EN

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 23.5.2008
SEC(2008)1957

COMMISSION STAFF WORKING DOCUMENT

REPORT FROM THE COMMISSION

Synthesis of responses

to the Green Paper on detection technologies in the work of law enforcement, customs and other security authorities

Synthesis of responses

to the Green Paper on detection technologies in the work of law enforcement, customs and other security authorities

Introduction

Recognising the important part that detection equipment plays in security, the Commission organised a Conference in 2005 entitled: Public-Private Security Dialogue: *Detection Technologies and Associated Technologies in the Fight against Terrorism*. As a follow-up to this conference, a Green Paper on detection technologies was issued at the end of 2006. The objective of this Green Paper is to improve the common approach to detection technologies by initiating a public-private dialogue, defining the role the Commission should play, and identifying the steps forward. This document summarises the responses that the Commission received in reaction to the Green Paper. This synthesis of responses does not commit the Commission to following up on any of the options outlined below. Concrete policy options on detection technologies may be pursued in specific areas, such as explosives, chemical, biological, radiological and nuclear substances (CBRN), etc.

Respondents

The majority of the Member States, several EU-related bodies, companies and security analysts submitted their answers.

Public sector

22 of the 27 Member States and a regional government from Spain submitted responses to the Green Paper on detection technologies.

Furthermore, 5 EU-related bodies responded to the Green Paper: Europol, the Article 29 Working Party, the JRC-IPSC (Joint Research Centre — Institute for the Protection and Security of the Citizen), the CTPG (Counter-Terrorism Project Group) and the ECAC Technical Task Force (European Civil Aviation Conference).

Private sector

The Commission received 23 responses from individual companies, (research) centres or institutes and 9 from associations or consortia. Additionally, 5 security experts reacted on a personal basis.

Reading Instructions

The answers are divided into two broad categories: public and private sector. The public sector can be broken down into the Member States (MS) and EU-related bodies (EUR). The private sector responses are from individual companies and (research) centres (I), consortia or associations (C) and personal responses (P).

The answers are summarised per category and per question. Not all respondents answered every question. How many respondents submitted an answer is indicated for each question. When speaking of ‘all’ or ‘most’, this is relative to the number of respondents that answered the specific question; it does not refer to the whole body of respondents.

1. Standardisation and security research

1.1 Standardisation

1.1.1. Are common standards needed in detection and related technologies used in the work of security authorities?

18 Member States responded to this question. They saw common, or at least minimal, standards as being useful. The 4 EU-related bodies that answered this question all think common standards are needed. 7 consortia and 17 individual companies or research centres/institutes/institutes answered this question. All believed that standardisation would be useful. 5 security experts responded to this question. All but one supported the need for standards. All stakeholders identified several areas in which standards would be beneficial.

Additional remarks include:

- Legal implications of data exchange must be kept in mind.
- Human rights legislation should be complied with.
- Standards should not hinder new technological development.
- Standardisation is important to safeguard both the integrity and authenticity of data shared between authorities (1 I), and the balance between security and privacy (1 I).

Some remarks were made regarding the way in which to proceed during the process of standardisation:

- Standardisation should be market-led and developed in cooperation with the industry (1 C, 1 I).
- The European Committee for Standardisation (CEN) should prepare and develop standards (1 C, 1 I).
- All stakeholders should be involved (3 I).
- Systems that have proven to be effective can form the basis for the development of technological and operational standards. Standards should be set for the different technologies that (sub) systems of a network are made up of so as to provide a baseline for detection procedures. Well identified requirements and operational capabilities should be taken into account (1 I).

Some observations or reservations include:

- Standardisation should not be only European; the US and Europe should engage in a joint standardisation effort. Ideally, standardisation should be carried out on a global level (2 C, 2 I). In addition, EU legislation should be technology-neutral (1 C).

- Standards pose a problem with regard to who they are designed for: manufacturers or users (2 I).

1.1.2. What standards do you consider to be a priority?

13 MS indicated their priorities. The question was interpreted differently by different MS. 3 EU-related bodies answered this question. 7 consortia or associations, 10 individual companies or (research) centres/institutes and two security experts indicated their priorities.

All stakeholders identified a number of areas and standards that should be considered to be a priority.

1.1.3. What standards lack financial support in the pre-standardisation phase?

4 MS answered this question. One European body said it developed its technological standards out of a budget provided by volunteer Member States. 4 individual companies answered this question. None indicated specific standards that needed financial support.

In general, all stakeholders that responded to this question supported the idea of financial support for the development of standards. Few specific areas for standardisation were considered to lack financial support.

1.1.4. To avoid any duplication and to improve transparency, would a regularly updated list/handbook/searchable database of past, ongoing and planned standardisation efforts in detection and closely related technological fields at national and European level be useful?

Public (MS)

All MS (12) that answered think an updated list/handbook/database would be useful. Secure access needs to be guaranteed.

Public (EUR)

3 EU-related bodies answered this question.

One did not consider a database to be a useful instrument (1 EUR) whereas another thought it could be, although some standards may be too sensitive to be made public (1 EUR). The third organisation recognised the problem of bringing together the end-users of technology. It proposed alternatively that the standardisation body CEN/CENELEC take the lead in standardisation activities (1 EUR).

Private (I & C)

9 individual companies or research centres/institutes/institutes and 5 consortia responded to this question. All responded favourably to the idea of a regularly updated list/handbook/searchable database. One expressed doubts as to the usefulness of a database (1 I).

Private (P)

Five experts responded to this question. All felt the proposed list/database/handbook is a useful or necessary tool (5 P). It would also prevent vested interest groups from agreeing on a standard ‘in secret’ and thereby putting other application vendors at a disadvantage (1 P).

1.1.5. Would you be interested in identifying and exchanging best practice in the use and handling of data and information collected by detection tools in an effort to comply in full with the relevant legislation and rules governing the use of evidence in court proceedings?

Public (MS)

14 out of 16 MS are interested in identifying and exchanging best practices. However, because of differences in legal systems and regulations, a single ‘best practice’ might not be suitable for all MS.

Public (EUR)

3 EU-related bodies answered this question, of which 2 indicated their interest in identifying and exchanging best practice. The third agency said that use of evidence in court was of no interest.

Private (I & C)

4 consortia and 9 individual companies or research centres answered this question.

9 individual companies or research centres and 3 consortia or associations said they were interested. One consortium was not interested.

Private (P)

All five experts would be interested in identifying and exchanging best practice, since compliance with legislation is an important issue (5 P). One expressed doubts regarding whether commercial entities would be interested (1 P).

1.1.6 What would be the best way of identifying and exchanging these practices?

Public (MS)

12 MS and a Spanish region mentioned several methods of identifying and exchanging best practices in the field mentioned above. The three methods most mentioned are:

- expert meetings / working groups;
- secure web portal;
- seminars/conferences.

Public (EUR)

One EU-related body answered that it could play a role by fully supporting these activities.

Private (I & C)

8 individual companies/research centres and 2 consortia provided suggestions. These are:

- A ratification process in which each country specifies where and how the standards are adopted (1 I).
- A European network of excellence on security research involving all the Member States, and responsible for reporting the main research results and their applications to crime prevention at national level (1 C).
- A European Union organisation could be created (1 I).
- Workshops for end-users and technology providers with restricted access (2 I).
- Semi-formal working parties on specific topics, which in turn report to a central management group that disseminates the information (1 I).
- EU and Member States-sponsored forums with private sector involvement. Interaction and cross-fertilisation of ideas with the public and private sector of other nations (e.g. the US) would also be beneficial. ISO standards committees have begun to identify promising technologies and processes. Their efforts will benefit from the support of EU customs and security experts (1 I).
- Establishing public-private partnerships, workshops, either public or private sector-sponsored conferences (1 I).
- Standard tests should be set up and the results disseminated to the relevant parties (1 I).

Private (P)

Four experts answered this question. They suggested the following methods:

- The EU CEN-European Committee for Standardisation could be assigned this task. The results could be disseminated through a dedicated web-site (2 P) and/or an e-guide (1 P).
- A central online reference point (1 P).
- Trusted open and closed environment (1 P).
- Group of personalities brainstorming (1 P).

1.2 Security Research

1.2.1 How should information on security research in Europe be disseminated in order to promote competitiveness while avoiding waste of scarce resources?

Public (MS)

13 MS and a Spanish region answered this question.

It was remarked that the issue of confidentiality and the free market principle should be borne in mind. Overall, it was seen as positive to disseminate information at European level. The mode most mentioned was a separate, secure mechanism or a secure database. A web portal, a network of contacts and a centre of excellence were also mentioned.

Public (EUR)

Two EU-related organisations answered this question. One emphasised the issue of confidentiality when disseminating information on security research. The other stressed the need for a strong central coordination of research efforts and the sharing of information on a restricted basis in Europe.

Private (I & C)

9 individual companies and 7 consortia or associations answered this question. Some respondents remarked that common action and better coordination and information exchange is required at national level, across the European Union (EU) and with other close allies, e.g. the United States (1 C, 2 I). Another agreed that dissemination of information regarding research will be most effective if conducted on a global scale (1 I). One consortium added that there is a need to improve internal EU dissemination in order to increase external EU competitiveness. Moreover, publications should be processed with clearance similar to that of defence research (1 C)

The availability of information on security research is the key factor for a quick and effective answer to the growing security requirements. It is important to underline that security cannot be considered a regional issue: one country's security depends on the levels of security guaranteed in the other countries of the Union (1 C).

One company remarked that this dissemination only applies to research funded by public organisations. In this case, ESRAB would be the obvious coordinator. Commercial research will be driven by need and published as marketing collateral (1 I).

The proposals for dissemination that were put forward mostly suggest creating a database/website, organising workshops or founding a new agency. More specifically, the following suggestions were made:

- The Commission should coordinate EU-funded projects better in order to prevent duplication (2 C, 2 I). At the very least, EU R&D funds should not be spent on technologies that have been developed by non-EU companies. Ideally, a system should be created in which experts from all over the globe are regularly consulted. Moreover, the EU and the US could identify lighthouse security projects in which they could invest jointly (2 C).

- Projects and their results should be readily accessible (1 I). They could be put on the internet (2 I), a web portal (2 C) or in a database (2 I) similar to Medline — along with the standards (1 I). However, security would need to be taken into consideration.

- Information should be disseminated both ‘horizontally’ (between companies in the same sector to boost their competitiveness and develop innovative detection solutions) and ‘vertically’ (between manufacturer companies and users in order to direct research into finding solutions to real life situations) (1 C).

- The currently available information should be categorised and an automated classification system could be devised to classify, label and disseminate new documents, according to the taxonomy (1 I)

- A summary of non-classified information could be sent to relevant parties. Those with a key role (funds, governments, industrial partners) could request further information (2 I).

- With regard to OSINT, the Commission should promote:

  - informal meetings where specific Member States’ agencies exchange notes on best practices in OSINT;

  - a trade fair of OSINT suppliers to enable all agencies to see what technologies and methodologies exist;

  - a website where all European OSINT suppliers are illustrated, broken down by the sub-segment in which they operate;

  - the creation of an In-Q-Tel type of organisation in Europe (1 C).

- A web-based journal (1 I).

- Organise a conference/workshop/forums (1 C, 1 I). Scientists, the industry and law enforcement agencies should take part (1 C).

- Found a security research observatory in which public, private and academic stakeholders take part (1 C).

- Create an independent European body to coordinate the activities of security research between public and private organisations (2 I). Because of the dilemma whether to adopt an open source or a proprietary source approach — as both have their advantages — it was proposed that the open source paradigm be adopted in the field of research, in combination with the creation of a transnational organisation in charge of collecting, testing, verifying, adopting and promoting the most interesting and “secure” solutions (1 I).

- Public national or European organisations could take on this role in consultation with the private sector (2 I).

- A list of recognised security research providers could be developed. This establishes an entry barrier to deter the uncommitted, yet sets the barrier at a level that still promotes competition and potentially collaboration (1 I).

- ESRAB could coordinate dissemination. It has the following advantages:

- – a single point of contact for all involved parties combines security needs, legislator needs, research and industry;

- – access to working and discussions groups should be kept “internal only” due to the security need;

- – participants can be screened / controlled (for instance a “clearance” document is required);

- – functionality of ESRAB is also controllable by the EU (1 I).

Private (P)

Five experts answered this question. The following suggestions were made:

- Academic institutions and non-academia should cooperate to a greater extent so that research results are better circulated (1 P).

- A private-public framework should be set up. Present examples from the USA are In-Q-Tel and DARPA (2 P).

- A central online reference point and a discussion forum or a headline group with subgroups focusing on the different technologies and their implications and restrictions should be set up (1 P).

- Central authority with regional offices (1 P).

2. Needs and Solutions

2.1 Technological needs and solutions

2.1.1 Are you interested in a broader debate on the role of detection technologies and the influence their use potentially has on European societies?

Public (MS)

15 MS were interested in a broader debate on the role of detection technologies and the influence their use potentially has on European societies. It was emphasised that human rights should be safeguarded when using and developing detection technologies. In some areas, such as aviation security, this debate is ongoing.

Public (EUR)

Two EU-related bodies responded to this question. One indicated its interest in such a debate, while the other emphasised that, when considering the European economic interests of detection, the right balance should be struck between security needs and European values.

Private (I & C)

11 private organisations and 4 consortia replied to this question. All but 1 association were interested or very interested in the debate.

Such a debate was considered important for the following reasons:

- to strike the balance between security and legal demands versus individual rights (5 I, 1 C); and to communicate this to the industry. Detection technologies and related issues such as interoperability and data sharing should be discussed, as should the impact on societies that interact with Europe (1 I);
- to investigate the role of detection technologies in the context of Homeland Security (1 I);
- to address concerns regarding the use of detection technology (1 I);
- to improve the European Research dialogue on detection technologies (1 C);
- to address the role of detection technology in supporting staff: how to enhance human capabilities by utilising the potential of technology (1 C);
- because the evolution of (cargo) security should take account of the effect it has on societies, including its effect on commerce, public health and safety, and personal privacy (1 I);
- because of interest from a marketing corporate citizenship and strategic evaluation stance (1 I);

- because only by continuous consultation will there be a complete match between what the public authorities need and what the private sector can offer (1 I).

It was also remarked that some needs or topics should be discussed in a restricted context to avoid, for example, availability of detection thresholds to the general public.

Private (P)

Five experts answered this question. All said they were interested in the debate. Both the balance between security and civil liberties and privacy (3 P) and the social and moral impacts that technological innovation has were mentioned as topics of specific interest (2 P).

2.1.2 In what specific areas do the relevant security authorities require technological improvements? Please specify the level of priority in relation to specific needs.

17 Member States, 3 EU-level bodies, 10 companies and research centres, 4 consortia/associations and 5 experts answered this question. Several specific areas were identified.

2.1.3 Is there a gap between requirements for detection capabilities and the technology currently on offer on the market?

In general, stakeholders identified several areas where improvements could be made.

Public (MS)

The 13 MS that answered were divided on the issue of whether there is a gap between requirements for detection capabilities and the equipment currently on offer on the market. Six were of the opinion that equipment is available, albeit at high cost. The other seven Member States felt there was a gap. This gap is mainly caused by the invisibility and shallowness (specificity) of the market. The latter is partly related to differences in legal frameworks.

Public (EUR)

2 EU-related bodies answered this question. One feels there is a gap. The other thinks there is technology on the market that can fulfil the requirements, albeit at high cost.

Private (I & C)

11 private companies and 4 consortia answered this question. Answers can be grouped into three categories: ‘Yes’, ‘No’ and ‘In Between’ (Perhaps/Depends).

One company thought there was no gap, as it had never encountered requirements from clients it had not been able to meet (1 I).

Most respondents (7I & 2 C) thought there was a gap. 2 companies or research centres/institutes and 1 association stated that this depended on the segment of the market considered (2 I and 1 C).

Private (P)

Three experts answered this question and all of them agreed there was a gap.

2.1.4 What are possible solutions to these gaps?

Public (MS)

6 Member States proposed solutions to bridge the abovementioned gaps.

The main solutions proposed are:

- (European) standardisation/harmonisation to increase the size of the market (making it less selective and more visible);
- exchange of information and increased interaction between users and producers;
- funding and stimulating research (new research, ongoing research and the transformation of research results into products).

Public (EUR)

One organisation proposed investing in coordinated research on new technologies at a multilateral level within Europe to obtain a good balance between detection capabilities and costs.

Private (I & C)

3 companies and 2 consortia answered this question. One company thought there are no obvious solutions to these problems with the present technologies (1 I).

Others proposed the following:

- Solutions have to be both operationally and technologically based (1 I).
- A working group of experts could give an overview of what is missing. Both major players and smaller businesses should be involved (1 C).
- Providers could propose easy to use materials (plug and play, etc.) to end-users (1 I).
- A possible solution to filling the gaps is both to integrate available technologies and to undertake research into future new technologies. Technical evaluation by reference centre is essential to help purchasers take an informed decision. However, the detailed plan of technological solutions addressing a specific threat is confidential. Fast detection of some of the most dangerous biological threats identified already exists. The cost-effectiveness of these solutions will depend on the size of the market (1 C).

Private (P)

Two experts offered a solution:

- Making the technology producers work alongside the Institutions and Public Administrations in order to focus better on current efforts, particularly in the phase of defining requirements and analysis (1 P).

- Offering an open, readily accessible public forum in which any solution provider can present their technologies to the authorities. It is important to engage all the possible stakeholders simultaneously so as to arrive at a practical solution that meets all requirements (1 P).

2.1.5 In what specific areas does the private sector already offer, or plan to offer technological solutions? Please state the timescale for when such solutions would be available, and cost-effective.

Public (MS)

In general, specific areas were identified.

5 MS answered this question. One said that the private sector did not yet offer solutions. While one said it could not provide a specific list, another specified some of the areas. Yet another stressed the importance of a cost-benefit analysis. Another MS highlighted the higher interest of the private sector in one particular area.

One EU-related body answered that, in one particular field, manufacturers in the private sector continuously develop new equipment (often with government funding) and launch it on the market.

14 companies and 3 consortia responded to this question. Several made general remarks; others highlighted specific technologies or applications. Three experts believed that private technological solutions were available on the market at different levels of development (2 I). Market analysts forecast that the sector of detection technologies is one in which much research will be done and many solutions will appear in the coming years (1 P). Furthermore, several areas were mentioned as being the most innovative.

2.1.6 Would it be helpful and useful to create a Europe-wide searchable list/database containing specific areas of needs of the relevant security authorities, and at the same time solutions offered by the private sector?

Public (MS)

13 of the 17 MS that responded were supportive of the idea of a European database. One doubted the additional value over existing databases and exchange mechanisms. The following views were expressed several times:

- It is important to identify the needs of users (so that the market can respond).

- It is important for users and producers to communicate.

- The database should be able to guarantee security/confidentiality of the contents and access should be restricted to authorities and relevant (private) partners.

Public (EUR)

4 EU-related organisations answered to this question. One supported the idea; the others raised questions or preferred other ways of bringing producers and end-users together.

The agency that opposed the proposed database suggests a website containing case studies in which people share their experience regarding a technological solution they have used. Another would like to see first how the database would work. Safeguards, such as the transparency of decisions regarding which solutions to include, should be put in place. The organisation that supported the Green Paper's suggestion remarked that a sufficient volume of potential buyers is important for the development of technology. Searchable lists could play a role in this. Confidentiality issues should be addressed, of course. Where the area of interest is very specific, however, the agency proposes the establishment of a task force (like the ECAC technical task force). The fourth agency supports the idea of the creation of a Task Force. This Task Force – in which the private sector should be involved to a certain extent – would oversee the different application areas, identify obstacles and communalities and duly inform both sides.

Private (I & C)

15 private companies/research centres and 7 consortia/associations responded to this question. 5 consortia and 10 companies supported the idea of a secured EU-wide database. 8 companies and 1 association provided alternative solutions. More specifically, 3 companies and one consortium both supported the database and provided alternatives; 5 companies and 1 consortium only provided alternative solutions.

One company explicitly opposed the idea, having doubts regarding attempts by governments to interfere with private companies' product development. It said that companies are perfectly capable of identifying the needs of the market, even when the market is made up of the public sector. It feels government or EU interference with research and product development in the private sector may in fact lead to investment errors and consequently wasted resources. It therefore advises against the idea of EU harmonisation of private industry's development of control and detection technologies (1 I).

Remarks that were made by those in favour of the database:

- Access should be well protected given the sensitive contents of the database (1 C).
- Updating and implementing such database will be costly. Moreover, it is questionable to all intents and purposes who the central authority should be (1 I).
- It will give oversight of the real needs while maintaining competitiveness among manufacturers. In the event that the Commission provides financial assistance, it must be researched how the initiative can boost the competitiveness of European Industries (1 C).
- The availability of a Europe-wide searchable database is the right way to promote public and private sector dialogue and it can be the source of identifying guidelines in the security research domain (1 C).
- A database for Member States to identify what analysis tools or methodologies exist, and to create a list of the equipment available, is useful. Similar work is

currently being done by DG ENTR in the Defence Industry Field (MEDI study — Mapping of European Defence Industry (1 I).

- We should include present and future needs and solutions to this database and establish priorities (1 I).

- Steps should be taken to ensure that innovation is not stifled by the development of stringent standardisation (1 I).

- Such a list/database is valuable, but it should be global (1 I)

- This would be a good way of stimulating development of the required solutions and might be an attractive marketing investment for some providers. It has to be verified, however, whether setting up this database/list does not overlap with any existing initiatives. Moreover, the security of the requirements might be a concern for the commissioning authorities if the database were freely available (1 I).

- It would be a helpful tool for offering existing solutions and developing new ones. A list of solutions may be of use if capabilities are reported fairly and the presentation of strengths/weaknesses and capabilities has been well thought through (1 I).

- Such a list/database would be essential to match the capacity to prevent and to respond to an attack while identifying multiple threats (1 C).

- This initiative would be useful, but only under strict conditions. First of all, this database should be accessible to all technology vendors, irrespective of whether they are European. Excluding non-European vendors would deprive EU public authorities of the opportunity of using technology that might be already available elsewhere. At the same time, however, this database must be closely protected, as it would contain much security- and commercially-sensitive information: if the integrity of the database were not guaranteed, technology vendors would probably not participate (1 C).

- It would be useful for both research organisations and security organisations. It could be hosted on an appropriate website. A global approach is needed however. References/links to wider global equivalents would be beneficial, both for cross-fertilisation and for access to solutions that exist already outside the EU (1 I).

Private (P)

Five experts answered that this would be helpful. It would help identify priorities for a developing new market (1 P). The private sector could also make suggestions for threats that might not yet have been recognised by the authorities (1 P).

If not, what other solutions would you propose in order to improve the information flow between those who need technological solutions and those who offer them?

Public (MS)

4 MS provided the following comments:

- A secure website could be an alternative.
- Interconnection of existing databases could be a subsequent step after a European database.
- It is important to look to the future and invest in anticipated needs.
- Other, existing initiatives, such as the ESRP, should be involved.

Public (EUR)

(See previous question)

- A website containing case studies drawn up by users.
- A public-private Task Force.

Private (I & C)

3 companies and one consortium both supported the database and provided alternatives; 7 companies and 1 consortium only provided alternative solutions (see also above).

Alternative solutions:

- There is a need for better interaction between users and producers/researchers. Users from specific sectors should coordinate and compile their needs, after which they can enter the dialogue with producers. The EC could facilitate this coordination. Moreover, an inventory should be made of methods and equipment that have been tested for specific tasks. Presently, compilations mostly just include producers´ information but the users would need comparisons and evaluations (2 I).
- There exists unfortunately a real distortion between the available technological offer on the market and the knowledge thereof by the security services. The solution would be more ‘exchanges’ and the setting-up of mechanisms that make suppliers and users of technology familiar with each other’s activities. These exchange mechanisms could be institutionalised by the creation of a European agency for security technologies that would propose different tools (questionnaires, supplier-user workshops, websites, etc.) in order to devise a road map (1 I).
- A working group on CBRN detection technologies could be set up to improve public-private dialogue and to design future standards (1 C).
- A science portal where users and/or providers can enter their needs and their offers could be set up. There may, however, be some constraints regarding EU directives on procurement and constraints regarding secure information (1 I).

- Publication of a study identifying European companies producing technologies of use in OSINT, to establish ´a map´ of European industrial interests. At the same time, MS should be encouraged to produce a common list of required functionalities in order to understand what is needed (1 C).

- Creating a bidirectional flow of information to close the gap between security organisations and private companies working in security technologies. The flow could be implemented in this way:

  – From firms to organisations by using a web portal where firms can advertise their solutions using a defined classification. Private companies will have the advantage of using free advertising space for their solutions.

  – From organisations to firms by using periodic communications to explain their needs and requirements. The portal and the data inside will be protected by secure access (1 I).

- The WCO (World Customs Organization) currently maintains a database of available systems. It would be valuable to add an assessment process to this database so that users can benefit from an independent analysis of these solutions (1 I).

- The traditional mechanism is that the managers responsible on each side take note of what is going on in the market. Trade journals and exhibitions are the main channels for communication (1 I).

- A database for Member States to identify what analysis tools or methodologies exist; and the creation of an inventory of what is available. A similar initiative is currently being deployed by DG ENTR in the Defence Industry (MEDI study — Mapping of European Defence Industry (1 I).

- The information flow should be promoted at two levels: procedural and technological. In the first instance, the information flow among public institutions can help to define the baseline of procedural standards. Subsequently, the operational specifications in terms of process flow and detection performance will determine the minimum technology requirements needed to accomplish the standards, and also the validity and completeness of the technology available on the market.

- Organisation of meetings and seminars for end-users and the private sector (1 I).

- Successful processes and technologies will be introduced either directly as de facto standards, or through official standards issued by bodies such as the ISO or EU CEN.

- Given that supply-side fragmentation is one of the problems, the Commission can help by establishing a sub-group focusing on OSINT issues to encourage large companies to act as systems integrators, as they have the scale to bring together small technology providers, while being mindful of the need to grow smaller innovative businesses and to protect their IP (Intellectual Property rights) (1 I).

Private (P)

Two experts responded to this question. The need for better interaction between those who need and those who offer technological solutions was emphasised as a critical point that is often overlooked (1 P). Two methods of interaction were proposed:

- Appoint a board (like ESRAB) responsible for defining a platform for detection technologies and a searchable database (1 P).
- Create an open, unrestricted forum. It is crucial, however, to discuss the needs with end-users and not, for example, policy-makers. Moreover, it is important to include SMEs (small and medium-sized enterprises) who may have problems overcoming the bureaucratic hurdles that official tenders bring with them (1 P).

Versatile Solutions

2.1.7 For what existing tools and equipment could the applicability and effectiveness be improved by enhancing their versatility?

Public (MS)

11 MS answered this question. The types of answers differed greatly. Possibly versatility was understood differently by different MS. Some MS underlined the benefits of versatility in terms of, for example, efficiency. Others mentioned specific tools that would benefit from versatility. Yet others mentioned the substances to be detected. One MS pointed out that detection tools had specific applicability and were not particularly useful for other purposes.

Public (EUR)

One EU-related body observed that equipment that has already been developed in one area (e.g. aviation security) can also be of use in other areas.

Private (I & C)

9 private companies and one consortium answered this question. 5 companies and 1 consortium provided suggestions for tools that would be more efficient when versatile.

One company remarked in general that poor knowledge of the operational capacity of equipment can lead to redundancy and unfortunate financing (1 I). Two companies questioned the value of versatility. One doubts the efficiency of versatility as a minimum time is needed to reconfigure a deployed solution to face new threats without decreasing security (1 I). Two companies stated that an increase in versatility may lead to the eclipse of some technologies; it is sometimes better to have a multitude of equipment, each covering a specific threat extremely well, than one machine handling them all reasonably well. Varying detection thresholds based on threat levels can be dangerous too, as terrorist may adapt their strategies accordingly.

Private (P)

Three experts responded to this question. They believed all equipment would benefit from versatility (3 P). It was also remarked that the versatility of tools must be enhanced through a modular approach to the software architecture used to manage these tools and equipment (1 P).

2.1.8 What new versatile tools and equipment are needed?

8 Member States answered this question and specified details. One EU-related body, 6 companies, 2 associations and two experts provided suggestions for new versatile tools.

In general, end-users should not specify technology, but rather prepare statements of capability and desired effect. Better training on current technological solutions should be provided by end-users to the operators of detection systems (1 P).

Portable and mobile solutions

2.1.9 What existing tools and equipment could be better and more effectively used in the work of the relevant security authorities if they were mobile and portable?

Public (MS)

14 MS answered this question. All agreed that mobility and portability of tools increase their usability and effectiveness. A minority felt that most mobile tools were already on the market. Others mentioned various tools that would specifically benefit from mobility.

Public (EUR)

One organisation answered that portability will enable equipment developed for the airport environment to be deployed in other areas, e.g. mass events.

Private (I & C)

8 Companies and 4 consortia or associations responded to this question.

One company responded that mobility is not always possible. Moreover, it tends to be the case that systems work better when they are not mobile. Compromises on detection/reliability tend to be made when mobility is increased (1 I). Another said that since the demand for portability was growing, Europe should participate in research concerning new detection tools, particularly as applied to mobile solutions (1 I). One company considered that most military equipment could be used for civilian security after some adjustments (including mobile and portable solutions). On the other hand, for security reasons, it may be difficult to transfer military technology to civilian use (1 I).

When considering the deployment and procurement of mobile and portable tools, the overall objectives need to be taken into account. Detection technologies are just one component in the system of solutions. Furthermore, the working / hosting environment needs to be considered, in terms, for example, of spatial and power requirements (1 I).

Private (P)

One expert also made concrete suggestions.

2.1.10 What new portable and mobile tools and equipment are needed?

Public (MS)

10 MS answered this question. They felt that there was a need for new mobile tools and that most, if not all, equipment could benefit from mobility and portability.

Public (EUR)

2 EU-related bodies responded to this question. They mentioned several examples of equipment and tools.

Private (I & C)

6 companies and 1 consortium answered this question. One respondent stated that the focus should be more on components that make mobility possible (like low consumption components, light and high power energy source, robustness of the equipment, easy to use equipment) than on mobile and portable equipment as such (1 I). Another added that the heaviest, most expensive and most immovable components of a security installation should be looked at to explore how these can be made transportable or virtualised in some way (1 I). A number of other concrete suggestions were made.

Private (P)

Two experts gave their opinions and suggested several types of equipment.

2.2 Interoperability of systems

2.2.1 What systems need improved interoperability?

Public (MS)

14 MS answered this question. All believed that interoperability or at least the possibility of exchanging data between systems is important. The need for databases and data systems of EU national authorities to be able to communicate was what Member States mentioned most. Possible legal constraints were acknowledged. Other specific systems were also mentioned.

Public (EUR)

3 EU-related bodies answered this question. One declared that all EU security information systems should be made interoperable, as should process-orientated systems that provide support to workflows. Another identified the need for interoperability between complementary detection equipment to enhance the detection capabilities of screening systems while reducing false alarm rates. Yet another stressed the importance of interoperability of equipment between agencies and States.

Private (I & C)

14 companies and 4 consortia reacted to this question.

The following remarks were made with regard to interoperability:

- Interoperability is one of the main requirements for detection systems because of the presence of vertical platforms, which are currently not interoperable (1 I). On the other hand, interoperability should not be overdone (1 I).

- Interoperability must be investigated at three levels: network, application and data management (1 I).

- Interoperability is fundamental to the success of both national and pan-European security and law enforcement activities; without true root and branch interoperability, European Authorities will fail in their responsibilities to protect citizens (1 I).

- Interoperability has two sides: technology and behaviour/culture. In terms of technology, IP (Internet Protocol) could function as the universal technology to enable authorities to work together. Common standards of processes and behaviour, however, are more important. Without mutual confidence that all are working with the same high standards, exchange of information will not take place. The benefits that can be accrued from real interoperability possibly outweigh the outcomes from all other potential activities (1 C).

- Another company divided interoperability into operational and technological interoperability. Operational interoperability consists of vertical (from local up to transnational levels) and horizontal interoperability (different institutions sharing the operation within a physical subsystem). In terms of technological interoperability, IP networks have been able to overcome some of the issues. However, some system components continue to need improved interoperability:

  - operational workflow among security organisations;

  - sensor information of diverse nature (sensor fusion);

  - COMMON fusion data models;

  - Executive Information Systems (EIS);

  - inter-application and inter-application communication protocols (1 I).

- For commercial reasons, it has proven difficult to get vendors to put data in formats available to other companies. If such cooperation or common formats of data are required, it may be necessary to regulate or legislate common data standards (1 I).

- Many current detection technologies and their support systems have limited interoperability. However, types of middleware infrastructure exist that can facilitate interoperability and accessibility of these systems with each other (1 I).

- All systems should improve interoperability (1 C).

Private (P)

According to two experts, all systems need interoperability. However, interoperable databases are what is most urgently needed (2 P).

1.1.6. **2.2.2 Would a study on legal and other constraints for interoperability of systems across the EU be useful to identify limitations?**

Public (MS)

14 Member States answered the question. All thought such a study would be useful, to serve as a basis for either agreements, common standards or even legal harmonisation. Privacy and data protection principles should be kept in mind.

Public (EUR)

Two public bodies answered this question. Both supported the idea of such a study. One pointed out that it would shed light on the full potential of the systems. The other highlighted the importance of legal safeguards and data protection principles when establishing interoperability; the fact that access to or exchange of data is possible may become a powerful drive in itself for de facto accessing or exchanging data.

Private (I & C)

9 businesses and 3 consortia answered this question. 8 companies and 1 consortium thought a study of this kind would be useful. One company believed that the study would be too broad, and thus its value would be questionable.

One consortium proposed a way of identifying interoperability issues regarding the use of OSINT (Open Source Intelligence): by making a model of what steps (modules) must be taken to move from information to intelligence, the ‘fault lines’ between technologies can be identified. Subsequently, a matrix can be devised to locate all European technology suppliers that play a role in each module. The Commission could inject the model into a wider industry debate to make sure all constraints are identified (1 C).

The following remarks were made with respect to the suggested study:

- Studies of legal constraints (especially intellectual property) would help to ensure the definition of open standards and studies of technical and business constraints would help to ensure effective, practical interoperability (1 I).

- The study could take profiles based on legal and organisational constraints as a starting point. These profiles could be implemented using Role-Based Access Control (an approach to restrict system access to authorised users) to make sure that legal requirements are met (1 I).

- Apart from investigating the interoperability of systems, the constraints between European countries should be addressed (1 I).

Private (P)

Five experts responded to this question. Four answered that such a study would be useful (4 P). The fifth expert stated that it probably would, as most (but not all) systems are usually designed to meet a local requirement, not an EU-wide one (1 P).

2.3 Integration of information from different detection technologies and improved data analysis.

2.3.1 In what areas do you believe that the integration of information from different detection technologies would improve overall performance?

All MS (12) that answered this question felt that the integration of different detection technologies would improve overall performance. 3 EU-related bodies responded to this question, one of them saying that data minimisation and purpose specification should be built into data analysis systems so as to prevent unrestricted data matching and database navigation. 9 companies and 3 consortia answered this question. Three experts responded to this question.

Answers from stakeholders identified several specific areas that would benefit from the integration of information of different detection technologies.

2.3.2 In what areas are improved data analysis techniques required?

10 Member States, one EU-related body, 7 companies or research centres/institutes and one association responded to this question. Four experts also shared their views. Stakeholders identified concrete themes which required improved data analysis techniques.

3. Use and certification of equipment and tools

3.1 Best practice and the use of existing tools and equipment

3.1.1 What would be the best way of identifying and sharing best practice in this field?

Public (MS)

10 Member States and one Spanish region answered this question.

The ways most mentioned of identifying and sharing best practices are:

- expert conferences, meetings and seminars (5);
- web portal or database (6);
- working groups (3);
- (experts) exchanging information and experience (3);
- operational cooperation and contact with experts in the field (3).

Public (EUR)

3 EU-related bodies answered this question. One of them suggested a web portal as a tool for systematic information exchange; another proposed a regular exchange of information in a well-organised structure. This would provide an overview of all the information to be maintained. The structure could take the form of working groups of security experts representing both governments and the private sector.

A third body would like to see the processing of personal data minimised as part of best practice.

Private (I & C)

10 companies and 5 consortia responded to this question.

General remarks

- Best practice should be identified and shared within each sector rather than at overall national level (2 C). Best practices must include aspects relating to human resources and training where these involve demonstrating vigilance and watchfulness to counter terrorist risks (1 C).
- Best practices are only relevant to the extent that users have the same setting, goal and aim or use is not affected by these factors (2 I).

Specific Suggestions

Interactive

- Common tests and exercises where practitioners directly interact and exchange experiences in the field. Projects should be funded for the testing and evaluation of methodologies and equipment (1 I).

- A forum where representatives of different governments with different expertise come together (like ECAC TTF in the area of aviation) (1 I).

- User forums, discussions and newsletters (a secure environment must be provided) (1 I).

- Conference/workshop with representatives from all relevant areas (science, industry, public sector) (1 C) / End-users workshop with feedback to technology or solution providers (2 I).

- Peer review among representatives of different organisations to examine best practices(1 I).

- Construction of a secure wiki-based site for knowledge sharing across multiple agencies, services and countries (1 C).

- To raise awareness of how OSINT can serve different areas of civil security:

  - informal meetings where specific Member States agencies exchange notes on best practices in OSINT;

  - a trade fair of OSINT suppliers to enable all agencies to see what technologies and methodologies exist;

  - a website where all European OSINT suppliers are illustrated, broken down by the sub-segment in which they operate;

  - the creation of an In-Q-Tel type of organisation in Europe.

‘On paper’

- Articles in a relevant magazine (1 I).

- ESRAB can identify and disseminate best practices (2 I), for example by way of a website / project database /mailing list, accessible for “cleared” participants only (1 I).

- Creation of benchmarks to validate a best practice or solution (1 I).

- Root cause analysis of threat resolutions to introduce feedback into the organisation and verify that the identified best practice responds to all the identified threats (1 I).

- Creation of a capability maturity model to assess the level of maturity and quality of best practices (1I).

Private (P)

One expert suggested paying more attention to suggestions from frontline officers and personnel, who have specialised knowledge (regardless of their rank), and giving such officers a forum in which to share their ideas with colleagues from other Member States and with the solution providers. Another expert wished to see more meetings of experts and groups of personalities.

Identification of best practice

3.1.1.1. Would it be through peer evaluation or questionnaires sent to the Member States?

Public (MS)

12 Member States and a Spanish region answered this question.

Peer evaluation (7) and questionnaires (9) were seen as equally valid methods for identifying best practice by the majority of the MS. Several other formats, such as those mentioned in the previous question, were repeated. The idea was put forward to create a database to collect best practices that will ultimately result in a 'European Standard'.

Public (EUR)

Two public agencies responded to the question. One indicated a preference for questionnaires. The other stated that, aside from peer evaluations or questionnaires, a well organised structure (such as mentioned in the previous question) should be established. Certification is a highly technical activity with grave consequences if not done properly.

Private (I & C)

5 private entities responded to this question. All had a different view.

- Neither evaluations nor questionnaires should be used (1 I).
- Questionnaires or feedback forms could be used to report usability issues on tools and equipment. An organisation should be established to collect and disseminate results (1 I).
- The most appropriate mechanism, whether peer evaluations or questionnaires, should be global and needs to be considered on a case by case, or theme by theme basis (1 I).
- Peer evaluation is the best solution, although questionnaires could be used as a first inventory (1 I).
- The best way is through meetings (1 I).

Private (P)

Four experts identified peer evaluation as the preferred method (4 P). One added that peer evaluation would also make it possible to define the best benchmark against which to validate tools and equipment (1 P).

Dissemination of best practice

3.1.1.2 Would it be through a secure and searchable database or through meetings and seminars?

Public (MS)

13 Member States and a Spanish region answered this question. The secure and searchable database (11) was the slightly preferred option over meetings and seminars (8). Many MS thought both methods were suitable.

Public (EUR)

Two public bodies responded to this question. One preferred sharing experience through meetings, seminars and documents produced by working groups. The other favoured a secure and searchable database of jointly assessed case studies.

Private (I & C)

7 companies and 3 consortia gave their opinions on the dissemination of best practice.

Searchable database (1 I)

- Meetings and seminars are too costly in terms of time. The prime source should be a searchable database with seminars and exhibitions as a secondary source (1 I).

Meetings and seminars (1 C, 4 I)

- Meetings and seminars establish a real network (1 C) and avoid poor translation problems (2 I).
- Meetings and seminars, followed up by regular communication to the industry (1 I).
- The idea of an “enhanced specific public-private sector dialogue on detection technology”, including the organisation of restricted seminars with Member States, the European Commission and the European Parliament, was supported (1 I).
- The effectiveness of security measures will be compromised if security practices are not kept confidential, and a database — even protected by passwords or other methods — would pose a high risk. As a result, meetings or other tightly controlled communications may prove a more effective method (1 I).

Both / Neither (2 C, 1 I)

- Both, to ensure the widest and most effective dissemination of best practice and to promote the sharing of knowledge about security among the Member States (1 C).

- Both databases and conferences pose the same problems regarding confidentiality, the choice of participants and those authorised to possess confidential information (1 C).

Private (P)

Four experts reacted to this question. One considered both methods to be appropriate (1 P). The other three stated that meetings and seminars are the most reliable method, although a database may be useful.

3.1.2 Can you suggest any other options on how best to identify and disseminate best practice in this field?

Public (MS)

11 MS and a Spanish region answered this question. Not all of them mentioned methods that they had not suggested in the questions above. Online distribution, for example in the form of a website, was mentioned most (3). Cooperation and contact between law enforcement / security authorities of the MS were also put forward.

It was proposed that certification efforts should be led by government bodies. The private sector, however, should be involved.

Public (EUR)

One public organisation suggested that this could be a function of the Council or the Commission.

Private (I & C)

8 private companies and 1 consortium provided the following suggestions:

General (1 C)

- Best practice studies should target not only Member States, but also sub-state stakeholders such as organisations and even citizens in order to examine not only best detection practices, but also “use” practices and the legality of the detection method employed (1 C).

Via existing structures (5 I, 1 C)

- Identification and dissemination can be handled by the national regulator (1 I).
- Articles from users and test personnel (1 I).
- Evaluation of security systems by Member States or a centralised testing body with information shared in a forum (such as the ECAC TTF for aviation) (1I).
- Establishment of best practices in training and methodology for each type of civil security force, possibly in the form of a manual similar to that produced by NATO for military purposes (1 C).

- A comprehensive audit of all existing tools and equipment should be performed, followed by the formation of technology-specific, multi-national user and manufacturer groups, to identify and develop best practice. Results would be disseminated via a secure database. Responsibility for continuous best practice development would rest with the technology-specific user group (1 I).

- To establish best practice, representatives of the Member States should participate in a ‘workspace committee’ that focuses on a specific domain of detection (e.g. customs) or on cross-cutting areas. The cross-cutting workspaces would work on topics like ‘architecture’ and ‘common data elements’ and coordinate the specific domains where they interact (1 I).

New organisation/body (2I)

- A subcommittee established from a community of experts from the EU that deals with, for example, border issues. The subcommittee can be extended to include all major trading partners (1 I).

- A new organisation that manages feedback forms and disseminates them to the Member States. The Member States may need to tailor them to their own needs (1I).

Private (P)

Three experts answered this question. All suggested dedicated conferences and seminars of relevant national experts (2 P).

3.1.3 If an upgrade of a tool or equipment was considered necessary and no authority in other Member States would have performed such an upgrade, would consultation with the private sector on the subject be acceptable?

Public (MS)

18 MS answered this question. 7 MS thought that the private sector should be consulted. 4 were in favour of consultation under certain conditions. Lastly, one MS stated that innovation in detection instruments is by definition a process based on communication between public institutions and the private sector.

Public (EUR)

Both public agencies that answered this question feel consultation with the private sector is acceptable. Appropriate control of restricted or confidential information is necessary, however.

Private (I & C)

10 Private companies and 2 consortia shared their views on consultation with the private sector. One merely stated that it is not enough to look at the technical capabilities of equipment; the purpose for which specific equipment can be recommended or certified (1 I)

also needs to be considered. The others all felt that consultation with the private sector was acceptable, or even natural or essential (8I, 2 C).

The following remarks were made:

- Confidentiality should be taken into account (1I).

- Closer public-private partnership is desirable (1I).

- The term ‘private sector’ needs to be specified (1 C).

- Since the private sector manufactures the equipment and typically performs the upgrades, consultation with the private sector is often standard practice (4 I).

- Although upgrading existing equipment is usually the best and most efficient way to enhance detection capabilities, sometimes new technology is needed. Vendors and developers are the experts and should be consulted (2 C).

- If this implies public-private funding of the project, the private sector would probably be happy to be involved (1 I).

Private (P)

All three experts that answered considered this consultation to be acceptable (1 P).

3.2 Identification and dissemination of best practice and the use of new tools and equipment.

3.2.1 What would be the best way of identifying and sharing information and best practice in this field?

Public (MS)

11 MS and a Spanish region answered the question. Most frequently mentioned were the following ways of identifying and sharing information and best practices:

- seminars and conferences (6);

- secure electronic database (4);

- working groups and meetings (5).

Public (EUR)

3 EU-related bodies answered this question. One of them suggested a web portal as a tool for systematic information exchange; the other proposed a regular exchange of information in a well-organised structure. This would provide an overview of all the information to be maintained. The structure could take the form of working groups of security experts representing both governments and the private sector.

A third body would like to see the processing of personal data minimised as part of the best practice.

Private (I & C)

6 companies and 2 consortia gave suggestions on how to identify and share information. They proposed the following:

- Articles from users and test personnel (1 I).
- End-user workshops with feedback to technologies or solutions providers (2 I).
- Databases and meetings or seminars, both with limited access, can complement one another. Moreover, the role to be played by public and private stakeholders needs to be clarified (1 C).
- Common forums, theme conferences, discussions and newsletters are very useful. Security needs to be taken into account (1 I).
- Conferences and requests for information to industry, academia and research institutes (1 I).
- ESRAB could identify and disseminate information (1 I).
- Both the availability of a secure and searchable database and the organisation of meetings and seminars on such issues are necessary to ensure the widest and most effective dissemination (1C).

Private (P)

Four experts on security suggested the following methods:

- Close links between security authorities and technology/solutions providers, organised within a standing European committee (possibly around a public “champion” for each sector, e.g. Europol or OLAF or ENISA), where periodic meetings and exchange of information are expected (1 P).
- The producers and the final consumers of the technological solutions working side by side (2 P).
- Encouraging cooperation between specialists from all sectors across Member States (1 P).

Identification of best practice

3.2.1.1. Would it be through peer evaluation or questionnaires sent to the Member States?

Public (MS)

11 MS and a Spanish region answered the question. Peer evaluation and questionnaires were mentioned equally often as methods of identifying best practice. Most MS thought that both ways are suitable. Other possible means that were mentioned included mostly personal contact between experts or authorities.

Public (EUR)

The organisation that responded did not consider questionnaires to be an appropriate method; group consensus would tend to yield the lowest common practice rather than the best practice.

Private (I & C)

4 companies provided an answer to this question. Two found neither peer evaluation nor questionnaires to be a suitable method (2 I). One considered meetings to be a better approach. The others did not comment on either method but noted that identification of best practice should be global in scale (2 I) and needs to be considered on a case by case, or theme by theme basis (1 I).

Private (P)

Four experts on security expressed their views on this question. One deemed both suggested methods to be appropriate (1 P). The others indicated that devising a good questionnaire would be difficult in this phase, since it concerns the use of new tools (2 P). One expert was doubtful about this option.

Dissemination of information and best practice

3.2.1.2. Would it be through a secure and searchable database or through restricted meetings and seminars?

Public (MS)

12 MS and a Spanish region answered the question. A secure database was mentioned by 11 MS, the restricted meetings and seminars by 9. The vast majority of the MS and a Spanish region deemed both methods to be appropriate.

Public (EUR)

One EU-related body answered that meetings and seminars are preferable. However, since these may be too time-consuming for some MS, an additional database would be useful.

Private (I & C)

4 companies indicated their preferences. One preferred a database, the other three favoured restricted meetings and seminars. The following remarks were made:

Database (1 I):

- Meetings and seminars are too costly in terms of time. The prime source should be a searchable database with seminars and exhibitions as a secondary source (1 I).

Meeting/Seminars (3 I)

- The effectiveness of security measures will be compromised if security practices are not kept confidential, and a database — even protected by passwords or other methods — would pose a high risk. As a result, meetings or other tightly controlled forms of communications may prove a more effective method (1 I).

Private (P)

Four experts reacted to this question. One felt both methods were appropriate (1 P). The other three stated that meetings and seminars are the most preferred method (3 P), although a database may be useful (2 P).

3.2.2 Have you any other suggestions for how to identify best practice in this field and disseminate them effectively?

Public (MS)

-

Public (EUR)

One organisation responded. It submitted the following suggestions:

- experts groups involving end-users and regulators;
- (security) audits.

Private (I & C)

6 companies provided the following suggestions with regard to the identification and dissemination of best practice:

- Articles from users and test personnel (1I).
- Through expert groups (such as ECAC) (1 I).
- For non-sensitive information, a variety of channels are available: database, publications, conferences, working groups, websites (1 I).
- A secure collaboration site for Member States to post questions and seek help/advice from others would be useful. Collaboration tools can be used to disseminate information in a secure environment (1 I).
- A comprehensive audit of all existing tools and equipment, followed by the formation of technology-specific, multinational user and manufacturer groups to identify and develop best practice. Results would be disseminated via a secure database. Responsibility for continuous best practice development would rest with the technology-specific user group (1 I).

- To establish the best of best practices, representatives of Member States should participate in 'workspace committees' that focus on a specific domain of detection (e.g. customs) or on cross-cutting areas. The cross-cutting workspaces would work on topics such as 'architecture' and 'common data elements' and coordinate the specific domains where they interact (1 I).

- A centralised point of contact at EU level for both Member States and industry (1 I).

Private (P)

Two experts proposed a network of end-users who would communicate and work together through a dedicated website (2 P).

Experimental and new tools

3.2.3 Are you interested in the trialling of new or experimental tools and equipment?

If yes/no, please explain

Public (MS)

The 13 MS that answered the question were all interested in the trialling of equipment. Many had additional remarks or reservations. Some emphasised the importance of experimental tools and trials, others underlined the importance of carrying out research at European level in order to avoid duplication and to be more resourceful.

Public (EUR)

One public agency answered this question. It is interested in trialling as experimenting with new tools is of vital importance to enhancing security.

Private (I & C)

8 companies and 3 consortia expressed their interest in the trial of new or experimental tools and equipment. One company would be happy to offer its expertise, another to offer its tried and tested tools. Additional remarks were made.

Private (P)

All five experts were interested in the trialling of new or experimental tools as they pave the way for improvement and new solutions (5 P).

3.2.4. Would partial financing of trials of new or experimental tools and equipment by the Community and/or the private sector be of interest?

Public (MS)

12 MS answered this question. All MS think that partial financing of trials of new or experimental tools and equipment by the Community and/or the private sector could be of interest; one claimed that it already exists. It was mentioned that the private sector does not

always have sufficient resources, especially in the initial stages, nor do some MS. In a qualification process, however, some degree of independence from the private sector must be maintained.

Public (EUR)

Two EU-related bodies responded to the question. They agreed that partial funding would be useful. Neither industry nor public stakeholders are normally willing to pay for large-scale demonstration projects. Moreover, some tests require funding to buy prototypes and to maintain the research facilities.

Private (I & C)

7 companies and 4 associations commented on this question. All thought co-financing by the Community and/or private sector would be of interest. The following issues were brought to the fore:

- The most promising tools should be tested, irrespective of whether they are European or not (1 C).

- Trials should be conducted with a spirit of cooperation so that everyone involved learns lessons and benefits. Real world data collection can be key for technology development, but because of the costs involved financial assistance should be considered (1 I).

- It is important to stress that the independence and integrity of the authority and freedom to choose other solutions are not affected by the trial (1 I).

- An overall financial package would strengthen solidarity and could increase Europe's industrial competitiveness (1 C).

- Trialling is extremely expensive. Furthermore, trials are currently repeated in multiple Member States, multiplying the cost to industry and government. Sharing data will significantly reduce costs. A single trial with a broader scope would be much more cost-effective than multiple tests (1 I).

- To avoid any waste of funds, such funding should be carefully apportioned to companies that can demonstrate the development of technologies that are both flexible and adaptable over a significant life-cycle (1 I).

- As public authorities are the main beneficiaries of detection technology, they could co-finance its development, in particular the ‘pre-competitive tests’. Qualification and certification have to be addressed for the pre-standardisation process. The private sector raised the question of the type of pathogens to be identified; the degree of specificity or sensitivity, etc. (1 C).

Private (P)

All five security experts supported the idea of partial financing. It was mentioned that public-private partnerships of this kind have already been established in the US (1 P). Moreover, such partnerships could launch pilot projects (1 P). Additionally, it was suggested that sharing the cost of development may lower the cost of the final product (1 P).

3.3 Use of data and text-mining tools

Awareness raising exercise

3.3.1 **Would Member States and the relevant European bodies be interested in sharing best practice and in the potential benefits arising from the use of data- and text-mining tools?**

Public (MS)

13 MS answered this question. The vast majority (10) of the states that answered this question suggested that they would be interested in sharing best practices. The others did not respond negatively, but pointed out that certain problems could arise when sharing knowledge.

Public (EUR)

Two EU-related bodies reacted to this question. They commented mainly on what the content of such best practices should be. One public body strongly advocated that best practice should include compliance with data protection principles.

Private (I & C)

1 consortium and 1 company answered this question, stating that Member States should be interested because their application to crime detection objectives could provide an innovative insight into security issues (1 C). Sharing is considered essential although privacy laws in individual Member States are likely to create a significant barrier to data sharing (1 I).

Private (P)

Four experts answered this question in the affirmative (4 P). This topic is of interest to both academic and other entities (1 P).

3.3.2. **Would Member States authorities using this technology be willing to share experience with their peers?**

Public (MS)

All 9 MS that responded to this question answered ‘Yes’. One MS added that the sharing of information in this field with other authorities and the procedures for exchanging information could be laid down in a common agreement between all or some of the countries taking part.

Public (EUR)

The results of Europol’s trials could be made available for interested parties.

Private (I & C)

One company answered that authorities were likely to want to share experiences. Sharing data, however, is more of a problem (1 I).

Private (P)

Four experts answered this question. Three estimated that authorities would not always be willing to share information because of the degree of sensitivity involved (3P). It was added, however, that it would be important to define the procedural protocols and standards that go hand in hand with progress in information technology (1 P).

3.3.3 **Would restricted seminars on the subject organised by the Member States, Europol or OLAF be useful?**

Public (MS)

13 MS and a Spanish region answered this question. All but one felt that such seminars were useful. Another MS specified that their usefulness would depend on the topic. It was underlined once again that sharing experience is valuable, especially at European level. With topics like these, however, confidentiality should be guaranteed. Europol was mentioned as a suitable candidate for organising seminars.

Public (EUR)

This might be a task for CEPOL ultimately. However, Europol would be glad to contribute to seminars.

Private (I & C)

4 companies and 2 consortia responded to this question. Three companies and 1 consortium supported the organisation of restricted seminars (3 I, 1 C). Another emphasised that collaboration between Member States and the relevant bodies is useful to identify the ‘champions’ in data and text mining technologies (1 I). Moreover, it was suggested that the Commission should draw up a list of available analysis tools and methodologies (1 C).

Private (P)

Four security experts answered that such initiatives would be useful (4 P).

Enhancement of the EU capacity for data and text mining

3.3.4 Would a centre of excellence at European level accessible to all Member States and their relevant authorities help to tap the potential of these tools in practice?

Public (MS)

13 MS and a Spanish region answered this question. The majority (9) were in favour. It was felt that such a centre could, for example, enhance the EU’s data mining capacity, cope with numerous languages, establish an agreed format of data and possibly relieve the burden of Europol. 4 MS expressed concern, among other things for reasons of redundancy because of already existing centres.

Public (EUR)

One public body remarked that the usefulness of data mining and text mining tools would have to be proven in a number of specific business scenarios. While the technology might be impressive, the delivery of better information to the right person in the right place at the right time is the only real test of worth.

Private (I & C)

4 companies and 3 associations responded to this question.

1 association and 2 companies replied that the creation of a network of excellence would be a first step towards bridging the gap between Member States with differing levels of expertise (1 C) and avoiding duplication of research and improving synergy at EU level (1 I).

3 companies and 2 consortia supported the establishment of a centre of excellence. More specifically,

- setting up of an I-Q-Tel type of organisation would help to stimulate growth among small local technologies (1 C); and
- it would provide the opportunity to capture and deploy best practice (1 I).

Private (P)

Four experts believed that such a centre would be useful (4 P), especially since security is a European issue (1 P).

3.3.5 If not, what other options would you suggest to maximise the potential of these tools?

Public (MS)

2 MS suggested other options. One suggested the sharing of best practices, seminars and exchanges. Another put forward the possibility of temporary use of demo versions (engines) of commercial and non-commercial technological solutions.

Public (EUR)

-

Private (I & C)

-

Private (P)

One expert suggested the networking of different centres of excellence dedicated to the use of these tools in an application security environment (1 P).

Identification and dissemination of best practice

3.3.6 Would a peer evaluation or a questionnaire sent to the Member States be useful in identifying best practice in the use of these tools?

Public (MS)

10 MS answered this question. 7 MS felt both peer evaluations and questionnaires are useful tools for identifying the best practice in data mining tools. 2 MS preferred questionnaires. It was remarked that questionnaires serve mainly to generate general and basic information. 1 MS believed that it was not possible to establish a universal best practice in this area.

Public (EUR)

One public body responded that it did not think these tools useful as they would risk being too qualitative.

Private (I & C)

2 companies answered this question. One agreed with both options. The other did not think questionnaires a suitable mechanism for accurate data gathering on complex systems and suggested peer review, backed by dedicated study and user groups, instead.

Private (P)

Four experts answered this question. Two indicated that both methods may be useful, but possibly difficult to carry out in practice (2 P). Since none of these tools is standardised, designing a valid questionnaire or organising a peer evaluation is a problem (2 P). One expert supported only peer evaluation.

3.3.7 If not, what other approaches would you suggest to identify best practice in this area?

Public (MS)

3 MS answered this question. The three approaches mentioned are:

- a secure database;
- sending out questionnaires to the universities and research institutions that are doing research in this field;
- sharing best practices, seminars and exchanges (as above).

Public (EUR)

One body proposed a collection of case studies to illustrate the benefits of using the tools, balanced against their full cost in terms of money and time. The point is that some agencies may find data mining more profitable than others. It may depend on the intelligence requirement.

Private (I & C)

One consortium and a company suggested the following:

- The Commission should encourage pilot or rapid prototyping projects to implement an end-to-end OSINT solution for specific types of security agencies across several MS and/or the EU institutions themselves. Such projects — with operators, security forces and private players — would develop technical integration and operational use and help to improve common methodological standards (1 C).

- Vendors can recommend best practices or refer to organisations that are currently using the tools (1 I).

- EU-sponsored meetings of delegates from the Member States (1 I).

Private (P)

Two experts in the field of security proposed the following alternatives:

- a review of the existing literature on the subject (1 P);

- the appointment of a trusted board or a network of private and public specialists, which exchange of information between themselves, with the EU and the MS (2 P).

Enhancement of the regional capacity for data and text mining

3.3.8 Would there be any spare capacity available in Member States and European bodies to help Member States that do not possess this technology to work on their documents?

Public (MS)

9 MS and a Spanish region answered this question. Opinions were sharply divided.

Public (EUR)

Two EU-related bodies responded to this question. Both had their doubts regarding the proposal. One would like to see it clarified further. The other saw the logistics of the proposal as a problem as the responsibility for errors would be hard to manage.

Private (I & C)

Two companies responded to this question. One stated that data and text mining are so sensitive that outsourcing is inappropriate (1 I). The other suggested that the Community look at ways of streamlining requirements for text mining in order to avoid duplication. Private industry could assist in this process (1 I).

Private (P)

Three experts answered that they believed such capacity to be available (3 P).

3.3.9. If there were no such spare capacity or only a limited capacity, would an EU-funded increase of capacity in Member States or at the European level be useful and practical?

Public (MS)

9 MS answered this question. All Member Status thought the proposed funding was both useful and practical.

Public (EUR)

One agency pointed out that this would depend on whether good research methods validated the usefulness of the tools.

Private (I & C)

One company answered that it would be worth a try (1 C).

Private (P)

Three security experts answered this question. They considered an EU-funded increase to be highly recommendable (2 P).

3.3.10 Would Member States that lack sufficient data and text-mining capacity consider using the tools of other bodies, if made available?

Public (MS)

The 5 MS that answered this question would all consider using the tools of other bodies. 1 MS did not consider this to be a very practical approach.

Public (EUR)

-

Private (I & C)

Two companies responded to this question. One answered that it might be possible if there were assurances that these tools do not ‘report their activities back’ to other authorities (1 I). The other strongly advised that Member States acquire their own tools as security authorities are most effective when they can manage and search for information themselves. Moreover, governments do not want other authorities to work on their documents. For financially less capable states, leasing or funding options could be considered (1 I).

Private (P)

Three experts responded positively to this question, provided that data protection was taken into account (2 P). It was remarked that tools have already been borrowed in the past by way of intergovernmental agreement (1 P).

3.3.11 Would it be possible to create European or regional centres for data and text mining which several Member States and their authorities could use for data and text mining?

Public (MS)

11 MS answered this question. A slight majority (6) favoured the creation of regional or European centres. One MS felt the creation of such centres was probable, while another accepted the idea conditionally. Three MS opposed the idea. One felt that Europol already fulfilled the function; the other supported national centres.

Public (EUR)

Two public agencies answered this question. One supported the idea of such centres; the other requested further clarification as to what such a centre would mean. It should not consist merely of a 'clearinghouse' of techniques for data extraction.

Private (I & C)

4 companies and one consortium answered this question. All think the creation of such centres would be possible (4 I) or even desirable (1 I) or necessary (1 C). A number of remarks were made on the issue:

- It may be useful to extend collaboration to include strategic non-EU countries (1 I).

- Such centres should have the responsibility of organising and handling all the regional efforts on security research by means of data and text mining, and promoting collaboration between the public and private sectors in order to tailor private solutions to MS authorities' needs (1 C).

- These centres should also serve as intelligence 'fusion centres' for collaboration between security agencies. To encourage increased information sharing and cooperation between national security authorities, implementation of an extremely successful model, such as the Californian Joint Regional Intelligence Centre, is recommended (1 I).

Private (P)

Four experts stated that this would be possible (4 P) and that such centres already exist (1 P).

3.3.12 Do existing data and text mining tools sufficiently deal with the various languages within Europe?

9 MS, one EU-related body, one company and one consortium, and four experts answered this question. Several concrete issues were identified.

3.3.13 Are there adequate tools to support authorities dealing with foreign language text and documents?

9 MS, three companies and four experts answered this question. Several concrete issues were identified.

Other

3.3.14 **If you disagree with any of the options suggested above, how would you address the concerns raised by this point**?

Public (MS)

One MS suggested another approach.

3.4 Testing and certifying the quality of equipment and tools

3.4.1 **Would creating a network of national certifying authorities sharing experience and knowledge, along with a system of quality certification and benchmarking, be useful?**

Public (MS)

14 MS answered this question. All support the idea of creating a network of certifying authorities. It would enhance efficiency. Moreover, harmonisation and minimum requirements would be beneficial to both public and private players. However, it should not have a negative impact on high national security standards.

Public (EUR)

Three EU-related bodies responded to this question. All three were (tentatively) supportive of the idea. One put forward the example of ECAC as a successfully functioning network of authorities.

Private (I & C)

<u>General remarks</u>

- Compliance with stringent standards should not stand in the way of the development of innovative technology (1 I, 1 C).

- Testing and certifying should be discussed together with standardisation efforts. Descriptions/specifications/list of tested equipment should be available to ‘cleared participants’ only (1 I).

<u>Answer to the question</u>

6 companies or research centres and 3 associations responded to this question. Three supported the creation of a network (2 I), two respondents supported the creation of EU-wide authorities – whether in the form of a network or a single European certification agency (2 C). Another preferred a single agency over a network (1 I) and one opposed the creation of a single authority (1 I). One consortium suggested that there is no need for such a network or authority (1 C)

The following additional remarks were made:

- Commonly agreed standards should be used and approval by one authority should be accepted by the others (1 I).

- This network could be responsible for publishing articles comparing tools and equipment (1 I).

- A certifying authority would be useful to the extent that certification and benchmarking promote quality, standardisation and open architecture. However, unnecessary certification requirements that would impede the development and implementation of security technology must be avoided (1 I, 1 C).

- As technology is deployed globally, US and EU standards should be recognised reciprocally. In addition, the EU should consider an equivalent of the US Safety Act. This EU safety legislation would allow technology to be certified and rated at different levels, so that technology users could have benefits if using the best rated technology (of a fiscal, insurance or other nature). It could also supply risk mitigation mechanisms to companies that could be sued following a terrorist attack (2 C).

Private (P)

Four experts answered this question. Three believed it would be a useful initiative (3 P). The other stated that the definition of agreed benchmarks is a prerequisite to correct comparison and certification (1 P).

3.4.2 If not, what other solution would you suggest to address the problem raised?

Public (MS)

Three MS provided suggestions. One felt certification and verification should be managed by Community legislation. The second stated that, for objective evaluations, it is necessary to have volumes of reference data. Such evaluation campaigns require considerable manpower, however. The third MS suggested exchange of experience with new detection tools among security authorities.

Public (EUR)

One agency suggested that it may be appropriate to have different states/laboratories responsible for testing and certifying different technologies, i.e. metal detectors, EDS systems, trace detection systems, biometric and access systems, imaging systems, etc.

Private (I & C)

One consortium suggested using a European Quality Mark rather than a network of authorities or centralised authority.

Private (P)

One expert suggested a network of trust.

3.4.3 Would common standards for certifying and benchmarking be helpful?

Public (MS)

14 MS answered this question. Practically all favoured the creation of common standards. It was thought that such standards

- are essential to acceptable certification;
- would complement cooperation efforts between public and private testing structures;
- build trust, which will enable MS to rely on each other's judgments.

Public (EUR)

Two bodies responded to this question. Both think common standards for benchmarking and certifying would be helpful, but that sensitive parts of security specifications should not be made public. Moreover, some states may feel more threatened and therefore require performance levels above the norm.

Private (I & C)

8 companies and 2 consortia answered this question. All agreed that such standards would be helpful or even necessary or essential. Certification should however be performance-based (capability) (1 I). The following remarks were made:

Such standards would be helpful:

- in guaranteeing consistency in the treatment of international activities across the Member States (to identify liability in the event of an attack and also to reduce the cost of protection and detection systems or installations by streamlining their production) (1 C);
- for data exchange and interoperability (1 I);
- to ensure that players in the critical market provide quality solutions (1 I).

In addition to common standards for benchmarking and certification:

- Compliance with standards should be considered as a certification activity. Moreover, the skills of the 'certifiers' should be tested and guaranteed (2 I).
- The Community should urgently consider tools for approval and calibration. These tools could be put in place at state level. But in that case, mutual recognition mechanisms (cross-certification) of this approval and calibration should also be included (1 I).

It was also remarked that a single set of common standards would be consistent with a single international certifying authority (1 I). 1 consortium believed that this was part of the European Quality Mark.

Private (P)

Four experts answered this question. All believed this would be useful, although the development of standards takes considerable time and effort. Moreover, devising standards for such novel technologies may be difficult (2 P).

3.4.4 If not, how would you ensure transparency of this process and usability of the results across the EU?

Public (MS)

One MS and a Spanish region answered this question. The following suggestions were made:

- Through a secure website for the authorities, which would contain the results and/or reports in question and which would allow users to comment on the quality of its contents.

- The European Commission should draw up a Common European Standard for certifying and benchmarking, such the European Standards for the requirements on information (as referred to above). Once the Common Standards are established, the technologies have to be certified and benchmarked by the Member States.

Public (EUR)

One public agency proposed the following process:

A document containing technical specifications will be made available for the appropriate authorities. This document will have been drafted by working groups of specialists. Stakeholders and manufacturers will be informed of the process. Information will be controlled and released only to producers that manufacture a specific piece of equipment. They will be obliged to keep this information secure.

Private (I & C)

-

Private (P)

-

4. Studies

4.1. Would you be interested in receiving studies on these topics based on the background information outlined in the Annex?[1]

Public (MS)

15 MS answered this question. All were interested in receiving studies. Some indicated preferences. One MS highlighted the importance of protecting data in case the development of new technologies should lead to more data processing. Another pointed out that some subjects have already been studied in the context of the ESRP and that DG JLS and DG ENTR should coordinate their activities in an effort to consolidate the links that exist between new technologies and their use by the authorities. One MS indicated that a study on law and specific detection technology and a study on specific detection technology and its practical use (studies 3 and 4 of the Green Paper) come under national jurisdiction.

Public (EUR)

Three EU-related bodies answered this question. All agreed that such studies would be of interest. One suggested that a privacy impact assessment should also be carried out. Another added that some studies may need to be periodically updated to take account of technology development and threat assessment.

Private (I & C)

9 companies and 5 consortia answered this question.

All were interested in receiving studies. The question was raised as to how access could be gained to the studies. Moreover, some respondents offered their expertise (1 I, 1 C).

The following topics were mentioned specifically:

- protection of mass events (2 C, 1 I);
- cooperation and information sharing among forensic laboratories and security research in states (1 C, 1 I);
- law and specific detection technology (2 C, 1 I);
- specific detection technology and its practical use (3 C);

[1] Studies on:
(1) technology and the protection of mass events;
(2) obstacles to cooperation and information-sharing among forensic laboratories and security research institutes;
(3) legal provisions regulating the use of specific detection technology;
(4) practical use of specific detection technology;
(5) legal framework governing the use of personal detection (including surveillance) across the EU;
(6) levels of acceptance of personal detection (including surveillance and use of biometrics) across the EU.
Further information is available in Annex III of the Green Paper

- personal detection technologies and biometrics (3 C).

Additional topics:

- data and text mining tools (1 C);
- mass land transport (1 I) / mass transit (1 C);
- equipment that meets genuine needs and works in operational environments (1 I);
- evaluation of (combination of) tools for use in a specific sector (1 I); evaluation not just of the detection capability but also of how they operate within the whole process of identification of, for example, CBRN (1 I);
- inventory of what capacities are needed at what level (if EU-certified laboratories of other countries can be used, a national laboratory may not be needed) (1 I);
- use of high-tech infrastructure in the area of security (1 C);
- role of data protection in the case of personal protection (protection of persons) (1 C).

Private (P)

Four experts answered. They would be interested in receiving these studies.

4.2 If not, please specify reasons and suggest alternatives of how to address the concerns raised

Public (MS)

-

Public (EUR)

-

Private (I & C)

One company specified that laboratories should also be certified to make it clear what capabilities it has and what analyses it can carry out (1 I).

Private (P)

-

5. Implementation of results of consultation

5.1 Enhanced specific public-private dialogue on detection and associated technologies

5.1.1 Would a tool such as an enhanced specific public private dialogue on detection and associated technologies be helpful in implementing the results of the public consultation on this paper?

Public (MS)

17 MS answered this question. 14 supported an enhanced specific public-private dialogue. 1 MS questioned the added value of formalising such debate. It was emphasised that experience and information should be shared on a technological level and not include personal data.

Public (EUR)

Three public bodies answered this question. All supported the idea of public-private dialogue. Such a tool is needed to identify and streamline different agendas. It was remarked that the main misunderstanding between the political side and research and industry is that defence and internal security are at the same time similar and different. A coherent strategy on European internal security can only be achieved if Member States have the same understanding and vision. Before the public authorities can have a meaningful dialogue with the private sector, public stakeholders should communicate amongst themselves.

In civil aviation, public-private dialogue on security has already been set up.

Private (I & C)

12 companies or research centres and 7 consortia responded. All thought this dialogue was helpful. Two respondents specifically indicated their willingness to contribute (1 C, 1 I).

Some additional remarks were made:

- Dialogue should be confined to practical solutions to specific problems (1 I).
- Best practices and guidelines should be the responsibility of the public sector and not influenced by the private sector (1 I).
- Dialogue should take place through a forum (1 I).
- Such a dialogue should be open not only to security authorities but also to the private sector, data protection agencies and citizens so as to ensure the legitimate implementation of security controls (1 C).
- Any initiative that promotes communication between the private and the public sector is beneficial (1 I). Private stakeholders and academia need vehicles through which they can communicate with Member States' governments (1 I).
- Technical specifications should be available to 'cleared' participants only (1 I).

- This dialogue can be used for the public authorities to express their needs and the private sector to present its new technologies. It could also address privacy concerns. Sometimes, new technologies are hampered in their deployment by existing EU regulations or standards. Therefore, legislation should have rapid built-in systems to allow fast introduction of breakthrough technologies (2 C).

- The EU Detection Forum has been set up to create an open dialogue with industry and public bodies in order to help shape European Policies in Security Research with the focus on detection (1 C).

- The dialogue should include providers from non-European countries in order to be meaningful (1 C).

- Security would need to be ensured (1 I).

Private (P)

Three experts answered this question. They responded positively to the suggestion of an enhanced public-private dialogue. One considered that a network would be necessary.

5.1.2 If yes, would you agree with the above suggestions or do you have different ideas?

Public (MS)

11 MS answered the question. 9 agreed and one provided the following suggestion: a working group involving the Member States should be set up to summarise the results of the consultation on the Green Paper. Subsequently, it should identify the priority areas in which specific action should be taken; without duplicating other measures implemented by the Commission such as FP7.

One MS specified that steps should be taken to improve coordination between the private and public sectors in order to close the gaps in the areas under consideration here. However, it did not agree with the creation of another body or entity, but felt that the scope and powers of existing bodies should be extended by creating forums for discussion and analysis.

One MS considered that for aviation security the current structures are sufficient.

Public (EUR)

Two agencies answered this question. One agreed, and the other suggested that the structure of exchange should be permanent in order to be able to release sensitive parts of technical specifications. This body should assess what information should be kept confidential and direct it to the right recipients.

Private (I & C)

5 companies and 2 consortia responded to this question. Three companies agreed with the above suggestions. Others added the following:

- open hearings in Member States in which the views of authorities, citizens and businesses are expressed (1 C);
- public-private dialogue on the use of technology in specific areas to focus the debate and avoid the formation of inappropriate general theories (1 I);
- a permanent body to oversee the public-private dialogue. The body should have a broad, global perspective and provide continuity over time (1 I);
- a CBRN task force made up of companies and public bodies to identify and discuss best practice on detection and associated technologies (1 C);
- a network of excellence, to be created (1 C).

Private (P)

Three experts responded to this question. Two agreed with the above suggestions, whereas the other proposed an alternative solution (see below).

5.1.3. If not, what other mechanisms would you suggest to follow up the results of the public consultation of this document?

Public (MS)

A Spanish region provided the following suggestion:

It would not be necessary to set up a new specific body because the Specific Group (within the Centre of Excellence mentioned earlier) could fulfil the functions.

As set out in the Green Paper, the Specific Group should consist of the following:

- *Participation*: the security services should take part in it.
- *Concrete and clearly defined objectives*. for it to be effective.
- *Standing committee*. to provide weight;
- *Forum*: for experts from both the public and private sectors.

The relevant regional authorities would be interested in helping to set up this body.

Public (EUR)

-

Private (I & C)

One consortium and one company answered this question:

- deliver a presentation to industry on what is required and how it is to be managed (1 I);

- adopt an integrated approach with a clear identification of difficulties in order to set the priorities (1 C).

Private (P)

The following alternative was proposed:

- setting up an international body consisting of specialists, public authorities and solutions providers (1 P).

5.1.4 Would you be interested in contributing to its work or directly participating in it?

Public (MS)

12 MS answered this question. 11 expressed their interest; one indicated they could not yet provide an answer. Reservations included the point that participation depended on the proposals and resources. Confidential information should be protected.

Public (EUR)

Three public bodies answered this question. Two indicated their interest in contributing. The other would also be interested, provided restricted and sensitive information is dealt with appropriately. The final decision, however, would have to be taken by the relevant hierarchical structures.

Private (I & C)

8 companies/research centres and 6 consortia answered this question. All would be willing to contribute.

Private (P)

Three experts responded. They would be willing to contribute (3 P).

Action Plan

5.2.1 Would an action plan be a useful tool for implementing the measures identified in the replies to this document?

Public (MS)

16 MS answered this question. 13 supported the idea, 3 were dubious. Comments that were made include:

- An action plan will ensure that results do not get lost and provides a tool for monitoring progress.

- First the results of the GP should be disseminated, then the action plan should be drawn up.

- The action plan should take into account that detection technologies are a national matter. However, it could lay the foundations for closer EU cooperation.

Public (EUR)

Three bodies answered to this question. All felt an action plan to be a useful tool.

Current existing initiatives should be taken into account.

Private (I & C)

9 companies and 6 consortia responded to this question. All considered an action plan to be a useful tool. Some additional remarks were made:

- The action plan should be developed in active conjunction with the respondents, including the private sector (2 I).

- Publication should be restricted to cleared persons (1 I, 1 C).

- The action plan should be made up of concrete proposals and not merely set out targets (1 C).

Private (P)

Three experts responded. They support the idea of an action plan.