a steering board that coordinates work and disseminates the results. Further value can be created by performing meta-analyses, putting together several studies, and impact analyses, to identify political implications. As more funding becomes available, studies of all kinds and sizes can be commissioned by the steering board, and performed by partners in collaboration.

Think ahead about obstacles and potential threats against the idea

Don't forget the T in the SWOT analysis. Many factors may impede the success of a European SWT: lack of funding, insufficient commitment from partners, limited involvement and interest from end-users, inefficient dissemination of results, and more. A direct threat against the operation would be pressure from actors in the security arena, that for own reasons will want to suppress, discredit or detract from the results.

PART IV: Recommendations

1. Pre-define the thematic extension of (Security) Tech Watch and select the target groups.

2. Encourage the building of peer-groups, sharing experience, discussing technology issues, building confidence and setting up the necessary conspiracy to drive the system forward - membership is on a deliberate basis.

3. Develop from these peer groups the building of a platform, including correspondence groups, governmental bodies, industrial and SME suppliers, research think-tanks, universities, trade-associations, etc. It can take over leadership and responsibility on certain Tech Watch-issues; make clear the national and EU role of this platform.

4. Workshop participants agreed that in order to proceed in the process of planning and elaborating recommendations for a European Security Technology Watch (STW) another planning workshop would be required. At this occasion a focus could be put on the efficient implication of New Accession Countries (NACs) and SMEs in the Technology Watch Process.

European Commission

Abstract
As part of the PASR 2006 supporting activity STACCATO an investigation into a European "Technology Watch" for security was conducted using amongst other means an expert workshop. This activity was run in parallel to the competence mapping of the security industry and academia of Europe which resulted in a database and separate report (STACCATO Deliverable 2.1.1).

Primary tasks for the technology watch could be 1: policy support: i.e. identifying security areas/topics in need of greater European focus and feedback on outcome of enacted policy; 2: "technology warning", monitoring emerging technologies for possible side effects detrimental to societal security; 3. technology transfer support, particularly for SME's since they are generally not capable of fielding their own technology watch efforts.

A Technology watch effort should be based on one or more already existing stakeholder networks of established European actors in the security arena – a 'club of the willing', containing at least 10 actors from both industry and academia. Such an organisation would need to be relied upon to be neutral and impartial, thus the work process must be fully transparent and open to scrutiny, i.e. with all conclusions traceable to their individual sources. The organisation and supporting processes need to promote speed and flexibility, in particular in order to help accelerate the standardisation process of emerging technologies and solutions.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

Publications Office
Publications.europa.eu