DECOTESSC1

Demonstration of Counter Terrorism System-of-Systems against CBRNE phase 1

Title :	Strategic roadmap
Number :	Deliverable D9.1
Authors :	Ingrid Bastings, Clara Peters and Jeroen Wevers (TNO) Herbert Wiesinger (AIT) Francoise Simonet (CEA) Gudrun Bunte (FhG-ICT) Sebastian Chmel and Hermann Friedrich (FhG-INT) Anneli Ehlerding and Hanna Ellis (FOI) Michalis Christou and Paolo Peerani (JRC) Friedrike Strebl (Seibersdorf) Nieves Murillo (Technalia) Anna-Mari Heikkilä and Ilpo Kulmala (VTT)
Classification level :	Public

Grant Agreement number :	242294
Project acronym :	DECOTESSC1
Project title :	DEmonstration of COunterTErrorism System-of-Systems against CBRNE phase 1
Partners:	TNO (NL, coordinator), AIT (AT), CEA (FR), Fraunhofer (DE), FOI (SE), JRC (EU), VTT (FI), Tecnalia (ES), Seibersdorf (AT)

SEVENTH FRAMEWORK PROGRAMME

Summary

This report describes the results of Work Package 9 'Strategic Roadmap' of the project DECOTESSC1, which is a phase 1 demonstration project within EU FP7 security call of 2008, in which the required steps are defined to come to an integrated European CBRNE counterterrorism capability.

Based on inputs from end users and the results from the work packages 5, 6, 7 and 8 a description has been made for each of the Top 25 Topics addressing how to go from needs (e.g. the Top 25 gaps) to demonstrated CBRNE capabilities (including products and services), using current technology as a starting point. In these descriptions also other (related) aspects are included, like legislation and ethical aspects, that may influence the overcoming of certain gaps.

Each of the roadmap Topics in itself is a conclusion on how to achieve a certain milestone (which capability needs to be achieved, which R&D and/or related issues need to be explored).
Besides this, every roadmap topic is mapped on a timeline, starting today and moving towards 2020 and beyond. Each of the 25 roadmap Topics was positioned on its expected end-date; given the current status of R&D and available products, the gap could be 'solved' at that point in time. Drawing a timeline provides valuable insight in time tracking of subsequent deliverables and milestones. At the same time the consequences of aspects which might delay or speed up progress can be observed.
The second aspect that was addressed in the overall conclusions was the relation that exists between the 25 roadmap topics. As stated before, none of the topics is a stand-alone issue and by analyzing the interdependencies one can get insight into which clusters of topics is predominantly present in the spectrum.

Figure 1 shows a visual representation of the topic-to-topic relationships; each of the topics is represented by a box. The separate topics have their importance, but given the amount of relations they have to other topics, it can be stated that the top of the prioritized list represents the system-of-system topics to address in the near future. In this upper half of the prioritized list, five clusters of topics are visible (see Figure 2). These clusters represent the 5 most urgent and feasible challenges that should be demonstrated in phase 2.

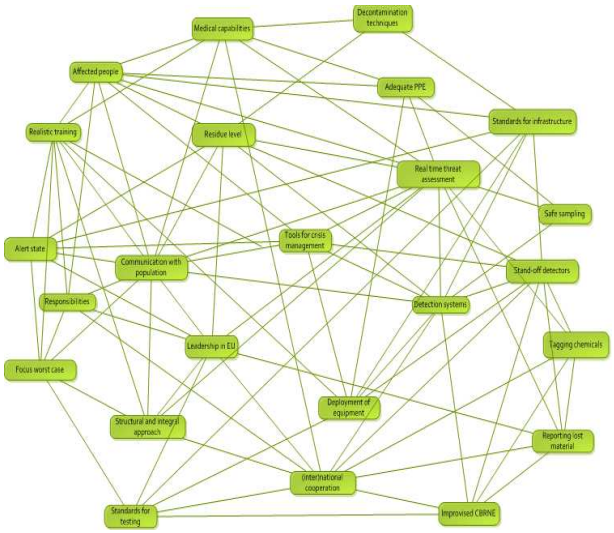


Figure 1 Relations between roadmap Topics

In summary, the Phase 2 demonstration project should focus on **Integration and Information** and exhibit a consistent and coherent portfolio of countermeasures for CBRNE terrorism. The most urgent and feasible challenges within integration and information are:

Fusion of information and establishment of a situational picture. As an element of a continuous CBRNE threat assessment there is a need for real-time situational awareness of the dynamic aspects before, during and after an incident. This includes detection, identification and monitoring of actors, agents, means of delivery, targets, and effects. In the case of assessing the CBRNE threat and impact,

the validity of the perceived picture of the threat and its consequences needs to be measured and verified.

Communication. Because of its low probability vs. high impact nature, CBRNE related communication to the general public requires special attention. In addition to general disaster management strategies, CBRNE awareness and resilience should be created. Aspects such as education, the role of local, regional, national and European authorities and the passive and active use of (social) media should be covered by a dedicated communication strategy.

Cooperation. CBRNE counterterrorism involves numerous players that have different skills, knowledge levels, approaches and practical experience with CBRNE incidents. In order to minimize the impact of an incident, extensive cooperation and coordination is required between these players. The requirement is thus to link the phases the security cycle, to pool (scarce) resources, to share (classified) information, and to use best practices from separate C, B, RN, and E experiences. A lot can be learned from and shared with other domains (health, safety, environment, defence).

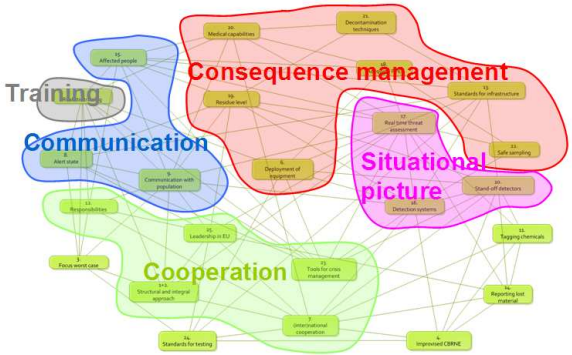


Figure 2 Roadmap Topics clustered

Consequence management. Many activities focused on an efficient handling of an incident require further improvement. Mostly post-incident activities (the response and recovery phases) are concerned, but these have a substantial relationship with pre-incident activities. These involve medical countermeasures as well as dealing with the effected infrastructure and area. Topics to demonstrated are: search and rescue, triage, on-site medical care as well as transport to and treatment in hospitals, containment/quarantine, self-help, decontamination of people/infrastructure/area, and dealing with chaos and the (longer term) psychosocial effects. Furthermore, adequate (personal) protection is an important aspect. Dedicated solutions are not always realistic and therefore integration with existing protection measures is required.

Realistic training and exercise. Current training and exercise does not fully reflect the complexity of CBRNE counterterrorism. Given the large impact and the organizational and financial burden of real-life exercises, new techniques (like the use of virtual reality and serious gaming) need to be further explored, developed and demonstrated to meet both needs and restrictions. There is a strong need to include aspects such as live agents, general population, and cross border cooperation.

Table of contents

1 Introduction

1.1 DECOTESSC1

The project DECOTESSC1 is a phase 1 demonstration project in the area of CBRNE counterterrorism, which was announced in the 2nd call regarding the research topic security within the specific program “Cooperation” of the 7th Framework Program for Research, Technological Development and Demonstration Activities (2007-2013) by the European Commission.
DECOTESSC1 proposes a DEmonstration of COunterTErrorism System-of-Systems against CBRNE terrorist acts that threaten and cause serious and widespread damage to human welfare and the environment. A CBRNE incident generally involves the destruction of property, injury, and loss of life; adversely affects a relatively large group of people; is “public” and can cause distress in the wider community for a longer time. CBRNE incidents include acts where the offence potentially has a political, religious or ideological objective or is a matter of national interest. CBRNE terrorism has unique implications relating to federal/provincial/territorial responsibilities, public safety, public confidence, national security and international relations.
During the DECOTESSC1 project, a thorough understanding of the system-of-system structure is to be developed, including a comprehensive taxonomy system. Next, the requirements for an ideal system will be proposed as well as a description of the current state-of-the art. Subsequently, a gap analysis should reveal the differences between the current situation and the ideal situation. The gaps thus obtained will be ranked. Also, in order to fill the gaps a strategic roadmap will be developed to guide the improvement cycle by proposing technological and organizational topics to be addressed and implemented in a future phase 2 of the demonstration project CBRNE counterterrorism.

1.2 Work package 9: Strategic roadmap

This deliverable belongs to work package 9, in which the required steps are defined to come to an integrated European CBRNE counterterrorism capability. These steps are described in ***a strategic roadmap (in terms of activities, timeline and participating entities)*** *that is executable as a part of Demonstration Program phase 2.*

The input for this work package was the Top 25 Gaps that were the result of work package 8 “Ranking of gaps”. The approach was to have interaction with end users on these Top 25 Gaps (during a workshop), dedicated to the long term perspectives, needs and development strategies concerning these Top 25 Gaps.
Based on the inputs from the end users and the results from the work packages 5, 6, 7 and 8 a description has been made for each of the Top 25 Gaps addressing how to go from needs to demonstrated CBRNE capabilities (including products and services), using current technology as a starting point. In these descriptions also other aspects are included, like legislation and ethical aspects, that may influence the overcoming of certain gaps. This all resulted in the description of the Top 25 Roadmap *Topics* in which all these aspects are included. We introduce the term *Topics* here (instead of *Gaps*), since a roadmap is about activities and goals, not about shortcomings. The term *Gap* refers to much to the latter, and the term *Topic* is more about the first.

By presenting the strategic roadmap not only for each of the Top 25 Roadmap Topics separately but also related to each other and over time, policy makers are able to allocate time and money to any future CBRNE demonstrator effort.

1.3 Guideline for reader

First of all, the letters in CBRNE have been studied together where possible and individually where needed in this report. As referred to before, the input for this work package was the Top 25 Gaps that resulted from work package 8 “Ranking of gaps”. In that ranking process, the specifics of the letters have no longer been taken into account, although some Gaps will be more dominant for some letters than for others. This means that the description of the Top 25 Roadmap Topics may vary on the letter or combination of the letters. The differentiations have been presented in the text accordingly.

Chapter 2 describes the method and process that has been used in this work package to come to the Strategic Roadmap.

In this report a description is given for all of the Top 25 Roadmap Topics. Since this leads to 25 different chapters, it was decided that the conclusions over all these Topics should be placed in a chapter *before* the Topics description rather than *after*. Therefore Chapter 3 illustrates the overall conclusions that can be drawn when reading through the Topics.

The Chapters 5 till 30 represent the Top 25 Roadmap Topics. Each of these chapters is structured in a similar way. In Chapter 4 this structure will be explained as to what type of information is included under each of the headings.

2 Method and process

In this chapter the method and process are described that have been used to come to the exploration of the Top 25 Roadmap Topics. Within the method and process three stages can be distinguished: (1) the third expert workshop of the DECOTESSC1 project, (2) the writing of the Top 25 Roadmap Topics and (3) drawing overall conclusions. Each of the paragraphs below will explore the method and process of each of these stages.

2.1 Third DECOTESSC1 workshop

The third workshop for the DECOTESSC1 project was held January 18-20, 2011. During this three-day workshop the expert group was briefed on the results of work package 7 “Description of gaps” and used these results to rank the gaps (work package 8). During the last day of the workshop, the Top 25 Gaps were explored upon by the expert group.

To focus this exploration, a Roadmap Information Form was developed previous to the workshop (see Figure 3). In this Form, all aspects that the DECOTESSC1 project team thought relevant for the roadmap were included. This starts with the rephrasing of the gaps into a ‘vision’: a roadmap is about achieving milestones. Therefore each gap needed to be rewritten into a phrase that started with ‘The EU (and its member states) should be able to….’. After that, a first estimate should be given on the timeframe in which this was expected to be achieved. To make this estimation, other information was needed: what type of products (capabilities or services) need to be in place to achieve the milestone? And subsequent to that, what type of R&D is needed to realize these products (capabilities or services)? Besides these questions, we also wanted insight in related aspects: legal, ethical but also economical, societal and environmental issues that influence possible solutions for a gap.

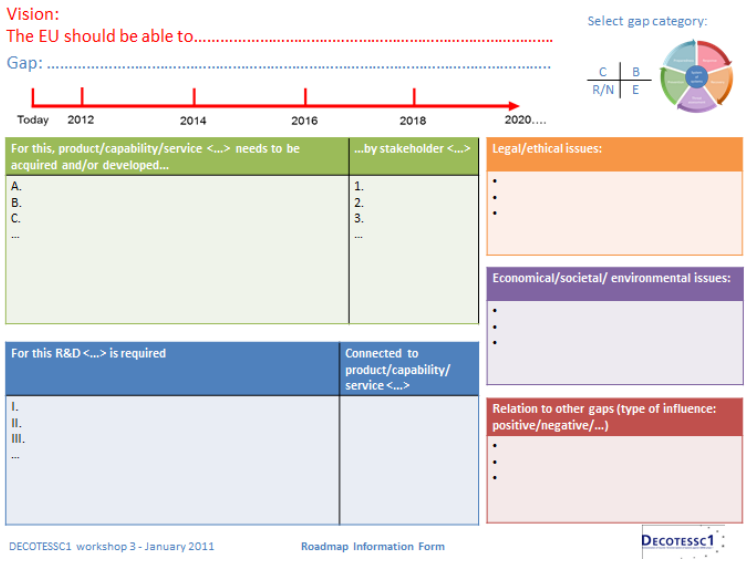


Figure 3 Roadmap Information Form

In the DECOTESSC1 project the system-of-systems approach is predominant. In the development of the roadmap this is shown by the relationships between the different gaps; none of the gaps is a stand-alone issue. All of them relate to other gaps, for instance through sharing of technology or information. This is why the Roadmap Information Form specifically addresses the relations between the gaps.

The objective of the workshop was to retrieve as much information as possible on the Roadmap Information Forms. Since the expert group was too large to do this plenary, the group was divided into subgroups of 4 people each, all consisting of 2 expert group members and 2 DECOTESSC1 consortium members. Each of this group was assigned a set of gaps to discuss and explore upon

within the small group. After that all the Forms were put onto the wall, on which a timeline was drafted. Each Form needed to be placed at the year in which the group expected that the gap could be solved. By the use of sticky memo-sheets everyone was given the opportunity to reflect on the results of others, thereby elaborating further on the Forms (see Figure 4 for a impression of the work).

Figure 4 Impression of work during third workshop

2.2 Writing the Top 25 Roadmap Topics

The results from the workshop were 25 Roadmap Information Forms with a lot of data on several aspects of the Gaps and subsequent Topics. These forms were distributed amongst all the DECOTESSC1 partners; one partner in the role of lead writer of the Roadmap Topic and another partner as reviewer. For each of the Topics a document was written combining the data from the Forms, the results from earlier Work Packages and some further research. Each document was structured similarly, representing the different aspects that were addressed on the Roadmap Information Form (see chapter 4).

2.3 Drawing overall conclusions

Each of the Roadmap Topics in itself is a conclusion on how to achieve a certain milestone (which R&D and/or issues need to be explored). Furthermore, there is the need for some overall conclusions; remarks to be made when overlooking all the Topics regarding the next phase.

The first aspect that we will draw conclusions on is the ***timeline*** *(see* Figure 5*)*. For this the same timeline is used as during the third workshop. The timeline starts today and moves towards 2020 and onwards. Each of the 25 Roadmap Topics is positioned on its expected end-date; given the current status of R&D and available products, the gap could be 'solved' at that point in time. Drawing a timeline provides valuable insight in time tracking orderly of subsequent deliverables and milestones. At the same time the consequences of aspects which might delay or speed up progress can be observed.

Figure 5 Timeline used during Roadmap process

The second aspect that will be addressed in the overall conclusions is the ***relation*** that exists between the 25 Roadmap Topics. As stated before, none of the Topics is a stand-alone issue and by analyzing the interdependencies one can get insight into which Topics are predominantly present in the spectrum. For this analysis, techniques based on Social Network Analysis[1] were used.

[1] For information see www.wikipedia.org, search for Social Network Analysis in English.

3 Summarizing conclusions

In this chapter, overall conclusions are drawn from the 25 Roadmap Topic descriptions. These overall conclusions are drawn from two aspects: (1) the timeline and (2) the relations between the 25 Roadmap Topics.

3.1 Conclusions drawn from the timeline

In Figure 6 the Top 25 Roadmap Topics are placed on the timeline. This timeline starts today and moves towards 2020 and onwards. In the description of the roadmap topics, each topic is placed on this timeline, positioned on that spot where, taking the current status of R&D and available products as a starting point, the gap could be 'solved'.
In the Topic descriptions, not only necessary R&D is addressed, but also related issues (like legal or ethical aspects that play a role when addressing that Topic). In the figure, topics that predominantly need R&D to reach the milestone, are colored **RED**. Topics where related issues are the main hurdles to overcome, are colored **YELLOW**. When both need almost equal amounts of attention, the topic is colored **ORANGE**. Some of the topics have smaller, white circles on the timeline; these represent in-between milestones that can be achieved earlier in time. Sometimes this is because of capabilities today are more advanced for one of the letters of CBRNE.

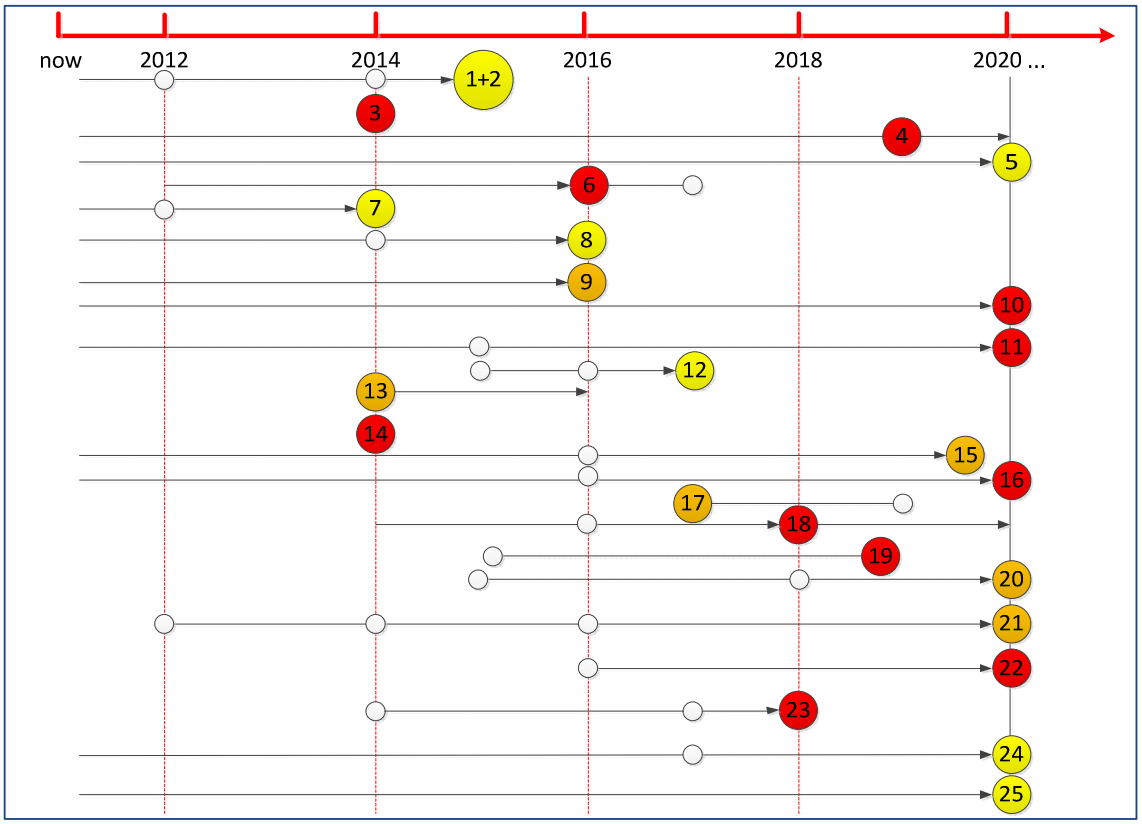


Figure 6 Roadmap Topics placed on timeline

When analyzing the information in the figure, it can be seen that although R&D in very diverse sciences is needed, the related aspects are very important as well. These related issues are very diverse

as well, for example from the *willingness* between EU-parties to share information to ethical issues concerning *privacy* of EU-citizens.

Looking at the way the Topics are scattered on the timeline, one can see that there is quite a range of expected end-dates. Given the complexness of the CBRNE-domain and the challenges that the domain faces, at first it was expected that the Top 25 Gaps would have been chosen from the focus of 'difficulty' and therefor would be placed later on the timeline. Apparently this criterion (difficulty) was not the most important one to score gaps; also the focus of 'daily problem with related issues as an angle' has been taken into account. This means that the Top 25 Gaps apparently represent the full spectrum of challenges throughout the CBRNE-domain.

3.2 Conclusions drawn from the relations

One of the elements that has been included in the description of the Roadmap Topics is the relation between the different Topics. Figure 7 shows a visual representation of those relationships; each of the Topics is represented by a box.
A line from one box to another means that these Topics are interrelated. It does not state what the type of relationship is (negative or positive). Some of the lines a thicker than others; when the line is thin, the relationship between the topics was only mentioned in one of the two related Topics (a 'single' relation), when a thick line is visualized, both Topics have addressed the relationship (a 'double' relation).

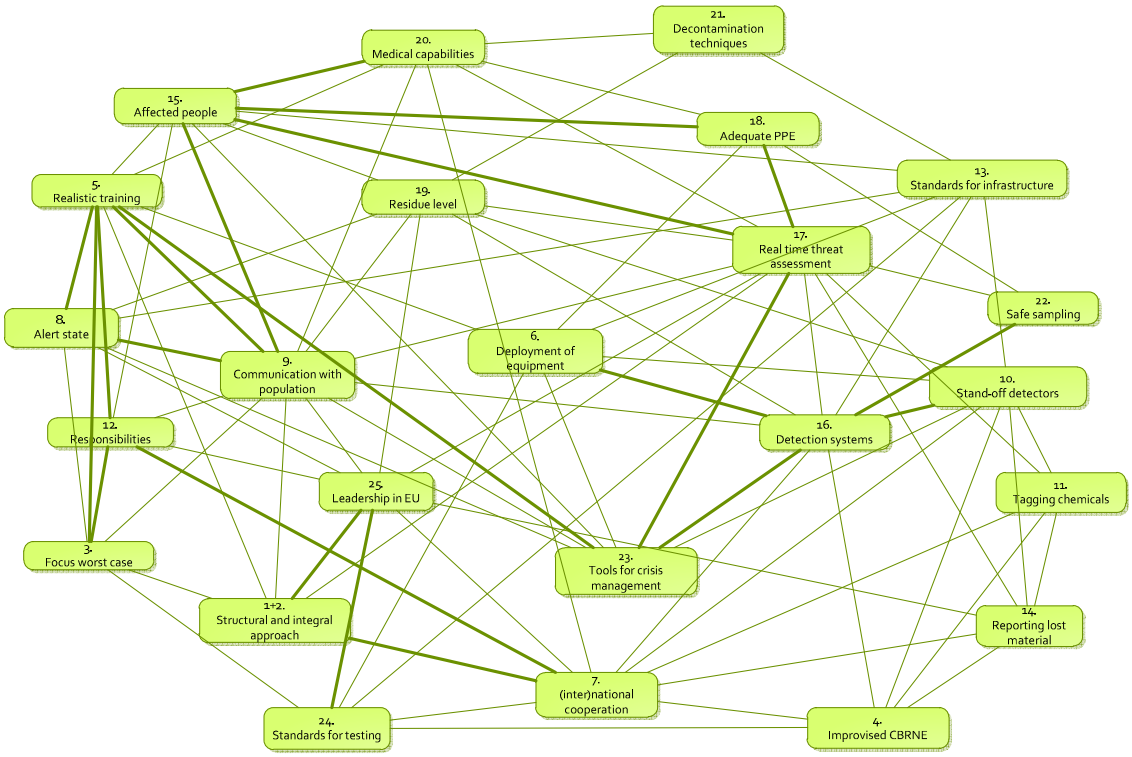


Figure 7 Relations between Roadmap Topics

When analysing this diagram, there are a number of observations that can be made:

The two Topics which relate the most to other Topics are no. 9 'communication with population' and no. 17 'real time threat assessment', both with a relation to 12 of the other 23 Topics (of which 3 are 'double' relations).

When looking at the number of relations a Topic has to other Topics, it is possible to prioritize the list of 25 Topics. The separate Topics have their importance, but given the amount of relations they have to other Topics, it can be stated that the top of the prioritized list represents the most predominant 'system-of-system'-like Topics; given the fact that these Topics relate very much to others, they are symbolic for the interdependencies in the CBRNE-system.
In this upper part of the prioritized list, five clusters of Topics are visible (see Figure 8). Below a short description of these clusters is given, together with the Top Topic numbers that represent this cluster, combined with some related Topics that are listed lower in the prioritized list.

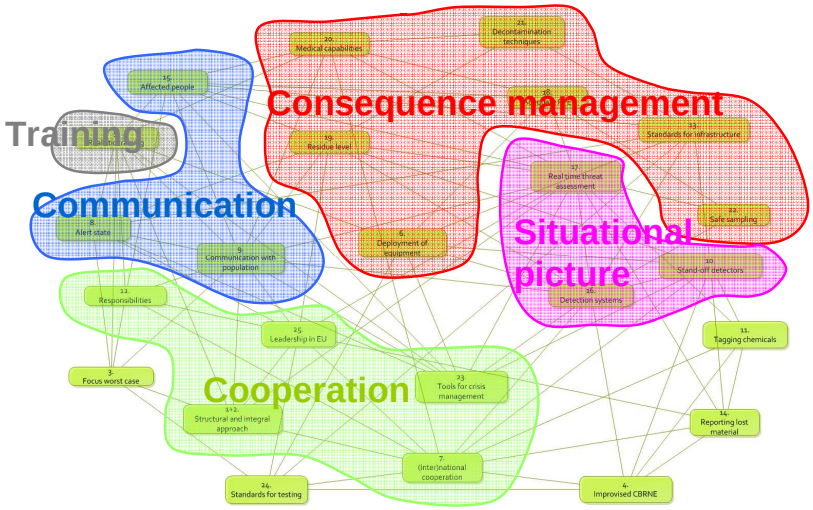


Figure 8 Roadmap Topics clustered

- **Fusion of information and establishment of a situational picture**. As an element of a continuous CBRNE threat assessment there is a need for real-time situational awareness of the dynamic aspects before, during and after an incident. This includes detection, identification and monitoring of actors, agents, means of delivery, targets and effects. Therefore the requirement is a common operational picture. In the case of assessing the CBRNE threat and impact, the validity of the perceived threat and its consequences needs to be measured and verified. (Topics no. 10, 16 and 17)
- **Communication.** Because of its low probability / high impact nature, CBRNE related communication to the general public requires special attention. In addition to general disaster management strategies, CBRNE awareness and resilience should be created. Aspects such as education, the role of local, regional, national and European authorities and the passive and active use of (social) media should be covered by a dedicated communication strategy. (Topics no. 8, 9 and 15)
- **Cooperation.** CBRNE counterterrorism involves numerous players that have different skills, knowledge levels, approaches and practical experience with CBRNE incidents. In order to minimize the impact of an incident, extensive cooperation and coordination is required between these players. The requirement is thus to link the phases the security cycle, to pool (scarce) resources, to share (classified) information, and to use best practices from separate C, B, RN, and E experiences. A lot can be learned from and shared with other domains (health, safety, environment, defence). (Topics no. 1+2, 7, 12, 13, 23 and 25)
- **Consequence management**. Many activities focused on an efficient handling of an incident require further improvement. Mostly post-incident activities (the response and recovery phases) are concerned, but these have a substantial relationship with pre-incident activities. These involve medical countermeasures as well as dealing with the effected infrastructure and area. Topics to be

demonstrated are:, search and rescue, triage, on-site medical care as well as transport to and treatment in hospitals, containment/quarantine, self help, decontamination of people/infrastructure/area, and dealing with chaos and the (longer term) psychosocial effects. Furthermore, adequate (personal) protection is an important aspect. Dedicated solutions are not always realistic and therefore integration with existing protection measures is required. (Topics no. 6, 13, 18, 19, 20, 21 and 22)

- **Realistic training and exercise**. Current training and exercise does not fully reflect the complexity of CBRNE counterterrorism. Given the large impact and the organizational and financial burden of real-life exercises, new techniques (like the use of virtual reality and serious gaming) need to be further explored, developed and demonstrated to meet both needs and restrictions. There is a strong need to include aspects such as live agents, general population, and cross border cooperation. (Topic no. 5)

When looking at the bottom of the prioritized list, this does **not** resemble unimportant Topics. These Topics are more stand-alone, and by solving these issues a niche problem is countered (Topics 3, 4, 11, 14, and 24).

Annex 1 Introduction to the roadmap topics

For the writing of the Topic documents, the structure presented below was used. Here each of the headings is briefly explained.
It must be stated that the exploration on these headings in the following chapters is only touching the surface. It is easy to argue that for each of the Topics one year of research could be done to get into the 'weeds' of the Topic. Given the amount of time (and resources) available in the DECOTESSC1 project it was not possible to go into a lot of detail.

Title:
Rephrasing of the gap into a short title which reflects the topic (milestone, strategy) that goes with the gap. In fact it is a short version of the top sentence that is on the Roadmap Information Form ("The EU (its member states should be able to….").

Introduction:
A short inducement on the topic, relating to the text on the relating gap that is covered in WP7, stating the reason why this topic is important

Description of the objective
A short description of the Topic itself (more explanation than the one sentence which is covered in the title). Also the mention of the timeframe in which we think it is realistic that the objective can be realized.

Products, capabilities and services
Achieving the milestones / topics that are addressed in the roadmap does not happen 'at once'. To make this possible, certain 'things' need to be in place, for instance:

- first responders need to have a specific detection system to be able to detect a specific hazard (= the availability of a specific *product*),
- authorities need to be able to influence the general public to make sure that they move away from an incident location (= the availability of a specific *capability*),
- first responders in member states of the EU that do not have very advanced training facilities, need to be able to take a training course in an other country (= the availability of a specific *service*).

Of course these three elements can be related to each other.
The first step in exploring the Roadmap Topics was listing those products (capabilities or services) that need to be in place before one can speak of achieving the milestone.

R&D
Given the current status of science and technology, the development of certain products (capabilities or services) is 'just' a matter of time. But for others there is a need for further research to make this development possible. The second step in the exploration of the Roadmap Topics was listing those types of Research & Development that are needed to be able to develop products (capabilities or services).

Related issues and difficulties
Although (the development of) science takes up a big part of the fulfillment of the Topics, there is more in life. Given the complex and cultured society the EU is, a lot of different aspects need to be considered when talking about implementing counterterrorism measures. With the writing of the Roadmap Topics attention has been given to the following issues: legal, ethical, political, economical, societal and environmental. For each of the identified issues a first reflection is given about the level of impact that can be expected.

Relation to other Topics
Although each Topic can be seen as an individual issue, in reality most of them are related to each other. For each of the Topics the relationship with other Topics (and therefore Topics) is given.

Annex 2 Structural cross domain cooperation for an integrated counter CBRNE-terrorism approach (Topic no. 1+2)

A2.1 Introduction

CBRNE counterterrorism is a multi-facetted domain with many links to other fields of work. Because CBRN incidents have a low probability, extensive dedicated research and development is often not feasible or even desirable. This makes learning from (existing knowledge in) other domains vital for an optimal CBRNE counterterrorism approach. Lessons learnt outside the field of CBRNE counterterrorism for example regarding natural disasters or medical procedures should be considered. These lessons learnt should of course be critically reviewed to see whether they are applicable to the domain of CBRNE counterterrorism.

Many organisations and mechanisms involved in CBRNE counterterrorism do not reflect the multi-dimensional character of the domain. They are often intended for one phase of the cycle or specialised in one of the threats (C, B, R/N or E) and often strongly focussed on governmental organisations. Especially, the response phase is covered well. Within the EU, there is a general rapid alert system called ARGUS, which is linked to other specialised system such as BICHAT (biological and chemical) or ECURIE (radiological). It is further complemented with mechanisms like the Community Mechanism for Civil Protection (including the Monitoring and Information Centre (MIC) and Common Emergency and Information System (CECIS)), which are in place to coordinate actions in case of large emergencies.

The lack of common understanding and cooperation between policy makers, first responders, crisis managers, research organisations, industry and other players *within* and *outside* the field of CBRNE counterterrorism can have severe consequences. It hampers an integrated and widely accepted approach to CBRNE terrorism, inhibiting for instance shared situation awareness and timely responses to crises, including criminal investigation activities. Also, standing operating procedures for first responders differ from country to country, which will affect negatively responses.

An important spin off of increased cooperation will be that double work, for example in developing new technologies, can be diminished. Conflicting approaches and procedures in cases of emergency will become clear and can be solved.

An integral approach to counter CBRNE-terrorism is essential in order to incorporate lessons learnt from health and environmental services, safety organisations and knowledge coming from sciences like psychology, information and technology.

A2.2 Description of the objective

An integral approach to CBRNE counterterrorism is required. Dedicated organisations on a national level are needed to bring together relevant scientific and operational expertise, intelligence, innovative solutions, and to promote cooperation. As many countries already have counterterrorism offices or dedicated CBRNE networks, the goal is integrate these and expand to other relevant institutions. On the EU level, a network that connects organisations and institutions from all member states working within the field of CBRNE counterterrorism has to be created. This network needs to have strong links to other domains that are relevant for CBRNE counterterrorism.

The creation of the network is foreseen for 2015. While there are already many organisations on Member State and EU level and initiatives to bridge gaps – for instance between civil and military, or

health and security – the first step will be to bring these together. Responsible authorities, often already existing, need to be appointed on short notice. Their first task will be to map and connect existing networks, cooperation efforts etc. relevant for an integral approach to counterterrorism. This should be finished by 2013. In the next step, multiple tracks will be followed. For one, a virtual environment and database enabling information sharing has to be created. It is foreseen that there will be ethical and technical challenges, which means that implementation is not likely before 2015. Other initiatives will be to organise common training and excercises, including curricula, and symposia in order to integrate all relevent domains. First excercises and symposia can be held in 2014.

A2.3 Products, capabilities and services

The first step for the integrated CBNRE counterterrorism approach will be the creation of a platform and a network of relevant organisations and institutions. The network will be composed of policy makers, national authorities, RTOs, industry working in the field of CBRN. Related and relevant domains should be identified and points of contact with these domains should be established. The network will continuously develop (new) connections.

To support the organisation in bringing together the network and different disciplines, some underlying products, capabilities and services need to be developed:

- A virtual environment in which connected organisations and institutions are able to present themselves, to work on common standards and regulations, to share and discuss best practices, and results of research. Using a web-based approach cooperation and facilitate information sharing will be supported. Part of the virtual environment will contain classified information; necessary precautions are taken to secure this information.
- On a regular basis, symposia will be organised to promote multidisciplinary and cross institutional sharing of latest insights regarding operational procedures, scientific research and innovative solutions etc. promoting an integral approach to countering CBRNE-terrorism.
- The network should facilitate the process for drafting common risk based scenarios, which challenge multiple stakeholders and multinational cooperation. Even so, lessons learnt from other domains can be tested on their viability for CBRNE counterterrorism. Based on these scenarios an integral approach can be developed.
- Support to cross-border and cross-domain training and exercises. The network will provide assistance in preparing cross border and cross domain training and exercises of first responders and organisations involved in crisis management

The prime stakeholder for creating an EU network will be the EU commission. As stated before, there are already some EU institutions in place that might take the lead in the process. The member states will create national institutions. In some countries, first steps in this direction have already been taken.

A2.4 R&D

The above mentioned integrated CBRNE counterterrorism approach requires a clear analysis of relevant organisations. All CBRNE stakeholders need to be mapped, on a national and EU wide level. The roles, responsibilities and interdependencies of all players need to be explored to show gaps or overlaps.

Furthermore, research has to show whether current databases can be adapted to new organisations and data or if a new database has to be developped. It is important that the database is suitable for sharing information in a secured way including between organisations and institutions which are normally not allowed access to a classified system. Therefore the database needs different layers of access for different participants in the network.

The relevancy of capabilities, procedures and knowledge coming from other domains for CBRNE field of work should be investigated. Part of this investigation is an assessment of quick win solutions: prooven techniques, procedures etc. which will enhance CBRNE counterterrorism efforts.

Common standards need to be developed – for instance for scenarios – in order to create a common understanding of the definitions and objectives of CBRN counterterrorism between all players.

A2.5 Related issues and difficulties

A successful creation of a network dedicated to structural cooperation within member states and across borders will strongly depend on mutual trust among participating organisations and institutions, promoting confidence, overcoming legal objections to sharing classified information and ensuring a secured environment for cooperation. There is a need to find a balance between several aspects:

- Promoting trust and cooperation between organisations which have at times conflicting and/or overlapping goals and responsibilities. The best approach will be to proceed step-by-step in order to build up mutual confidence. A common dialogue and understanding is needed to overcome cultural differences. Implementing quick win solutions might be a good way to proceed, because it will provide an (constant) impetus for cooperation.
- Sharing as much information as possible and bringing together as many relevant parties, while at the same time ensuring information security. The goal is to incorporate knowledge from as many domains as possible. This will certainly raise questions about (information) security issues. Classified information of the government and business sensitive knowledge are some examples which are at odds with cooperation.
- The bottom line will be the question whether or not cooperation is beneficial for all participating organisations. This will require that, right from the beginning of the process leading to increased cooperation; it has to be made clear what the added value is. The exact advantage is difficult to determine at forehand and will differ for each organisation.

A2.6 Relation to other Topics

The subject of this roadmap can be seen as an organisational solution in countering CBRNE terrorism. Therefore it is strongly linked to many other Topics, like for instance the limited cooperation and sharing of information, nationally and internationally (Topic 7). Also, the lack of EU leadership (addressed in Topic 25) is highly connected. In short, the proposed network will also tackle these Topics.

Annex 3 CBRNE Threat assessment based on a set of validated scenarios (Topic no.3)

A3.1 Introduction

When considering the potential risks and the consequences related to a given threat, there is a general tendency to concentrate the attention to the scenario that generate the most dramatic consequences (*worst case scenario*). In the case of terrorist attack with CBRNE, the attention is often attracted by the catastrophic scenario of the successful deployment of a high potential Weapon of Mass Destruction, such as a nuclear bomb or a weapons-grade bioagent, producing a huge disaster. This is based on the underlying assumption that if enough protection is provided to handle the worst-case scenario, then protection is sufficient for any kind of scenario. However, this assumption is not always correct: There are cases in which countermeasures designed for the "worst" scenario are of little or no help for a less severe scenario. Furthermore, the definition of the "worst" scenario itself is usually based only on the first order effects (e.g. number of casualties), not taking into consideration the secondary and tertiary effects, i.e. impact to the society. Finally, this approach does not always consider the fact that, in order to succeed in such a "worst case" attack, terrorists would need to have access to extremely protected material, to acquire sophisticated components, to have specific and deep knowledge, to avoid the possibility of being detected during the preparation, and so on. All these factors make the worst case very unlikely to happen in practice. Other types of attacks, producing lighter consequences but being much easier to accomplish, need to be considered much more in a comprehensive and balanced threat assessment approach.

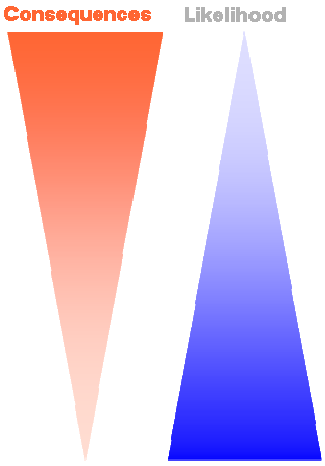
A3.2 Description of the objective

The EU and the Member States should be able to base their CBRNE countermeasures on a balanced and comprehensive scenario-based threat assessment – not just on a worst-case approach. This threat assessment should be:

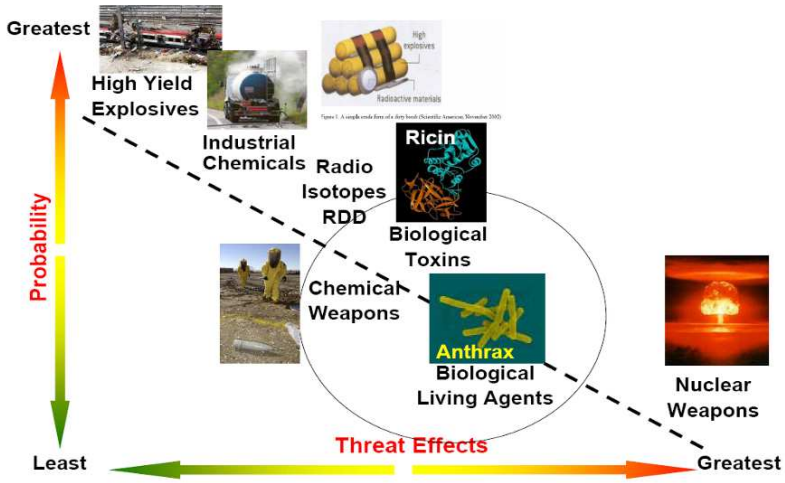
- based on the combination of both consequences and likelihood, i.e. it should be risk-based
- taking into consideration not only 1st order effects, but also 2nd and 3rd order effects
- considering the complete range of scenarios (scenario-based) and addressing the most important of them, following screening and risk-based selection that should be included in the threat assessment. The range of scenarios should be complete both in terms of possible agents used (E, C, B, R, N) and in terms of means of delivery and routes of exposure (including food, water, air, contaminated surfaces)
- being able to distinguish real threats from hoaxes.

The importance of taking both the likelihood and the severity of consequences can be demonstrated by taking the RN threats as an example: It is easy to show that there is a sort of inverse proportionality between the consequences (in terms of number of casualties) and the likelihood of a successful attack (linked to the degree of difficulty) for four different types of RN attacks: a full potential nuclear weapon, and improvised nuclear device, sabotage of a nuclear plant and a dirty radiological bomb.

- **Seizure of Nuclear Weapons–** of particular concern are thousands of deployed and stored nuclear weapons and materials
- **Theft or Purchase of Fissile Material to Build a Nuclear Explosive Device–** an improvised nuclear device (IND)
- **Attack on or Sabotage of Nuclear Facilities,** including nuclear power plants spent fuel storage sites or weapons production facility
- **Manufacture of Radiological Dispersal Devices (RDDs)** (such as *dirty bombs*)



Similar considerations can be done in the general CBRNE space: Traditional attacks with conventional explosives are generally producing less direct consequences than attacks with combined threatening material (CE, BE or RE), while the likelihood of conventional attacks is much higher than the likelihood of complex attacks involving CBRN material. This is illustrated in the following diagram, prepared by CEA, one of DECOTESSC1 partners. Clearly, all areas of the (probability-consequences) space need to be considered in threat analysis and all possible threatening materials, with possible combinations.



Another very important point is the need for the assessment of consequences to be extended to 2nd and 3rd order effects – not only direct casualties, in order to assess the impact of the attack to the society rather than to individuals. It is necessary to always keep in mind that the main target of any terrorist act is the society, not the individuals. In most cases the terrorist aims at creating these 2nd and 3rd order effects (interruptions of services, spreading of terror, etc.) rather than to the 1st order consequences. Furthermore, the "system-of-systems" approach requires employing a 3-layer model of the society, assessing the probable effects to all 3 layers and designing countermeasures according to these impacts.

The ability of a comprehensive threat assessment method to distinguish between real threats and hoaxes and to provide guidance on how to distinguish and how to deal with them is certainly a need and an important gap that needs to be covered.

A3.3 Products, capabilities and services

There is a clear need for a risk-based approach in threat assessment of CBRNE events. The challenging tasks here are: (a) assessing the 2nd and 3rd order effects; (b) assessing the likelihood of a successful attack, or – indeed – those components of the likelihood that can be controlled; and (c) combining consequences with likelihood in a risk-based metric, useful for planning countermeasures and protection strategies.

Generally, in safety assessment the risk is defined as the product of the probability of an event multiplied by the consequences:

R (risk) = P (probability) * C (consequences)

In the field of security the application of a comprehensive and rigorous risk evaluation is quite complex. In fact, if it is relatively easy to estimate the direct consequences of an attack, it can be difficult to have a correct evaluation of the probability of success due to the strong importance in the process of the human factor and his decisional process. In fact when analysing a typical accident in a safety risk study, most of the events are linked to success/unavailability/failure of subsystems that can be accurately determined in statistical terms. In a terrorist attack we often need to be able to determine the probability that a person takes a decision or not and this depends not only on mechanistic processes, but also on human behavioural aspects. To overpass this bottleneck, the analysis needs to focus on those elements of the probability of an attack that can be influenced, such as the availability of high-risk chemicals, or radicalization of people. Therefore there is a need for **research on better understanding what determines the likelihood of attacks, which of these elements can be influenced and how**.

A capability to have a reliable and accurate method to assess the risk connected to the different types of CBRNE attacks is necessary in order to plan in an efficient way the resources for counteracting. Focusing only (or too much) on the worst case scenario would expose the community to events that even though may have lower impact, may happen in practice more frequently and cumulate heavy costs on the long term.
The influence of scenario on training is also important. Training needs to be based on realistic scenarios, which should be debated and validated as much as possible. A complete categorization of scenarios, ranging from low- to high-consequences level, is absolutely essential. Furthermore, the validation and application of risk-based methods in threat assessment can be promoted through national and international Operational Centres of Expertise. In that context, and in the development and validation of methods and tools, the involvement of the private sector can also be investigated in a public-private partnership (PPP). A clear distinction between threat assessment and risk assessment should also be made.
Various experts need to be involved in the development of these capabilities, with multidisciplinary background. The involvement of law enforcement and rescue services is also essential.

A3.4 R&D

Implementation of the human factor effect into system analysis methodologies for risk evaluation is the most challenging issue in threat assessment for CBRNE hazards. It requires the introduction of psychological, anthropological and cultural issues into stochastic algorithms. Decisional process may change the strategy during the attack, so generating non-constant success/failure probabilities. Game theory and other similar disciplines may help in improving the correct calculation of probability.
Research is needed to better understand what determines the likelihood of attacks, which of these elements can be influenced and how.
Additional research is necessary in order to get sufficient insight into 2nd and 3rd order effects. It is essential to understand the link between 1st order consequences (casualties) and 2nd and 3rd order effects, as well as whether there are measures interrupting these links.

It is also necessary to develop a database of past incidents and a systematic method to identify and extract lessons to be learned. This will not only provide trends in terrorism activity, but will provide valuable feedback for better understanding the dynamics of attacks and for determining necessary data of threat assessment.
Once the methodology is available, a comprehensive and systematic analysis will be required to scan a large amount of case studies covering all the possible scenarios.
This will have then to be categorized and ranked in terms of higher to lower risk in order to serve as input to a comprehensive risk/benefit analysis, for instance when considering the opportunity to deploy or not certain countermeasure actions.
Transfer of the risk analysis methodology to final users (mostly law enforcement and national authorities) will require also an intensive educational and training effort.

A3.5 Related issues and difficulties

There can be some initial costs related to R&D and then to training, but they will be compensated by an increase of the global efficiency of the security system and by a public perception of a security feeling.

Willingness and methods to securely exchange sensitive information concerning vulnerabilities has to be considered. Difficulties related with the development and population of the incident database also have to be overcome.

An additional societal issue that requires proper attention is the difficulty to explain to the society that protection is not anymore based on worst case. Indeed, it is difficult to explain to society and end users that worst-case scenarios are not used or less used. People in general believe that they are less protected if worst-case scenarios are not considered.

A3.6 Relation to other Topics

Topic 3 is related to the other Topics in threat assessment and to Topics in decision making procedures for deployment of countermeasures, especially with Topics 1 and 2 (structural and integral approach). Addressing this Topic has also positive influence to resolving Topic 9 (communication with population) and to Topic 5 (realistic training).

Annex 4 Effective research on improvised CBRNE devices and identification measures for illicit production facilities (Topic no. 4)

A4.1 Introduction

The use of Improvised Explosives Devices (IEDs) is the most often used vector applied for terrorist attacks. Improvised Explosives Devices are made of military, commercial or homemade explosives being used in an improvised manner for producing an explosive charge. An IED may be combined with radioactive ("dirty bomb"), chemical or biological materials to increase the effects of the terrorist attack on people or infrastructure by dispersion of the agents over a large zone. The recent attacks have shown the great imagination of terrorists to synthesize explosives and to prepare the explosive device (printer in a cargo).
Priority is made here on the early detection of the illicit production of explosives. Improvised explosives may be easily synthesised using normal household chemicals, so-called precursors, in homemade terrorist kitchens. Emissions coming from such kitchens and from illicit storage rooms may provide a future detection possibility if appropriate new detectors are developed.
The IEDs contain several components (main charge, igniter, booster, wires, timer, containment) which might be assembled shortly before the bomb will be set to the place for an attack.
Therefore to prevent a terrorist to execute an attack, the detection of precursor chemicals and explosives in particular to identify illicit explosives production facilities, the detection of explosives and assembled IEDs in a lot of civil environments such as stations, airports, infrastructures, streets and in safe condition for the intelligence services and first responders are the gaps to overcome.

A4.2 Description of the objective

Main objective is to have effective *capabilities* for the detection of illicit production facilities of precursors and explosives, for the detection and identification of explosives in improvised CBRNE devices and in safe condition for intelligence services in the prevention phase and for first responders in the preparedness and responses phase. A further objective might consider also that the detection and identification procedures may benefit of the use of a database with specifications and characteristics of improvised explosives and detection methods and include web monitoring to detect attack preparedness.

The timeframe of this objective is 2018 although certain tasks should start immediately and could be accomplished earlier. The timeframe of realising the mentioned capabilities is mid-to long term.

A4.3 Products, capabilities and services

- Special detection equipment (capabilities)

When prevention activities have failed or have been circumvented, it is up to detection tools and practices to limit the risk of criminal activities with the use of explosives. Different components of an explosive device can be transported by different persons, and an IED can then be constructed or mixed on-site. The future developed detection tools (including the detection of the initiator of the explosive) and strategies for improvised explosives or precursors might contribute to find terrorist kitchens for homemade synthesis of explosives and storage rooms or to counteract illicit transportation issues before a bomb is assembled and set in place.

Studies regarding improvised explosives devices should look at potential vapour plumes coming out of IEDs as well as realistic surface concentrations.
The list of potential improvised explosive materials used in terrorist attacks is quite large.

A lot of detection methods have been developed mainly for the aviation security. Bulk explosives detection techniques including metal detectors, trace detection systems for vapour or particle analysis, stand-off explosives detection systems, imaging detection techniques and scanners, detection of explosives with some animals have to be improved and combined to cover the entire threat. A major problem to overcome is applying these techniques to other scenarios such as the subway system, sport arenas or open spaces such as market place to detect the transportation of single improvised bomb components or precursors as well as to test them for the detection of terrorist homemade kitchens.

- Remote expert support (service)

A network of experts on explosives and on the detection of explosives has to become a permanent structure (A Network on Detection of Explosive -NDE- is now financed by DG HOME for a limited period of time). This network could have a supportive role in case of crisis and could for example organise regular events (such as a conference on detection of explosives, demonstration of technologies, etc.) on relevant topics. It could aggregate information from across the Member States on their national activities regarding characterisation of explosives and detection of explosives, create and support work of an e-community on detection.

However, the network would not substitute any responsibilities of the public authorities (particularly not regarding scenario and requirements identification). Private sector (both solution providers and solution “clients”) could be part of the network.

- Web monitoring

Internet is both a great source of information and at the same time used for dissemination of information on bomb making which causes significant dangers. Today teenagers construct bombs at home getting instructions and ordering the necessary ingredients via the Internet. How to deal with the access to information and to materials on bomb making via the Internet is a broad issue. This concerns not only the explosives compounds but also the synthesis of dangerous chemical agents and of biological agents.

The survey of internet is to identify people that disseminate information on bomb making, to identify people that are searching information on how to construct bombs and how to order the necessary ingredients. It needs to use search engines and to work with Internet Service Providers.

- Database for technical data on explosives

A database containing the specifications of explosives produced within the EU could be created. The database would target specifications of explosives needed by the forensic community and by the experts on detection. The database should also identify best practices of detection solutions usage and deployment, training and skills requirements, generalised results of tests, types of solutions and their best application, a sort of equipment manual etc.

Such data may be useful for enhanced detection probability as well as for forensic investigation. Existing network (e.g., forensic network) could share such data or databases could be managed by a Member State or by other relevant organisation such as Europol.

National security authorities would have as complete information as possible about the explosive.

- Knowledge exchange with other areas e.g. Military

Armed forces have great experiences on detection of explosives and IEDs during the peace-keeping missions all around the world. This knowledge has to be exchanged with civil bomb disposal teams and first responders.

A4.4 R&D

- Detection equipment usable for CBRNE

Given the threats of Improvised Explosive Devices to security in general and airport security in particular, measures aimed at improving the usage of detection technologies should be contemplated, in particular for hold luggage. Research in this area should be supported. In addition, cargo which is transported on a passenger plane should be subject to the same security procedures as hand and hold luggage. All the detection systems contribute to prevent illicit trafficking of threatening material. But the control of traffic at harbours and airports is challenging due to the high amount of maritime containers or airplane cargos to control. There is no efficient system at that time able to detect threat materials without perturbing the flow of goods and people.

A comprehensive approach to detection is necessary. The detection of explosives can be achieved with various techniques including volume detection systems, sniffer dogs, trace detection systems. Practice has shown however that the use of a single detection technique may not lead to satisfactory results when it comes to the detection of explosives. Consequently, a combination of methods may be necessary. Research on heterogeneous data fusion to give an alert and identify the threat has to be amplified.

The detection of illicit substances during the production/purchasing phase is also prevention of an attack and research projects are needed for the detection of unauthorised synthesis of explosives and their precursors.

The precursors to explosives include any chemical compounds or elements that can be converted to an explosive compound through a chemical reaction or series of reactions. They are generally legal to purchase, store and use. Further research should be conducted concerning enhancing detectability (additives). The usual focus is on enhancement of detection equipment capability to detect explosives. However, the problem could be partially addressed by enhancing detectability of commercially available explosives and relevant precursors. This could be done by additives. At the same time, the additives could serve also for the purpose of traceability. Research is needed to define additives to precursors to prevent precursors from being used to manufacture explosive devices.

As most of the information related to the detection of explosives may be sensitive and/or classified (studies regarding the impact of improvised explosives devices, analysis of typical concentrations of such formulations in different containments, test available and future developed detection systems for the detection of illicit production facilities, especially precursors and improvised explosives etc.), any follow-up activities in this area will have to take this into consideration.
This should be done while always taking due consideration of the applicable security rules.

- Web research

Internet is both a great source of information and at the same time used for dissemination of information on bomb making which causes significant dangers. Advanced information processing tools are necessary to analyse the web content. The previous mentioned network of experts has to be involved. The monitoring of specific websites has to be done with specific search engines and with Internet Service Providers. Harmonisation of criminal sanctions across the EU for those who distribute bomb making expertise has to be prepared by the Commission.

- Case studies and research

The establishment of scenarios and requirements for civil security (where is detection of explosives needed? What and how much of it should be detected?) are essential for future work. Such scenarios are necessary in order to be able to focus resources and research; concentrate the debate on specific and concrete issues and problems; enhance the understanding of the problems of relevant actors across the EU including the challenge of the time of detection and false/positive alarm rates. The scenarios could be developed on the basis of sectors/security missions (e.g. aviation, mass transit, major events, forensics, bomb disposal detection, etc.).

- Related to tagging chemicals, finding modification to substances

The vast number of chemicals available on the market coupled with the fact that hundreds of chemicals have explosive potential in ambient conditions creates an extremely complicated environment for addressing the issue of the security of explosives. What complicates the issue further is that thousands of compounds can react together to make explosive materials without a need for sophisticated equipment.
Possible measures involve modifications to, or restrictions on, the nature of chemicals available. Some measures have been already identified which would make the use of certain precursors in manufacturing improvised explosives devices more difficult and might prevent their use by terrorists. Research and development into additives (to prevent the use of the precursor in explosive) and inhibitors (to suppress the explosive properties) may help in finding improved measures.

A4.5 Related issues and difficulties

- Legal/Ethical issues with web monitoring

The survey of internet is to identify people that disseminate information on bomb making, to identify people that are searching information on how to construct bombs and how to order the necessary ingredients. The web monitoring (collection, processing, analysis and communication of open source information) has to comply with legal considerations and has to respect the principles of privacy and data protection of citizens.

- Economical issues: high research costs

The list of potential energetic materials used in terrorist attack is quite large and especially the spectrum of improvised homemade explosives is still enlarging. Due to the various natures of the explosives and the various types of IEDs and scenarios of attacks, the detection and identification of improvised CBRNE devices and production facilities needs a large panel of detection methods and a large set of experiments with dangerous materials that need specific security procedure. This generates high research costs of development and test. For example the program launched recently by Spain costs already 20 M€.
Concerning the tagging of chemicals or the modification of substances to prevent their use by terrorists, the financial impact for the producers or manufactures has to be limited.

- Database requires confidence.

While very useful, the database approach will face highly classification issues and has the danger of even stimulating improvised explosive production.

As most of the information related to the detection of explosives may be sensitive and/or classified, any follow-up activities in this area will have to take this into consideration. Therefore, the work in this field could be pursued in an approach based on secured and trusty exchange of classified information inside the EU.

A4.6 Relation to other Topics

Topic 7 ((inter)national cooperation): the research and localization of illicit production facilities may be facilitated by collaboration between the various actors in charge of intelligence survey of illicit activities and by sharing information (even classified) between the various actors.

Topic 10 (stand-off detectors): similar techniques may be used for the stand-off detection of explosives and chemicals agents and for the detection of products emitted by illicit production facilities.

Topic 11 (tagging chemicals): chemicals that are used for explosives fabrication could serve for the effective research and identification of improvised CBRN devices and production facilities.

Topic 16 (detection systems): on the development of multithreat detectors can increase the chance to identify “dirty bombs” i.e. find bombs by identifying gamma-radiation.

Topic 24 (standards in testing): the sensors to search and identify improvised CBRNE devices and production facilities need defined parameters and standards.

Annex 5 Common realistic EU-curriculum to CBRNE training, with the use of new techniques (Topic no. 5)

A5.1 Introduction

Modern society is vulnerable to CBRNE terrorist attacks. Despite the low probability nature of the threat, the impact of these attacks is expected to be very high. Training (and exercise) lies at the basis of every kind of preparation for a CBRNE incident. Without realistic practice in advance, the effectiveness of authorities (including police, fire brigade, (emergency) health organizations, government, etc.) before, during and after crisis moments will be significantly lower.
Furthermore, training is ideal for bringing organizations together and increasing mutual understanding, for testing new equipment and evaluating, improving and tuning procedures (see also [1]).
'Rivalry' between organisations can be an obstacle for effective performance of crisis management authorities and first responders. The basic starting point should be that training *together* will lead to increased mutual understanding, adaption and perfection of procedures, and therefore improves overall performance during crisis situations.
Specific characteristics of CBRNE-incidents (scale, complexity and financial burden) make that today training often is limited to small elements of an incident. Also due to these facts, great differences exist between the training curricula of the different member states. These existing curricula can be used as a basis for further exploration towards more integration and realism as well as existing EU- and member state initiatives.

A5.2 Description of the objective

To achieve a comparable level of expertise amongst EU-first responders, a common approach between the EU and its member states to CBRNE training is needed. In practice this means that the EU and its member states have to develop a curriculum for CBRNE training which provides a realistic and solid ground for training first responders and crisis managers. This curriculum can, at first be in practice within a couple of years, but to be fully operational a short decade is needed.
CBRNE training is meant to prepare first responders and crisis management authorities in case of a CBRNE incident. A realistic setting for training is seen as an important condition for improving their performances. Realism means developing training (and exercises) in which:

- multiple organisations are involved,
- at times cross-border assistance is required,
- at times the population is included,
- the interaction between multiple phases in the security cycle is included,
- cross border and/or multiple event(s) will occur, and
- in some occasions a life agent will be deployed.

Given the large impact and the organisational and financial burden of real-life exercises described above, new techniques from educational sciences (like the use of virtual reality and serious gaming) need to be further explored to meet both the need and restrictions. Preferably, training should take place in a (semi-)operational context, including simulation if required or more feasible.

A5.3 Products, capabilities and services

The main product of a common CBRNE training for EU member states will be an extensive curriculum. This curriculum consists of two main parts: (a) a list of existing training facilities that can be used throughout Europe and (b) a guideline for developing new training, that can/ has to include several elements:

- A realistic set of training scenario's, or at least guidelines on how to develop realistic scenario's and the elements they should contain,
- A number of agreed exercise methods; training can be conducted in several ways, but given a certain level of effectiveness handling crisis situations, certain methods have more preference than others. Best practices from several countries can be used to determine these methods.
- Insight in the behaviour of agents after a release; to build realistic training, knowledge of the realistic evolution of an incident is crucial. One of the elements in this evolution is the dispersion of CBRN-agents in built area,
- Insight in the behaviour of people (first responders and public) in case of a man-made CBRNE-incident. Also relating to the evolution of an incident, people that are involved behave in such a way that this influences the handling, positive or negative,
- Insight in the operational functions that take place before and after an incident,
- Insight and guidelines in the use of life agents during training and exercises,
- (technical) Means available to support the training (e.g. manuals, simulation tools, exercise fields for life agent training, observations tools). New techniques from educational sciences should be available as well: for example virtual reality and/ or serious gaming provides the opportunity to train first responders and crisis managers in situations which be difficult to replicate in real life exercises. For instance, very large number of persons, life agents and weather conditions are aspects which are difficult to control but can have a major influence on situations.

The curriculum can contain of a generic component, relevant to all stakeholders but also includes specific curricula (courses, elements, etc.) for specialists involved with handling CBRNE-incidents. CBRNE-incidents. Any exercise should be finalized by a structured feedback-session collecting lessons learned from training participants and organizers to maximise efficiency of the exercise.

A5.4 R&D

For the development of a representative set of scenario's, that reflects the realism of CBRNE-incidents, more research needs to be conducted to identify what makes a set representative and what elements should be included in those scenario's.
The dispersion of CBRN-agents within built areas is not common knowledge and should further be explored, in a way that complex sites can easily be modelled by authorities that make prediction of contaminated areas.
Research needs to be done in the field of behaviour of the public in CBRNE-incidents and the operational functions that take place before, during and after an incident and the way both react upon each other.
Next to this, there needs to be research in how these elements can be included in training, learning from educational sciences as much as possible.. Training methods should be developed and/or chosen that match best the operational requirements, given the restrains on finance and time. New techniques from educational science should be fully explored, like Virtual Reality.

A5.5 Related issues and difficulties

A common approach to realistic CBRNE training will be confronted by several challenges. The first challenge is creating an approach which is supported by relevant stakeholders; defining a common ground, encompassing different organisations and nations, requires consideration of responsibilities of involved organisations.

Training in populated areas will effect daily life and therefore call for reluctance from general public (and may be authorities).
Drafting a list of existing training facilities, making sure that they are available for foreign use as well, can increase the burden of those facilities and therefore make nations reluctant to open up their facilities. On the other hand this might be a possibility for those training facilities to open up for new customer groups (inside and outside their own country), which rises the viability of those facilities.

Looking at increasing realism in training, especially for training with life agents there will be issues about regulations but also the willingness of nations (and first responders) to experience this kind of exercises. Beside that, environmental but also health and safety issues have to be taken into account when implementing life agent training facilities in a standardized EU-curriculum. It should be carefully evaluated whether this type of training is needed and what the added value can be expected from it.

Cross-border training means a major effort but experiences exist that such kind of events are very valuable and increase the willingness of organisations to cooperate across borders. Some of the difficulties may be overcome with virtual training techniques and learning from experiences in other areas of security.

A5.6 Relation to other Topics

In general this Topic relates to all of the other Topics, since training is the 'precursor' of the 'real-thing'. Therefore all aspects addressed in the Topics can (or should) be incorporated in realistic training and exercises; from communication to the public till specific decontamination techniques. But, given the exponential increase in complexity and financial burden to realise this total integration, there can be selected a number of Topics that have a more intense relation to realistic training than others.

Topics 1+2 (Structural and integral approach): working on a structural and integral approach will greatly stimulate efforts to develop a common approach to training. An EU wide network, involving relevant organisations from member states, is an excellent forum for cooperation.

Topic 3 (focus worst case): training often makes use of scenario's. When new, validated scenarios (or criteria for those scenarios) are available, they should be integrated into the EU curriculum to support an univocal approach of the topic throughout Europe.

Topic 6 (deployment of equipment): besides using equipment in practice, training is the best way of learning how to handle and use equipment. Integrating the use (new) equipment, non-experts etc. in training is therefore relevant.

Topic 8 (alert state): To test methods and procedures to create a shared situational awareness about the alert state, first responders, but also the general public can benefit from exercises in which both are trained.

Topic 9 (communication with population): A common approach to realistic CBRNE training will also touch upon the subject of common strategy for public communication. The population can be involved in exercises in order to (1) get used to government communication; what to expect from the authorities and how to deal with specific information. But also authorities (2) can use the exercise to get an insight into what type and form of communication effects the population in what way and from that derive the appropriate strategy.

Topic 15 (affected people): To test methods and procedures to identify affected people, first responders, but also the general public can benefit from exercises in which both are trained.

Topic 20 (medical capabilities): interaction between first responders and the way in which their capabilities are sufficient in handling a crisis are best explored in a real event. But to make sure that obvious flaws are tackled, training of all capabilities in their construct is necessary.

Topic 23 (tool for crisis management): the best way to test tools for crisis management in a training environment (see also the relation to Topic 20).

References

[1] ESRIF Final report, Brussels, 2009

Annex 6 Need for better deployment of equipment in terms of user friendliness (non-experts), mobility, risks etc. (Topic no. 6)

Note: The content of both Topics no. 6 and no. 18. closely relate to each other. Therefor some of the text in the Topic descriptions is the same.

A6.1 Introduction:

In the response phase, first responders need to work directly at the scene of the incident, under unknown or hazardous conditions, to save lives and to carry out the necessary interventions to minimize the threat. Often, first responders enter the threat area without knowing the exact nature or magnitude of the danger. First responders have only their equipment for protection and most of them are specific for each threat; for example, fire protection materials may not withstand other threats (besides high temperatures and thermal radiation) such as chemicals or microbiological species. This lack of multi-functionality is a gap to be solved in the next years. Aspects such as, comfort when in motion and the need to carry out necessary bodily functions are seriously hindered or lacking in some of today's protection equipment.
This is very important not only for the well-being of the first responder but also for the quality of their field work, specially when they are wearing the PPE for a long time. Another aspect to consider is the use of PPE by first responders not acquainted with it for example, firemen are not acquainted with chemical or nuclear protection equipment but may need to carry it depending upon the nature of the threat.

It is important to define what does CBRNE PPE mean, Normally, it includes two concepts:

- the equipments and wearable clothes necessary to protect intervention personnel against harmful substances (CBRN), and also against heat, dust, impact of falling objects etc.
- the perimeter barrier and detection equipments.

This gap covers the first concept, PPE, the second one will be covered by other gaps.

Technological assessment of PPE should cover a broad spectrum of aspects such as clothing materials (new materials more effective to protect first responders and to prevent them from new hazardous materials or CBRNE threat substances), non electronic equipment (such as liquids contamination detection, highly toxic vapour detection or individual decontamination) or electronic equipment to provide information about the CBRN hazards that will affect them immediately (dosimeters, sensors, etc); standards, light-weightiness, comfort, etc. Additionally, it is important to consider the sampling aspect, threshold for detection and decontamination procedures.

In connection with PPE, user-friendliness has to take into account the impairment of visual and auditory information, helmets, protective shields or CBRN full-body suits limit the view of FRs. Typically, ears are always covered and therefore, communication will normally depend on head-sets inside the helmet to support FRs communication within the team. Another aspect of usability related to the wearing of PPE is the operational functionality of detection and communication devices. Small buttons cannot be pressed when wearing heavy heat-protective gloves, small readings cannot be recognized under sub-optimal light conditions and with an eyepiece in front of the face.

A6.2 Description of the objective

The objectives proposed to achieve more comfortable and easy to use equipment are quite miscellaneous and cover a broad spectrum of developments, from the development of new materials

and functionalities of the clothes themselves, mask and dosimeters to their testing near real conditions or their standardization, not forgetting the effort needed to train first responders without the expertise on PPE for C or B threats. The time scale proposed is 5 years.

A6.3 Products, capabilities and services

1.- Improvement of PPE in terms of multi-threat, comfort, motion and reduction of potential risks.

The potential combination of more than one threat by terrorist during the attack is a possibility to have in mind during the analysis of present needs of PPE. This means that some effort should be done on R&D to develop more efficient materials for clothes in case of multi-threats including hazardous substances. The mitigation of the risk of contamination could be achieved by the integration of sensors and detectors on PPE. To cover all aspects of PPE, comfort on motion or easy of use by non-experts have to be improved. End users, industry and R&D institutions have to work together to achieve more efficient and comfortable equipment and clothes for personnel protection equipment. The time frame of this need is around 4 years.

2.-Capabilities of training for experts and non-experts in case of multi-threat.

A great effort should be done to train experts in case of multi-threat attack and to coach non-expert actors in the use of the special equipment that first responders have to use on CBRNE scenarios. It is important to train aspects such as clothing, best practices, correct use of dosimeters or alarm systems and decontamination of PPE. Civil and Military authorities and first responders' agencies in cooperation with the European Civil Protection institutions should develop a training program to cover the aspects mentioned previously. The R&D contribution on the training could be done by establishing specific exercises, developing software tools or coaching on the correct use of systems (masks, dosimeter, etc). European authorities in cooperation with R&D institutions and CBRNE experts have to analyse the viability of a European Training Institute. The time-scale proposed to acquire these capabilities is 6 years.

3.- Inventory of actual capabilities.

The inventory of actual capabilities at European level is an important need to structure, in the most efficient way, the logistics for sharing such equipment. To achieve such a goal, end users and European authorities should cooperate to define how PPE equipment could be shared along Europe and the most efficient way to do so. Time scale for the inventory could be around 4 year.

4.- Definition of new regulations and standards to incorporate innovations more efficient into PPE equipment.

It is important that the European Commission and Authorities propose common polices and guidelines to National governments to structure the integration of advances in materials and equipment for PPE. European countries should integrate into or directly adopt European Standards and regulations in their national standards. The main actors involved in the standardization processes are European, national and local agencies in cooperation with end-users and R&D institutions. The time scale would be around 6 years.

A6.4 R&D

- Development of new materials for making PPE clothing more ergonomic and efficient in case of multi-threats, mitigating the risk of user contamination and facilitating dressing. Important efforts should be done in developing new materials for protecting personnel form Chemical or Nuclear

and Radiological in combination with Biological threats. The proposed timeframe for this development is 5 years.

- Investigation on dosimeters integrated into the clothes or breathing equipment to alert first responders of exposure level or damage. The time frame is 3 years. The advances obtained in this area could be useful for other sectors like the health care, biotechnological or PPE for safety use. The development should include Aerosols for biological agent discrimination and collection.
- Research on the integration of low cost sensors in the protective clothing.
- The presence of specific substances, communicate with operation control, determine long-time exposure, etc. The time scale to integrate these developments into actual clothes is 4 to 5 years.
- The definition and harmonization of standards and protocols should follow the development of materials and the testing activities. The proposed timeframe is 6 years.
- Testing of PPE under pseudo-real conditions should be accomplished during the next 6 years.
- Improvement of present training exercises and definition of new ones including the cooperation between different actors and countries should be carried out in the next 4 years. Development of simulation tools for training exercises will help first responders in acquiring rapidly the necessary skills to carry out their job effectively.

A6.5 Related issues and difficulties

The harmonization of the actual equipment is a hard task due to complex fact like some equipment belongs to militaries or like authorities unwillingness to show their capabilities. These aspects are link to economic aspect where the cost of new equipment is important and the identification of the liability of achievement and maintenance of equipment is not clearly identified. Should it be responsibility of the sport arena owner? or should it be responsibility of the authorities? Finally, a big difficulty of this high cost equipments is their durability and their reutilization after decontamination.

A6.6 Relation to other Topics

The lack of more efficient and user friendly PPE is of vital importance for the response phase and is intimately related with the development of improved, faster and more reliable stand-off detectors. The potential impact of a multi-threat attack should be kept in mind and the development of equipment, clothes and detectors that can detect multiple threats and the degree of hazard (instead of agents). Besides the relation with Topics 10 (stand-off detectors) and 16 (detection systems)considered previously, there are strong links with Topics 18 (adequate PPE) and 24 (standards in testing).

References

Decotessc1 D6.2 / N. Brousse-Ducrocq et al. (2010): Decotescc1 Deliverable Report D.6.2 – State of the Art description.

Protective Materials for Emergency Responders. Dr. Sergey Gordeyev, NanoObservatory
http://www.observatorynano.eu/project/filesystem/files/Protective%20Materials%20for%20Emergency%20Responders%20UPLOAD.pdff

ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form:
http://www.esrif.eu/documents/esrif_final_report.pdf

European Standards: http://www.hse.gov.uk/foi/internalops/fod/om/2009/03.htm

Protective Materials for Emergency Responders. ObservatoryNano (2010)

http://www.observatorynano.eu/project/filesystem/files/Protective%20Materials%20for%20Emergency%20Responders%20UPLOAD.pdf

Workshop on Chemical, Biological, Radiological and Nuclear Research.
http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4574

Annex 7 Effective sharing of information on EU level (Topic no. 7)

A7.1 Introduction

Since terrorism is international, where the actors and information often move between countries, it is necessary that the counter actors in different countries can share information. The information to exchange is from the exchange of scientific and technique knowledge, through the exchange of best practices up to the exchange of sensitive information concerning the threat level. At the international level, for example concerning the airplane security, sharing information is effective between the actors but it has to be generalized in all other domains.

Today there is a gap of uniform EU-wide synchronised structures on how different kinds of authorities, such as for instance the police, intelligence and the customs, in the member states exchange information, and a lack in natural collaboration ways. Different authorities also lack an easy and fast way of exchanging classified material, there is a need for technical development in this case. For example it is impossible to email information of higher level than restricted today. Since different authorities often have different cultures, it is necessary with a common information sharing policy for authorities, something which today often has gaps, possibly due to lack awareness of other organisations and resources, lack of clear communication channels or difficulties due to legislation and/or regulations. The legal and regulatory aspects are also a problem in the collaboration and communication between military (e.g. the NATO) and civilian authorities.

A7.2 Description of the objective

The main objective is to create a better link between existing communication structures, organisations and standards for the purpose of information sharing on EU-level (e.g. Europol, MIC, CECIS, ARGUS, NATO etc.) or when necessary to create such structures and organisations in fields where there is a lack of them (especially in the field of communication structures for information sharing and cooperation before an incident or a crisis occurs there is a lack of sufficient sharing of information and best practice at present day). These actions should allow and advance better cooperation and collaboration between national and international agencies, institutions, end-users and further in CBRNE security involved civil and military organisations. The timeframe for achieving the objective is about 3 years.

A7.3 Products, capabilities and services:

1) Capability of cooperation and collaboration between agencies or institutions on EU-level

There should be an EU-wide sharing of best practice, information and knowledge to ensure uniform technical and organisational level. All involved and relevant player like end user, national and international authorities (intelligence, police, fire fighter, military forces etc.), R&D facilities and so on should share continuously the relevant information. The timeframe for achieving a significant advancement concerning this capability is about 3 years.

2) Uniform communication and information sharing structures and channels for **unclassified**

information sharing within EU (Service)

The main instruments for uniform communication and information sharing structures are information sharing platforms in form of a network or forum. For the realisation of such platforms on one hand technical aspects like hardware and software are needed and on the other hand also legal aspects like laws, concepts and guidelines must be taken into account. At present time exists many different civil communication and information sharing structures and organisations like MIC, CECIS and ARGUS or military information sharing structures within the NATO. The unification or at least a closer cooperation between the mentioned organisations would improve the communication and information sharing within EU concerning all parts of the CBRNE counterterrorism. The timeframe for achieving these capabilities is about 3 years.

3) Communication structures and standards for sharing of **classified** information between responsible stakeholders within EU (Service)

Sharing of classified information needs a much higher security level than sharing of unclassified information. Therefore the EU-wide implementation of an encrypted communication programme (e.g. chiasmus) respectively system is mandatory. In cases when the classified information has a too high classification level to be shared by electronic or mail communication there should be a fast, reliable and uniform procedure for the information sharing by envoys. Though there was a significant improvement on EU level concerning the sharing of classified information, at present day there are still differences between different EU members and therefore a lack of unification of legal issues. The timeframe for achieving these capabilities is about 3 years.

A7.4 R&D

- Investigation on existing European communication structures, platforms, concepts, hardware and software and their possible unification. The timeframe for this investigation is about 1 year.

- Improvement of communication hardware and software for sharing classified information. The timeframe for this improvement is about 2 years starting subsequent to the finished investigation on existing European communication structures, platforms, concepts, hardware and software and their possible unification.

- Development of improved software for declassifying of documents and reports. The timeframe for this development is about 1 year.

- Research on how to improve thrust to share information. This research is mainly about psychology. The timeframe for this research is difficult to estimate.

- Research on ergonomics of communication software, hardware, concepts and platforms to ensure user-friendliness and usability. The timeframe for this research is about 2 years starting subsequent to the finished investigation on existing European communication structures, platforms, concepts, hardware and software and their possible unification.

A7.5 Related issues and difficulties

- Motivation of the people:
  People may not have the willingness and allowance to share information due to instructions of national authorities or just due to the fact that they are not seeing the need of sharing of information.

- Efficiency and user friendliness:
  The communication and information sharing structures may become too costly or time-consuming and therefore a lack of acceptance could arise.

- Classified information:
  For unifying structures an EU-wide agreement is needed. But establishing or realisation of unified structures for sharing of classified information could be not accepted by national institutions at all.

- Communication security
  The realisation of information sharing structures for classified information could fail due to problems in the field of communication security.

A7.6 Relation to other Topics

Because the sharing of information is a crucial requirement for the successful cooperation between all the different parts of the CBRNE security field there is a general relation to all other Topics. Especially with the Topic 1+2 (structural and integral approach) there is a severe connection. It is also in connection with the Topic 25 (leadership in EU).

Annex 8 Harmonized alert state protocols within the EU (Topic no. 8)

A8.1 Introduction:

When the threat level is raised, e.g. due to intelligence information, announcement or an incident, ideally all parts of the society act according to an alert state protocol. The alert states correspond to a threat level, and include action plans for all parts of the society and the communication between them and within the EU. The public needs to be aware of the current alert level, corresponding to different working methods for the different authorities and actors in the society, in order to be involved and not only receive information.

The member states today have different national alert states protocols, which are all connected through several instances within the EU who are working on the matter of crisis management and coordination. The different Directorate Generals have rapid alert and information systems within different sectors, such as the CECIS, Common Emergency Communication and Information System. The CECIS facilitates communication between the MIC, Monitoring and Information Centres, and the National Authorities, making response more efficient in case of an incident. The MIC, in turn, is the operational centre of the Community Mechanism for Civil Protection. For example, in case of a crisis a country can turn to MIC through the CECIS to ask for assistance.

The ARGUS system is a web-based system, introduced in 2006, for the internal crisis coordination of the Commission between all the different DG systems. ARGUS allows for a rapid exchange of information from sector-specific alert systems between different Directorate Generals in the Commission in the event of a risk of multi-sectoral crisis. It also provides a way to ensure communication needed for high-level political coordination during a major cross-sectoral crisis, and it provides a common source of information that will be sued by the Commission to communicate with the citizens. For example, if there is a crisis in one sector which might influence other sectors, the DG representatives can alert each other through ARGUS.

Harmonised protocols for alert states among the member states in the EU would increase the common awareness and understanding, and increase the awareness among the citizens to the threat levels and corresponding actions. It would also, together with other directed efforts, lead to a better knowledge about the crisis management of the EU among both the involved parties and the public.

A8.2 Description of the objective

Harmonisation of the different alert state protocols and plans for the member states would enable more efficient coordination of resources, help and information, and increase the understanding of the protocol of other member states.

A way to work towards the objective could be common guidelines from the Commission on how the protocols should be developed and what should be included, standardise them and implement them in the protocols of the member states. It is important to note that harmonisation does not mean that the protocols should be the same in the member states, but rather that they should be compatible and follow the same structure, and thereby understandable and easy to access for other member states. For example a specific threat might have a high risk in one MS and low risk in another or the threats or organisations might differ. The principle of the plans should be natural for responders crossing borders when forces are gathered as well as for citizens travelling across borders.

A suggestion, when drawing guidelines for the harmonisation, is to include the public as part of the alert protocols. In this time of intense migration and tourism within the EU, harmonisation and public involvement could increase the efficiency of the plans when they are put into practice.

Getting an overview of the differences between national protocols and create guidelines is estimated to be possible within a timeframe of 3 years, to thereafter adjust the national protocols and implement them in the society of the nations within another 5 years.

A8.3 Products, capabilities and services

The following capabilities are steps in the way towards harmonised alert state systems in the EU.

- Knowledge about function and capabilities of national alert state protocols should be available, to map out the current situation with weaknesses and strengths. This is a question for the European Commission to solve in collaboration with the Community mechanisms for civil protection.
- Guidelines should exist for harmonised protocols, and standards should exist for the national protocols.
- Roles of different actors in the EU crisis management system strengthened, in order to coordinate the harmonisation and guidelines. This includes implemented harmonised standards for information sharing through the EU systems, through eg. ARGUS.
- Capabilities to handle data fusion and analysis in the harmonisation process and in the continued coordination work.
- Political agreement nationally and on an EU level should be reached.
- Testing of harmonized protocols in each country and in collaboration across borders.
- Guidelines and standards implemented in national alert state protocols

A8.4 R&D

The following research and development steps are needed in order to reach the capabilities mentioned above.

- Research on the function, capabilities and weaknesses of the current alert state protocols in the member states. The research would consist of studies of already available data and studies in the respective countries.
- Research on the national differences in threat situation, geographic situation, culture etc, which might influence the alert protocol of the country.
- Development of guidelines for harmonised EU alert protocols. This should be based on the above research on current functions and national situations.
- Development of protocols nationally according to the harmonised plan. These should be in line with the guidelines. They should not be in conflict with national law.

A8.5 Related issues / difficulties

- *Legal*

The guidelines for the national alert state protocols should not enforce actions or plans in conflict with national law.

- *Ethical*

If the harmonisation leads to changes of the national protocols, responsibilities, methods etc, there can be an increased risk of mistakes such as delays, miscommunication etc. during the transition period. This could increase the risk of the citizens.

- *Political (was not explicit mentioned in the RIF)*

The harmonisation relies greatly on political will. It can also be sensitive to changes in the political climate. The project would not be possible to perform without a conclusion on this part.

The new protocols also have to be adapted by the national first responders, and there has to be a positive incitement or a clear benefit for them to do so.

- *Social*

Changing national plans under an European leadership might result in a feeling of loosing national power to the EU, which could lead to conflicts in the society.

A8.6 Relation to other Topics

Topic 9 (communication with population): Regardless if the public should be included or not as a part in the alert plans, the strategies for communication on the situation should be included in the alert state plan. If the citizens are involved in the protocols, there is also a need for strategies informing them beforehand on the plans and actions.

Topic 25 (lack of authority leadership in EU): The harmonisation needs to be guided by the crisis management centres with in the DGs or the European Commission. Therefore they need to have authority to realise their task, and the knowledge of their objective should be higher.

Topic 3 (focus worst case): There is a need to focus on the relevant scenarios at all levels in the development of guidelines and alert protocols.

Topic 5 (realistic training): This is a way to include the public in alert state plans and to create understanding of the harmonisation between protocols.

Annex 9 Effective communication with public concerning CBRNE crisis (Topic no. 9)

A9.1 Introduction

During crisis situations (but also in general), protecting social wellbeing in a society is – next to the primary actions after an incident – the most important task of authorities. It requires constant communication to and with civilian population. This communication involves people who are more or less directly connected to the incident (victims, bystanders and spectators, or providers of (spontaneous) help, local residents) but also encompasses the general public (nationally, but in some cases also internationally). Each group has a different need for information; the message of authorities has to match with these needs. "Besides their direct impact….CBRN agents pose a special challenge to manage their psychological effects on the population. …. A timely, competent and reliable communication by first responders and authorities is crucial in the management of a CBRN(E) crisis" [5].
These demands on the way of communication are easier said then done. Communication before and during a crisis is no longer the sole domain of governmental authorities and coordinating these flows of data is almost unfeasible. This has several reasons. First of all there is the simple fact that civilians are often the first to reach a crisis area (let alone when they are targeted) and also often the first to give response. With the rise of social media, and multiple means for communication within easy reach of general public, a flow of information will start, leaving the authorities without an opportunity to take the initiative. On the other hand this flow of information can be a valuable source for authorities. Secondly, the media will be attracted to the area, broadcasting their version of the situation, not seldom with their own 'self-pronounced' expert on the topic. A related factor to this is that the public does not know who to trust; there is very much information available – even contradictory – which makes it impossible to identify the 'correct' information like advise and orders by the responsible authorities. This aspect is further aggravated by the fact that it takes time for authorities to collect facts to create a coherent and 'correct' picture. By the time the official version of the incident is ready to be released, already a dozen other versions exist and authorities have a hard job assuring that their version is the correct one. Finally, there are the organizational challenges. During a crisis multiple organizations will be involved, many with their own press officers, without a clear coordinated line of communication with the population and with their own professional and social networks.
All these aspects described above often causes the authorities to seem to be behind in communication with the public *after* an incident has occurred. To some extend this can be prevented with communication *before* incidents: 'How do authorities prepare a population for crisis and inform about actions to take', and 'how do they convince the public to really use this information' are some of the questions which can be dealt with before an incident. As [1] states: "… extensive public information on the process and outcomes of risk assessments will be necessary to lead to a better understanding of the risks and to enable all stakeholders and the general public to become more engaged in emergency planning, preparedness and response." In the current situation, guidelines for crisis communication stipulate that authorities tell people what to do. Research after crisis situations has shown that these orders are often disobeyed [2]. This makes new guidelines which do effect public reaction during disasters necessary.

A9.2 Description of the objective

Communication in general can serve three purposes:

- sharing of information,

- influencing an attitude of people towards a topic/ organization and
- making people behave as one wants to.

Developing a strategy for effective crisis communication (before, during and after an incident) needs a comprehensive approach in which these three purposes need to be matched to the different groups of people; it is about getting the right information to the right audience, timely, informative and – if necessary – actionable. To maintain trust to authorities, this information should also be reliable and accurate.

Time frame: Applying recent insights in governmental communications strategies can be *started* from today, also relating to current available communication mechanism in the EU through the CCA [3]. Realization of a more matching communication strategy however can be from 2016 onwards, due to the fact that not all the necessary information and (scientific) knowledge is currently available and technology (especially for social media) will stay in development,

A9.3 Products, capabilities and services

Increasing trust of the population in authorities is an essential part of communication. Public attitude towards authorities is based on expected governmental capabilities in assuring social cohesion and showing political leadership. Furthermore governments needs to inform civilians about response capabilities, procedures etc. This will also lead to increased public awareness about potential threats and how to react during incidents. In general, governments need an information plan in which will higher level aspects (social cohesion etc.) be addressed and crisis response and management aspects will be clarified.

Effective public communication during a crisis situation will depend on several capabilities and services. The first aspect will be a clear strategy for communication, not only guidelines for the member states based on CCA, but also arrangements for EU-wide crisis (via CCA).

A clear strategy means that the authorities have a comprehensive approach which is agreed by all involved organizations and in which purpose, means, roles and relations between these aspects are clear. Clearly defined procedures and a single point of communication are important organizational aspects, supporting a sound strategy.

Media and social media will be important during crisis situations for sharing of information. The capability to interact with the public is of great meaning for dealing with victims, bystanders etc. Involved authorities (from local, national to EU) need the ability to use both kinds of media to inform the population correctly. This use refers to (1) the use as mean of communication to the public (in order to influence their behaviour), but also (2) as mean for retrieving information from the public.

Via weblogs, twitter etc. (if working during crisis) it is possible for authorities to gain insight in the real time information needs of the population and understand issues causing fear. This can be used to optimize government communication to the population. These (social) media can also be used to improve the preparedness and awareness of the population and it enables a pro-active discussion.

A9.4 R&D

The R&D portfolio for public communication during crisis will have a socio-psychological and technical component. Socio-psychological research will look for answers regarding question like:

- how does communication in general (and governmental communication specific) influence the population and in what way can new communication guidelines be development to support that;

- what kind of messages (including the content, who brings the information and format it is presented in) is suitable for which group of the population in a certain situation and how can pre-prepared messages (by authorities or companies) play a part in this;
- whether there are cultural differences within a society or the EU with regard to responding to crisis and crisis communication;
- what is or can be the role of the (public) media and press;
- how can (social) media and its applications be used in a secure way;
- how can CBRNE crisis communication learn from (un)successful experiences during other types of crisis (e.g. natural disasters and accidents)?

The technical side of public communication will be about efficient use of media. The role of social media during crisis is of course very important, not least because people will start informing each other about the situation and therefore influence the public reactions. However, social media also offer new possibilities for crisis authorities to reach infected people and to inform the population. R&D is needed for instance to find out which kind of messages are most effective, or defining strategies to deal with differing information or preventing network overload.

A9.5 Related issues and difficulties

The core of communication is information. As stated in the introduction, the government is not the only source of information and often not the first to get the message out. Attempts to regulate the flow of information might appear to be as government censorship, especially when the media is denied access to certain areas or is used by government to spread information. Trying to come to an agreement about the role of media during a crisis will face the danger of a government trying to control the press.
On the other hand, when governments start using social media to spread information to the public, this can be seen as an invasion of privacy, similar to the spreading of spam-mail to large groups of people.

Special attention needs to be paid to securing the capacity of communication lines. During crisis situation, there is a severe danger of overload of the communication network (see also [4]). The government has to assure that it has back up ways of reaching the population.

A9.6 Relation to other Topics

Topic 1+2 (Structural and integral approach): Communication to the public relates to all the different phases in the security chain; communication and the way it occurs influences the phases themselves, but also communication itself is influenced by processes that take place during phases and authorities or organizations that are involved.

Topic 5 (Realistic training): The population can be involved in exercises in order to (1) get used to government communication; what to expect from the authorities and how to deal with specific information. But also authorities (2) can use the exercise to get an insight into what type and form of communication effects the population in what way and from that derive the appropriate strategy.

Topic 8 (Alert state): Uniform knowledge and awareness about alert states with the public only can be achieved via the use of government communications. Information about these states and the appropriate action to take, for public but also other authorities and organizations involved, is one of the aspects that need to be addressed in governmental guidelines for communication with the public.

Topic 12 (Responsibilities): Given the fact that a large number of organizations is involved with CBRNE incidents, the risk increases that, from these organization, different information can/ may be

sent to the general public. Streamlining this risk is of enormous importance to uphold communication effectiveness.

Topic 15 (Affected people): To ensure finding affected people, communication is a very important medium. Not only in addressing those who are affected, but also giving the information on how and were to react.

Topic 16/17 (Detection systems and real time threat assessment): Information coming from detection system is crucial to make sure up-to-date (and correct) information is send to the public.

Topic 23 (Tools for Crisis Management): A communication strategy should be part of good crisis management; it is the way to include the general public in the upload and aftermath of an event and even in the most early stages of crisis management communication to the public can do service.

References

[1] EC SEC_2010_1626, COMMISSION STAFF WORKING PAPER
Risk Assessment and Mapping Guidelines for Disaster Management, Brussels, 2010
[2] Evacuatiebeslissingen: informatiebehoefte en advise (*Decisions on evacuation: information need and advice*), J.H. Kerstholt, C. Caljouw, TNO, 2010
[3] EU 10011/1/07 REV1, Report and revised Manual on EU emergency and crisis coordination, Brussels, 2007
[4] EU 16285/09 EU Emergency and Crisis Coordination Arrangements in Brussels (CCA) – CCA exercise 2009 (CCAEX09) - Final Evaluation Report, Brussels, 2009
[5] ESRIF Final report, Brussels, 2009

Annex 10 Effective detection of threatening CBRNE material (Topic no. 10)

A10.1 Introduction

In all areas of countermeasures against CBRNE attacks, be it threat assessment, prevention, preparedness, response or recovery it is crucial to be able to detect and, if possible, identify the threatening material. The overview of the situation and all actions to be taken depend on a fast, sensitive and reliable detection and identification. For more details see DECOTESSC1 report on WP5, especially chapter 5.4 and on WP7, chapter 3.4 and 4.4.

A10.2 Description of the objective

Current technologies for detection and identification of CBRNE material comprise a broad range of technology development levels. While for many substances useful detection devices are already on the market, for others, especially concerning the CBE threat, not even a suitable method exists (cf. DECOTESSC1 report on WP6 and WP7, chapter 4.4). Generally, the development of stand-off and instant scanning detectors, which are fast, robust, reliable, affordable and which do not disturb business continuity when applied in the prevention or preparedness phase, is an open challenge. True stand-off detectors for explosives are currently in the research status. Marketed sensors / detection instruments are capable of detecting some used E components, but simultaneous detection of all potential threat substances is not possible. Also parallel detection of e.g. C and E substances is not possible. Available E detectors are designed and applied mainly for airport security while other scenarios (open markets, stations, goods traffic etc.) are not covered / tested until today. Regarding especially B threats it is challenging to develop detectors with instantaneous detection capabilities making it unnecessary to analyse the potential threat with laboratory methods. Even developments of orthogonal sensors combining different detection principles might provide future improved capabilities to detect CBRNE threat materials. Quasi-Stand-off capabilities of future detectors might be provided by use of air- or ground-vehicles to allow detection within secure distances for the operators. Also with respect to detection of RN material improvements are desirable. Different detection and identification technologies should address different usage cases like control at subways, borders, entrances in general, large area surveillance, monitoring of goods traffic and so on (see DECOTESSC1 report on WP4, Chapter 3.3.1 “Targets”). The lack of the ability for fast scanning of huge amount of containers with respect to threatening CBRNE material claims particular attention. The timeframe for achieving the objective is about 3 to 10 years, depending on the special technology, but has to be extended for more complicated developments; in principle technology has always to be adapted to the current situation and is always to be developed.

A10.3 Products, capabilities and services

1) Effective detectors

As outlined above the availability of suitable CBRNE detectors for the different usage cases is varying a lot depending on the threatening material, the techniques and the operating sites (e.g. airports, harbours, stadiums, etc.). While for many substances, especially out of the CBE area, currently detectors are insufficient or even missing, in other cases useful devices exist. But also an improvement with respect to fast (instant monitoring), robust, fail-safe, reliable, easy-to-operate (also for non-experts, possibly automated) and affordable detection and identification is highly desirable. Where useful solutions already exist they should be tested for their applicability in different areas and implemented within a short time.

2) Automated information processing

The data analysis and interpretation is an inevitable part of getting results from detection systems. The information has to be processed to be useful for threat assessment, alerts, response strategies and so on. The processing can be done automatically (data fusion, automatic alarm, decision support interfaces etc.) or with support by experts. Related products and services are available for many detection devices, but they have to be improved and systematically developed, not least facing the ongoing development of detection techniques. Also technical and methodological solutions for the problem of false alarms (false negative and false positive) are needed.

3) Expertise

To implement and possibly also to operate highly sophisticated detection systems profound expertise is necessary. Thresholds, cut-off limits and so on have to be implemented. A related service could be offered by research institutes, state authorities or industry. It is conceivable to transfer the measured data directly to a centre where experts analyse them and support the involved category of persons like border officers, security staff, first responders, police and so on. Regarding improvised explosives devices special networking activities including bomb disposal teams, police and other users might help for developing new detection strategies as well as improved detectors even for newest threat components.

4) Procedures and User Training

It is a commonplace that the best devices are useless without proper handling. In addition the system of systems for countermeasures against CBRNE attacks needs strong interaction between all involved parts. Therefore procedures have to be defined how to use detection devices, what to do with the results and where to report. This holds for all involved category of persons in threat assessment, prevention, preparedness, response and recovery. Also joint training concepts are needed.

A10.4 R&D

- Development of improved detectors:
  As stated above, research and development of detection and identification technologies for CBRNE material stand at different technology development levels depending on the threatening substances, techniques and operating sites. Developing or improving the technologies for detection is a big task which has to be addressed in different approaches. Especially functions and capabilities such as stand-off detection, detection of all or at least more E components than today, detection of improvised threat materials and multi component detection for multi hazards (C+B+R+N) should be addressed. Furthermore the detectors should be fast, robust, reliable, affordable and not disturb business continuity. Also new fields of research, e.g. non specific B-Detection, have to be entered. Detectors resp. systems must be robust and operate reliable in different environments. References to promising ongoing research can be found in the DECOTESSC1 report on WP6. The target timeframe depends on the respective technology development level. A close cooperation between end users, manufacturers and research institutes is desirable.

- Data fusion:
  The fusion of different detection data (e.g. motions of persons and signals of threatening material) is important to get an overview of the situation or to localise sources of danger. Promising ongoing research has to be promoted and new concepts and systems have to be developed. System

solutions could be tested and developed including existing and well functioning detectors (e.g. gamma-detectors).

- Reliability of results:
  A particular attention has to be paid to the reliability of detection and analysis results, including the problem of false alarms. This is not only a problem of the detection techniques itself but also of the data analysis and may be addressed in different ways. Promising ongoing research has to be promoted and new concepts and systems have to be developed.

- Detection strategy:
  To support the defining of procedures (see above) research on optimizing of detection strategies (how to perform a systematic search, where to place detectors etc.) is recommendable, including improved sampling strategies.

A10.5 Related issues and difficulties

- CBRNE standardisation criteria and testing:
  The implementation of new detection devices poses the question of standardisation and testing. The end users want to be sure, that the techniques fulfil certain criteria and are well tested, if possible by independent laboratories. Tests have to be done in a real environment (under difficult conditions). For more details see Topic 7.

- CBRNE certification issues
  Closely related to the question of standardisation is the question of certification. A European wide accepted CBRNE certification system could help end users as well as manufacturers.

- Privacy:
  Detection procedures and scanning of private goods or persons is always connected with the problem of privacy. This has to be addressed in a systematic way.

- Safety of detection systems:
  The safety of detection systems is an issue that deserves particular attention, especially in cases where the persons who use the systems are no specialists. E.g. the safety of lasers in certain systems has to be taken into account.

- High development costs:
  As is well known the development of high tech products implies high costs. This might involve financing problems. But not investing in research or installation of new sufficient equipment would not be effective for counteract terrorists actions.

- High operational costs:
  The operation of highly sophisticated detection systems, the maintenance and the training for the personnel involved, implies certainly high costs. This might put end users off establishing the new technologies.

A10.6 Relation to other Topics

Topic 7 ((inter)national cooperation): The above outlined issues of standardisation, testing and classification are related to the general problem of sharing information as addressed in Topic 7.

Topic 13 (standards for infrastructure): Usage and development of detectors are related to the question of standards for security relevant infrastructures. These standards should be mandatory and ensure the

use of adequate detection equipment, control barriers etc. and international interoperability as addressed in Topic 13.

Topic 16 (detection systems): There might be technical or conceptual relations to another kind of detection systems that can detect multiple threats and detect degree of hazard instead of agents. This is outlined in more detail in Topic 16.

Topic 24 (standards in testing): When new developments approach the status of being ready for use they should be taken into account while developing standards and certification procedures. These are addressed in Topic 24.

Annex 11 Effective methods to tag precursor substances usable for homemade synthesis of improvised threat materials by terrorists (Topic no. 11)

A11.1 Introduction

Based on the recommendations of the explosives security expert task force group there is a strong demand on efficient tagging materials and related detection techniques which could be used for the enhanced security of citizens. Suitable taggents may help to find terrorists chemical kitchens in the neighborhood of normal houses before the terrorists can assemble an improvised explosive bomb or prepare an E attack. The actual list of E specific precursor substances until now comprises substances such as normal household chemicals, fertilizers and basic chemicals used in a lot of chemical production processes. The substance list may also be extended to e.g. typical substances which can be used for homemade production of C and B agents as well as future precursors.
As an already existing tagging method the use of EGDN, DMNB or MNT (ethyleneglycol dinitrate, dimethyldinitrobutane or mononitro toluene) should be mentioned here. Following the Montreal Convention from 1991 commercial plastic explosives should contain small amounts of the mentioned substances in order to facilitate the detection of stolen or smuggled commercial products. Due to the increased evaporation tendencies of these tagging materials smuggled explosives may be found at airports with detection equipments such as ion mobility spectrometers or chemiluminescence detectors. Also the applicability and safe transport and storage of e.g. fertilizers was recently covered by new regulations.

A11.2 Description of the objective

The objective of this subject will be to test and develop suitable tagging substances which would make it possible to detect a terrorist homemade kitchen using established or future developed detection equipments. Another option might be the addition of a taggent or additive to typical precursors which inhibits the use of the material for the production of CBRNE threat substances. The typical reactions or reaction pathways of the precursors, for e.g. in medical, technical and chemical applications, should preferably remain unchanged. Optional tagging materials should not lead to health, safety or environmental problems if added to a specific precursor substance during its normal usage. Potential solutions should be well-tuned with respect to the whole range of concentrations of household chemicals taking into account the professional use of the precursors for current technical applications. For some products the addition of for example a coloring agent may be sufficient to achieve a faster recognition of abuse, such as the coloring of fuel oil to prevent the use as gasoline for cars. Others products might need inhibiting agents making the precursors non-reactive to terrorists needs. For some precursors their fully prohibition or a limitation of their accessibility might be necessary.

Regarding the time frame of R&D projects and potentially regulating initiatives for single products and applications, overcoming the gaps will be on a mid- and long-term time scale. With the recently started EU FP7 security project PREVAIL a first step might be solved in 3 to 4 years for single substances, but further research calls for developing new strategies and product solutions will be necessary to address more or all of the most-used precursors.

A11.3 Products, capabilities and services

- Development of new and/or test of available tagging materials and/ or inhibitor substances adequate to reduce the easy use of precursors for terrorist applications

- Specific taggents, markers and inhibitors should be easy to detect, cheap and easy to integrate in precursors products not altering the normal usage / applications of the precursors
    - acetone as cleaning agent or hydrogen peroxide as disinfection agent should still be possible
    - enhanced detection capability should be tested and proved
    - normal applications and reactions of precursors in industrial processes should be unchanged if possible
- The new taggents, markers and inhibitors should be handled as all new chemicals substances and formulations (REACH, DHS etc.) meaning that their properties regarding health, safety and environmental effects are well checked
- National and EU expert groups and intelligence services should work together to ensure an update of the current list of precursors with potential for abuse by terrorists taking into account new results of threat assessment and future terrorist attacks

A11.4 R&D

- Development of suitable taggents, markers and/or inhibitors for selected precursor substances related and applicable to the normal concentrations and application pathways
- Test of especially the explosive properties of newly tagged materials / products to achieve non-reactive products
- Study the reactivity of tagged / inhibited new precursors to ensure the non-usability for terrorists needs
- Study the normal reaction pathways of tagged / inhibited precursors to retain the current technical applicability in chemical production processes as far as possible
- Evaluation of the safety, health and environmental effect of suggested taggents, markers and / or inhibitors; for example the enrichment of potential additives for fertilizers such as ammonium nitrate and related substances in the food chain should be studied in order to be sure that the additives do not have unwanted effects.

A11.5 Related issues and difficulties

In view of the widespread use of the precursor substances in all kinds of different daily applications using different product concentrations and marketed product types the development of a fit-for-all-purposes tagging material, marker or inhibitor for a single precursor is a huge technological challenge and would need distinct insight in the production and application chain of this precursor. Nevertheless this issue should be solved in order to increase the security of the citizens by revealing terrorist homemade kitchens and improvised explosives synthesis labs before a threat device can be assembled or an attack is carried out. If a fit-for-all-purposes solution is not possible, different solutions for selected applications of a special precursor product might be easier to achieve. The development and test of suitable taggents, markers and/or inhibitors should be closely related to the development of sufficient, fast and reliable detectors which will involve further research activities. With the two EU FP7 research projects LOTUS and EMPHASIS first attempts are made to look for suitable detection systems for detecting gaseous air plumes of terrorist synthesis labs (LOTUS) or to test potential sensors and detection equipments for the detection of indicative plumes in the sewer (EMPHASIS).

If suitable taggents, markers and/or inhibitors are found the use of these may be regulated legally but first the use should be tested on a voluntary basis for specific products / applications.

The development and the application of efficient taggents and/or markers and inhibitors will cost money and may influence the product prices. An efficient cost-benefit analysis is therefore needed before the introduction of the tagged or inhibited precursor containing products or precursor

formulations are brought to the market. In contrast to the costs another aspect might be a potential legal stop for sale if nothing is done.

A11.6 Relation to other Topics

Topic 1+2 (structural and integral approach): A thorough update on the precursors lists should be achieved by using information of national and EU organizations which new chemicals have been used in future terrorist attacks.

Topic 4 (improvised CBRNE): The development of taggents (Topic 11) is closely related to the development of new, fast and reliable detection techniques and detectors (Topic 4). On the one hand the new addition of taggents should not reduce the current detectability of the precursors on its own. On the other hand the new taggents may need the development of new detectors and detection techniques capable of detecting the added substances.

Topic 10 (stand-off detectors): Effective detection of threatening CBRNE material - This Topic is addressing the development of suitable fast, reliable handheld, remote and/or stand-off detectors for CBRNE threat materials.

Topic 14 (reporting lost material): Effective control of production, storage and transport of threatening CBRNE material – This Topic addresses needs regarding the legal and regulating issues as well as the control measures for a safe and theft-free storage and transport of CBRNE materials.

Annex 12 Development of capabilities on organizational structure and optimal distribution of responsibilities and roles for the actors in CBRNE events (Topic no. 12)

A12.1 Introduction:

Response to CBRNE attacks always require the presence of a big number of different actors such as police, medical services, firemen, military as well as specialised personnel which, depending upon the nature of the incident, may be experts in radiology, nuclear, explosives, etc. This fact complicates the overall operability and makes necessary that responsibilities are very clearly identified. Moreover, both are related since lack of clarity in the latter will seriously handicap operability right from the start or hinder the activities to be done by other actors; such us collection of evidences. The organizational aspect need to be improved at the overall security chain, from the preparedness to the response including the recovery, as well us the identification of the responsibilities. In case of IEDs scenario, the sample collection is carried out after the victims and medical services left the area and evidences can be removed, destroyed or contaminated accidentally from scene. Or more recent examples, like Japan nuclear disaster where seawater was contaminated with iodine-131 when the crisis managers try to minimize the problem.

At present, there is a gap of clearly identified responsibilities of the different actors necessary in a CBRNE event as well as in the operability. In some instances this is the case even to a national level where, for example, there are situations where operability was low due to the fact that it was unclear who had the responsibility between municipal police, regional police or national police. Even in the case when they are clearly identified, there may be different between different countries involved in the same event. This is an important point since these events can affect a large number of countries simultaneously as was the case with the Chernobyl accident. Operability is also hindered by other important factors such as the lack of adequate material needs such as protective clothing or real-time contamination detection equipment and the lack of sufficient intra-EU training and benchmarking for different scenarios which in themselves are usually very complex given the large number of variables they can depend on.

Actually, there are a germ on the interoperability and share of responsibilities level base on actual international activities on the civil response like cross-border cooperation for rescue on the mountains, long tunnels (English/France or France / German Alps tunnels) or natural disaster international aid like tsunamis, earthquakes, typhoon, etc. The largest operation in which the Mechanism of International Cooperation, MIC, has been involved since its creation was the Haiti earthquake.

A12.2 Description of the objective:

The objective is two-fold. On the one hand, to create guidelines and operative procedures where responsibilities are clearly identified and are as homogenous as possible between different EU countries and /or actors and, on the other, to improve operability in the handling of these multi-actor CBRNE events by means of establishing a set of well defined, standard scenarios for intra-EU training and benchmarking as well as develop and provide adequate material means to all actors for carrying out their work in the safest and most effective conditions possible.

A12.3 Products, capabilities and services:

To solve a complex problem is it need to now the behaviour/influence of individual parameters in the overall situation. The CBRNE scenario is a complex situation, where the identification of

responsibilities and best operability procedure need to be known before the actors incursion on the scenario. To establish and cover this gap is mandatory, as starting point, the identification of standards in scenarios even, if they are basic /partials scenarios. The definitions of standards should be cover by all actors involved on the response phase like police, military corps, national authorities, EU agencies, health care, etc in cooperation with R&D expert on the scenarios definition to share their previous experience and to achieve commune EU standards. The timeframe for achieving this capability is 2016 years.

Based on the understanding of standards scenarios should be propose a guidelines or working paper at the EU level compiling the fundamental rules and roles of the first responders on case of CBRNA incidents. As well, has to be proposed robust crisis management procedures to support the Member States in case of a crisis with cross-border and multi-actors implications have been developed at the EU level to facilitate the operability of the several different collectives of first responders. R&D effort is being developed at EU level in project like COPE (Common Operational Picture Exploitation) where the aim of homogenized, internationalized and optimized the wide range of command and controls used by first responders. The proposed guidelines and benchmarking need to be easy to do and interiorized as a routine by actors. The timeframe for achieving this capability is 2016 years.

The guidelines and procedures should be trained by the diverse first responders and the best route to achieve this goal is the development of training exercises. The operatives' test of the organizational, the best practice definition, the identification of responsibility, etc should be identified during training exercises and during the post analysis of the exercises. All first responders sector in cooperation with authorities and R&D institutions should propose agenda and training methodologies and contest to enhance the European Training Curricula on CBRNE exercises. The timeframe for achieving this capability is 2017 years.

The identification of the need, best practices and guidelines on materials means should be a task of the training exercises and a specific chapter in their conclusions. The realization of exercises near-real conditions is one of the most important aspects of the training. The carried out a safety use of the materials of means is fundamentals and should be considered in training exercises. The timeframe for achieving this capability is 2017 years.

A12.4 R&D:

(i) Investigate the existing operative procedures and assignation of responsibilities for CBRNE events existing in Europe. Identify similarities and differences between them and establish recommendations for a more coherent framework at the EU level. The timeframe for this investigation is 5 years.

(ii) Investigate past experiences within Europe of the most relevant CBRNE threats that have occurred to identify what shortcomings and problems have been identified in each case in relation with unclear assignation of responsibilities and inadequate operability. Special emphasis on those cases that involve various countries simultaneously. The timeframe for this investigation is 5 years

(iii) With (i) and (ii) develop a set of comprehensive and detailed threat scenarios where all potential responsibility issues and well as operability shortcomings are resolved. It should also include suitable operational guidelines as well as an indicator-based evaluation procedure. The timeframe for this investigation is 5 years.

(iv) Research to improve material means for the relevant scenario actors targeted to improve the operability for actuation in different CBRNE scenarios, very specifically targeting in the standard scenarios of (iii). There are many different

- *Develop fast, precise and lightweight CBNR dosimeters to identify the exposure level and nature of the HAZMAT hazard. (>2016).*

- *Develop standards for equipment with the aim of making possible that first responders can share equipment and specialised personnel whenever necessary (2018).*
- *Develop advance materials to cover the overall spectra of HAZMAT (>2016).*
- *Develop more effective breathing systems (2016).*
- *Design of new concept and joints for the clothes components (2018).*

A12.5 Related issues and difficulties:

- Acceptance of standard scenarios and procedures. May be hindered by the reluctance to change established procedures. In some cases national organisation may be a problem since different European countries have very different degrees of autonomy between different regions within them.
- Acceptance of standardisation in equipment and protective materials. May be hindered by specific industrial interest of different countries as well as different perception of threats. For example, France has a 58 nuclear reactor whereas Spain has only 8. On the other hand, Spain has a long history of terrorist attacks whereas France has not.

Legal aspects. It may be a problem when trying to establish intra-European standards regarding responsibility assignation or operability issues. What may be legal in one country may require legal changes in another. **[5 to 10 lines]**

A12.6 Relation to other Topics:

The identification of responsibilities and operability of first responder is intimately related with the identification and validation of scenarios, as well as the assessment of threats. The lack of such aspect was identified by the expert groups on Topic 3 (focus worst case). The limited trans-national exchange of information and cooperation in confidential or procedures questions (Topic 7: (inter)national cooperation) or the enhancement of the European Curricula on CBRNE training (Topic 5: realistic training) is connected with the identification of responsibilities and interoperability.

References:

D2.3 COPE (Grant Agreement nº 217854) / Leena Norros et al. (2010): COPE Technology enabled capacity for First Responders.
ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form:
http://www.esrif.eu/documents/esrif_final_report.pdf
"EU capacities to respond to CBRN attacks and CBRN incidents" (2010)
http://www.hse.gov.uk/foi/internalops/fod/om/2009/03.htm
DoD CBRN Defense Doctrine, Training, Leadership, and Education (DTL&E), Strategic Plan.
http://www.acq.osd.mil/cp/dod.cbrn.defense.dtle.strategic.plan_5dec08-v4.pdf

Annex 13 Develop and define minimum standards for security relevant infrastructure (Topic no. 13)

A13.1 Introduction:

The set-up and availability of minimum standards for the use of adequate CBRNE detection equipments in security relevant infrastructures or the use of secure-by-design building materials is very rarely elaborated today. C and B standards or harmonized procedures today only exist in the military range. R and N detector standards are somewhat more elaborated also in the civil application field, but harmonized minimum standards used in all European countries do not exist. Regarding E detection equipments the only field with existing minimum standards is found in the field of airport security checkpoints made up by the ECAC. Therefore measures and regulations for setting up minimum standards especially dedicated for the application in security relevant infrastructures are highly required. Infrastructures for example include transportation infrastructures such as rail, road, marine and air transportation systems, stations, tunnels, bridges, power stations as well as for example buildings in which a large amount of people is present. An essential pre-requisite before minimum standards for security relevant infrastructures could be set in place is the need of testing the capabilities of available detector systems and to evaluate these against the needs of the specific circumstances and requirements under realistic infrastructure scenarios.

A13.2 Description of the objective

Objective will be to establish regulations which set minimum standards for security relevant infrastructures to ensure the use of adequate detection equipments as well as the use of building materials which are for example highly blast-resistant (E) or non-adhesive to CBRNE agents.
The mentioned infrastructures and locations need to be considered as different realistic scenarios with their different, specific frame conditions to define suitable and applicable detection needs. Existing CBRNE detectors should be tested for these different scenarios and new techniques should be developed if the today available techniques are not sufficient for ensuring the security of relevant infrastructures. Furthermore protection of infrastructure needs to be considered already at design phase (Security-by-design concept) to build up for example blast-resistant walls and buildings, to use construction materials which are non-adhesive for CBRNE agents or to install secure-by-design ventilation systems. As today not all relevant threat substances can be detected the objective will also be to ensure an enhanced development of new detection equipments and decontamination standards as well as best practices for their application in security relevant infrastructures.

A13.3 Products, capabilities and services

- Definition of real scenarios to be tested, evaluated and potentially regulated by minimum standards such as for example protection of security related infrastructures, mass transportation systems, large area surveillance etc. including CBRNE substances / concentrations to be detected
- Detectors capable of detecting the necessary CBRNE agents, concentrations (bulk, vapor or solid traces) with or without direct sampling
- Measurement of realistic concentrations and deliberation profiles of CBRNE agents
- Validation panels for adequate selection of relevant CB agents and procedures for warning detection methodologies
- Standards for evaluating the decontamination of affected CBRN infrastructures / buildings
- Standards for evaluating construction of buildings and/or ventilation systems to ensure no or minor contamination of the environment and to reduce potential effects to people

A13.4 R&D

- Development of common testing and trialling procedures / methodologies for selected scenarios of relevant infrastructures to test available and future CBRNE detectors
- Development of suitable standard reference materials for testing and evaluating for example trace explosives detection systems (vapor and surface contaminations) including specific analysis of stability and life time of the reference materials
- Development of validation panels for CBRN agents / concentrations to be achieved by contamination procedures / processes
- Test of available detection equipments for selected, infrastructure specific scenarios (others than airport checkpoints)
- Development and evaluation of new detectors for specific infrastructure-specific scenarios with realistic threat substances concentrations and relevant threat substances
- Development of suitable detectors for detecting the actual decontamination concentrations and testing them in real operating environments
- Test and simulation of threat substances concentrations and deliberation profiles
- Elaboration of suitable test objects or test chambers for testing detectors including the realistic deliberation profiles and/or the concentrations to be detected on surfaces of bombs
- Development of new ventilation systems (CB) or building constructions to resist attacks (E) including for example new materials to be used (Secure-by-design concept)
- Development of minimum standard values to be achieved by detection and also for decontamination procedures

A13.5 Related issues / difficulties

The development of common testing procedures / methodologies for security relevant infrastructures requires a lot of time and financial costs. The role of actors and financial payers should be well elaborated before standardization issues get started.

The realistic application scenarios should be well selected to enhance the security of citizens and to ensure the protection of security relevant infrastructures and to balance the costs against the efforts.

Set-up of minimum standards is a legal aspect to be set in place by governmental agencies or bodies which must be accepted by the member states before they can be used. If minimum standards are set and attacks or negative health effects are not diminished by them this could lead to financial / legal claims afterwards.

The handling of CBRNE agents / samples is a legally restricted field; test centers should be able to keep the necessary restrictions and legal demands.

The set-up of minimum standards for security relevant infrastructures will mean that companies, communes and/or infrastructure operators will have to invest a lot of money for installing new detection equipments, new building materials or secure-by-design installations such as ventilation systems etc. These financial aspects should not put a to high burden to small SMEs, small communes or poor countries. On the other side the additional financial investigations will save money in not needing to re-build otherwise destroyed infrastructures and buildings. Apart from that the lives of dozens, hundreds or thousands of citizens will be saved which could not be calculated in money.

Tests in real environments or city buildings should be well organized in order not to produce a potential threat to the health of people being present and not to damage the environment.

A13.6 Relation to other Topics

The here mentioned Topic number 13 is mainly looking into measures during the prevention phase of the security cycle and is closely related to the following Topics:

Topic 6 (deployment of equipment): This might be also an issue for solutions developed under Topic 13, but is not essential for the protection of security-relevant infrastructures.

Topic 8 (alert state): These might influence the secure-by-design and decontamination issues of Topic 13.

Topic 10 (stand-off detectors) and Topic 16 (detection systems): This describes the development of new CBRNE detection equipments more in general while part of Topic 13 is closely related to the application of detectors for securing infrastructures.

Topic 15 (affected people): E.g. groups of people travelling from contaminated areas to clean areas is more looking to needs during the recovery phase of the security cycle

Topic 24 (standards in testing): This is closely related to this Topic 13, but addresses more the test of the limit of detection and capabilities for specific standards not looking at special realistic test scenarios / environments as mentioned in this paper.

Annex 14 Effective control of production, storage and transport of threatening CBRNE material (Topic no. 14)

A14.1 Introduction

The first step for a wilful actor towards a CBRNE attack is to acquire the threatening material. Therefore it is of outstanding importance for state authorities to control production, storage, processing, use and transport of the substances in question. If losses are reported in a timely and comprehensive way, a valid and up to date assessment of the current threat situation and proper prevention measures, at best seizing of the material, are possible. Because of the cross-border activities by terroristic groups an international control regime with well-functioning control mechanisms is necessary. For more details see DECOTESSC1 report on WP7, chapter 3.3-3.5 and on WP5, chapter 3.6 and 4.3.

A14.2 Description of the objective

Production, storage, transport, processing and use of threatening CBRNE material should be effectively controlled. Related legislation, procedures and control mechanisms for reporting losses of material have to be established or improved. A well-recognised European authority dedicated to collecting reports and cooperating with national as well as international organisations has to be established. Experience with existing control mechanisms (as e.g. with the IAEA data base ITDB, OPCW and others) should be exploited. More details to existing control procedures and organisations can be found in DECOTESSC1 report on WP6, chapter 2 and 3. Such a centralised European control mechanism should be achieved until 2014, but has to be further developed and adopted in future.

A14.3 Products, capabilities and services

1) Unified legislation in all EU member states concerning monitoring of threatening CBRNE material

An effective central control on threatening CBRNE material is only possible if it is regulated by law. Following existing regulations (see DECOTESSC1 report on WP6) a unified legislation for such a central control has to be developed. Procedures have to be clear, unified and conceived in a way that allows fast information transfer. Losses of threatening material during production, storage, processing, use or transport have to be reported to a centre and from there information has to be distributed to ensure adequate measures. At this the problem of classification is to be taken into account. Therefore the required regulations should refer to the access to information as well as to sufficiently secure technical solutions for information transfer.
In this context a central European authority has to be allocated competences, possibly also national CBRNE centres to direct the information flow.
This is a task to be done by the European Commission together with the Member State governments, supported by relevant stakeholders from industry, applied research and jurisprudence.
Because of the high importance an ambitious time schedule is recommendable. At least draft contracts and bills are desirable until 2014.

2) Sufficient access controls to production, storage, processing, using and transport facilities

Control on threatening CBRNE material includes a restricted and monitored access to the relevant facilities. Therefore adequate access controls to production, use, processing, storage and transport facilities are necessary (cf. report on WP5, 4.3). Existing access regulations should be harmonized adopting general regulations to local characteristics. Technical solutions might be improved, not least

to minimize costs, and an EU reporting mechanism in case of irregularities has to be established. Fast prosecution, also across borders, has to be ensured. While the regulations and the reporting mechanism has to be implemented on a legal base provided by the European Commission with the Member State governments, the technical aspect involves industry and research institutes. Also different technical aspects should be taken into consideration, e.g. possibilities to culture biological agents (e.g. extract of concentrated pathogens).
Since control mechanisms already exist, certain improvements and unification should be feasible in 3-5 years.

3) Monitoring of threatening CBRNE material transport

Transports of threatening CBRNE material have to be continuously and uninterrupted monitored and documented. Therefore, unified procedures have to be implemented. The documentation has to be collected in the suggested European authority to provide a complete picture of the production, storage and transport of the material.

4) Promotion of reporting of losses of threatening CBRNE material

Experience with existing data bases in the present context shows that it is difficult to ensure reliable reporting. This has to be promoted therefore in an adequate manner, e.g. via special workshops for staff members of the involved stakeholders, contributions to conferences and so on. Efforts have to be done when the control system comes into force, probably earliest 2014.

5) European CBRNE centre

The sketched control system requires the institution of a European authority like EURATOM dedicated to collecting reports, evaluating them immediately and cooperating with national as well as international organisations and agencies like IAEA and others (refer to DECOTESSC1 report on WP5, chapter 3.8). Even while the comprehensive control mechanisms are still under construction a related authority could start and coordinate the different processes to establish the final control system. So the centre should be established until 2014.

A14.4 R&D

- Lists of threatening CBRNE materials for regulation (for capabilities 1), 3), 4)):
  To control threatening CBRNE materials it is inevitable to know the substances that could be abused for a CBRNE attack. Research can provide comprehensive lists for each category of substances. An overview of already available lists is given in the DECOTESSC1 report on WP6, chapter 2. Of equal importance is to know which substances could become a threat in future (see e.g. the project PREVAIL, DECOTESSC1 report on WP6). For this purpose related research activities are and will be always necessary in chemistry, biology and nuclear physics. These activities involve sensible information – an issue addressed below and explicitly in Topic 7.

- Recommendations for legislation and regulation on common control procedures and regulated CBRNE materials (for capabilities 1), 4)):
  To establish the above sketched unified legislation in all EU member states concerning monitoring of threatening CBRNE material profound expert knowledge is necessary regarding the substances in question, the ways of production, storing and transportation, the possibilities of detection and also possible abuse. Furthermore support from jurisprudence and social sciences will be relevant.

A14.5 Related issues and difficulties

- Punishments and prosecution
  The effectiveness of control has to be ensured. Therefore significant punishments and prosecution across the member states are necessary, regarding thefts as well as denial of reporting. This issue has to be addressed by the related authorities.

- Additional Work for involved organisations
  The comprehensive documentation will cause extra work for the involved organisations, which might be difficult to deal with. Possibly the personnel has to be increased.

- Classification issues
  The sketched control mechanism requires circulation and filing of sensitive information. Therefore an adequate access restriction for the information flow and saving is necessary. This is difficult to achieve on a transnational level. In addition national authorities might have reservations to share certain information.

- Incomplete reporting
  Incomplete reporting may scale down the usefulness of the control system significantly. This refers to timely international coordinated reactions to acute occurrences as well as the use of the system as a basis for planning and mid or long term strategies. This problem claims particular attention.

- Missing consensus amongst member states
  The unified legislation in all EU member states concerning monitoring of threatening CBRNE material as well as the general acceptance of a European CBRNE authority might be difficult to be asserted. Missing consensus amongst member states may cause delays or even obstruct an effective central control.

- Improved technology to detect and identify threatening CBRNE material (for capabilities 2), 3))
  Suitable detection systems have to be established at the access points of production, storage and transport facilities for threatening CBRNE material. Furthermore detection and identification systems are necessary to monitor the transport and support book keeping. This requires ongoing research to improve the detection capabilities. At the same time new techniques may help to reduce the costs of the devices. The research activities should not only focus on the detection process itself (see Topic 10) but also on improvements concerning the technology and procedures for detection systems as a whole, including the optimal positioning of the detectors, also data processing, transfer, and fusion. The different requirements for the different production, storage or transport facilities are to be taken into account regarding e.g. robustness or accuracy. Also the problem of false alarms has to be considered. Improving the technologies for the detection systems is a big task which has to be addressed in different approaches by research institutes and industry. References to promising ongoing research can be found in the DECOTESSC1 report on WP6.

- Relevant institutions for controlling access control
  Relevant institutions have to be identified which will check if the access control is up-to-date.

A14.6 Relation to other Topics

Topic 4 (improvised CBRNE): Research on improvised CBRNE devices and production facilities can give hints on which kind of CBRNE material should be considered as threatening and with what priority. The related problems are described in Topic 4.

Topic 10 (stand-off detectors): As outlined above the intended control system involves adequate detection techniques, which are addressed in more detail in Topic 10.

Topic 7 ((inter)national cooperation): The sketched control mechanism will include transfer and storage of sensible information. As outlined above this concerns classification problems. Sufficiently secure technical solutions for rapid information transfer are necessary. These issues are further outlined in Topic 7.

Topic 25 (leadership in EU): The above mentioned possible problem concerning consensus is related to the problem of leadership within the EU, such as the lack of an EU coordinating body for keeping uniform rules for measures and for information, further addressed in Topic 25.

Annex 15 Fast and reliable identification of affected people (CBRNE) (Topic no. 15)

A15.1 Introduction:

Fast identification of people affected by a CBRN incident is important. First, the degree of contamination of persons by threatening materials should be diagnosed quickly, ideally already on-site. This would expedite triage and allow medical staff to begin appropriate treatment as early as possible. (ESRIF report, p. 146). Especially in the case of C-agents this could make the difference between life and death. Secondly, the psychological reactions might not only affect people near the impact site but also people living far away. Many persons who feel like they have been contaminated will ask for medical help, thereby overloading the medical response system. This can partly be managed by using reliable diagnosis tools to verify a dose below threshold for victims and assuring them that no further treatment is necessary (ESRIF report, p. 146). Finally, fast and reliable information on the number of affected people is necessary for getting an idea on the size of an incident as input for the decision support. The knowledge about the magnitude is crucial for the further planning (needed staff and equipment) of response and recovery activities like evacuation, patient transport, treatment, decontamination etc.
In the case of biological threats, the identification of affected people is important to decide on triage and quarantine, and to limit and forecast the spread of the disease (D7.2, chapter 6.5). Nevertheless, available diagnostic methods are time-consuming and yield first results only after a number of hours (days). This causes the difficulty of keeping potentially affected people under control (limiting their freedom of movement) for a considerable time span. For C and RN threats contamination by threatening materials can be detected more easily, whereby differentiation between those who can spread the agent and those who are clean can be done faster.
For radiological incidents, a practicable handbook for the effective and timely triage, monitoring and treatment of people exposed to radiation following a malevolent act has been developed in the framework of the FP6 project “TMT-Handbook. This handbook could be used (in adapted form) for the development of similar procedures to give guidance on identification of affected people in C and B incidents.

A15.2 Description of the objective

The main objective is to develop capabilities for information collection (incl. interviewing people) on site and transmit data via secured networks concerning the identification of affected people. Information also include measurement results from detection systems (to define the level of contamination of people and/or environmental media like air, food etc.). While for RN methods are already available and need only further improvement for low dose ranges, innovative approaches in developing suitable indicators for the determination of affected people are necessary to cover B and C threats (time frame: 2020).

A15.3 Products, capabilities and services

- For identification of affected people the development of standardised operation procedures for information collection and processing is necessary in order to get reliable and trustful results. The task “Diagnosis” means not only the integration of a bunch of different information into a final yes/no decision (affected/non affected), but also the identification of the threat in order to select suitable specific treatment, if necessary.
- For RN, technical solutions for detection and identification of the threat substances are already available. Diagnosis of B-infection is a typical medical task, nevertheless, methods for fast

identification of infection before symptoms are developed needs to be improved. For C-threats, at the moment most detection/ identification systems can only cover a limited range of possible agents. Therefore there is a need of further improvement of identification capabilities.

- A further crucial piece of information is the scientifically based definition of limit dose values for B and C agents. In the case of RN the scientific debate discriminates between acute radiation effects and stochastic radiation effects. While for the acute radiation effects the dose limits are agreed, for stochastic radiation effects (i.e. development of radiation-induced cancer) there is no "harmless" dose, so the smallest measureable amount of dose can have a negative health-effect. In this case, pragmatic (health political) decisions have to be made. This should be done on a European harmonized level.
- As a consequence of the identification of affected people, there is a need to develop suitable procedures for the further handling of the selected group. Especially solutions have to be developed for containing people near the scene of event (or near medical checkpoints for later decontamination, treatment…)

A15.4 R&D

Concerning research and development, some of the points mentioned below at least partly have been covered by recent calls of the FP7 security programme. Nevertheless, cross-cutting and integrated initiatives, including medical, psychological experts as well as first responder organizations to bring in the operational aspect of applying procedures under stress conditions are needed.

- Development of rapid diagnostics for B (time frame: 2020)
  Research on presymptomatic clinical diagnostics which are operable under field conditions: Identify markers/metabolites linked to groups of agents during early immune response on different sampling media (e.g. nasal swaps) (D7.2, chapter 6.5)
- Development of rapid diagnostics for low doses of R (time frame: 2016)
  Fieldable R/N biodosimetry (or fast post accident dosimetry) and chemical, biological point of care diagnosis (D7.2, chapter 6.5)
- Development of rapid diagnosis to C exposures (time frame: 2016)
  - Research on potential acute and delayed adverse health effects from low-level exposure to nerve agents and development of sensitive markers for exposure (from ESRIF, p. 146);
  - Development of exposure markers for C agents relevant for triage and estimation of actual exposure/uptake/excretion (from ESRIF, p. 152)
- Development of procedures for countermeasures and treatment of affected people for B and C including distribution of responsibilities to follow the "tagged" / listed people (time frame: 2016)

A15.5 Related issues and difficulties

Whenever the health status of individuals is under discussion, immediately appear issues of privacy (protection of sensitive information about possible morbidity) and other ethical aspects like the cost efficiency (cost-benefit analysis) of expensive treatments.
If people get officially the status of being "affected" by an incident, there should be clear responsibilities who is going to cover costs for late effects of health impairment (treatment and rehabilitation cost, early retirement …). Public information and maybe regulations are needed in order to avoid discrimination of affected people (e.g. when applying for a job; higher life insurance rates etc.).
Strong negative psychological effects have to be expected for people who get the information that they have been affected by a CBRNE incident, and now have to fear for negative late health effects. For example, low doses of radiation will show effect (cancer) only after a time-span of decades. Medical monitoring for such long period can put a serious (psychological) burden to the people

Group-specific information has to be pre-prepared for the distribution amongst affected people which answers all questions concerning specific and necessary treatment, probable effects /health problems, recommended precautions to be carried out by the individual him/herself (like regular health monitoring, change of life-style), positive influencing factors, lists of institutions providing (psychological) support, further information etc.
Privacy of affected people: keep people on-site means impairment of their freedom to move and may be executed against their personal will

A15.6 Relation to other Topics

Topic 9 (communication with population): Efficient communication to manage psychological effects of CBRNE incidents is a key factor for successful crisis management. Affected people will have a strong need for information. Only then panic and fear can be reduced effectively. Overwhelming of medical infrastructures by affected people seeking for help can be avoided by straightforward communication giving advice for the correct behaviour of people.

Topic 12 (responsibilities): Decentralized medical staff and hospitals have to cooperate in order to manage a large number of victims. Emergency medical transport has to distribute victims to available medical infrastructures in order to avoid overwhelming of the nearest hospital.

Topic 20 (medical capabilities): Medical capabilities to diagnose and treat CBRN threats effectively are necessary to treat affected people.

Topic 17 (real time threat assessment): Simple bar code generators and readers would be a helpful tool for tagging large numbers of people. This directly relates to ESRIF and findings from D7.2 about the administration of evacuees and patients in a mass casualty scenario. In order to assure proper mitigation an IT-based system for recording, tracking and tracing of individuals is required.

References:

D7.2 – Ehlerding, A. et al. (2011): Decotessc1 Deliverable Report D7.2 – Gap analysis.
Rojas-Palma, C.; Liland, A.; Jerstad, A.N.; Etherington, G.; del Rosario Perez, M.; Rahola, T.; Smith, K. (eds.) (2009): TMT-Handbook. Triage, Monitoring and Treatment of people exposed to ionizing radiation following a malevolent act. ISBN 978-82-90362-27-5; 290 pp. Available in electronic form: http://www.tmthandbook.org
ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form: http://www.esrif.eu/documents/esrif_final_report.pdf

Annex 16 Fast and reliable detection systems that can detect multiple threats and detect degree of hazard (rather than agents) (CBRNE) (Topic 16)

A16.1 Introduction:

First responders, called to a scene of incident have to face a wide the spectrum of possible CBRNE threats leading to the requirement of preparing for any of the CBRNE threats. In reality, often FRs do not have the necessary equipment on board (PPE, rapid detectors for threat assessment) to deal with CBRNE threats. Moreover, the usual basic equipment of a typical fire fighter amounts to 10 kg or more, so every other gadget (like hand-held CBRNE detectors) means an additional burden which limits the operational capabilities of FRs in the field and in typical rescue operations. A solution to this problem could be a multi-threat sensor, which does not give specific information on substances but only a rough indication on the nature of the threat and the degree of hazard. Such kind of information is sufficient to make on-site decisions, e.g. whether it is safe to enter a building or contaminated area, move forward into the direction of the hot zone of an incident (Decotessc1 D.7.2, chapter 6.6) or whether identification or adequate handling of injured people is correct.
An ideal instrument would

- identify all relevant agents instantaneously at the site of the incident,
- have a high sensitivity,
- produce very few false positive results,
- allow user-friendly handling for non-expert operators.

Currently available detection and identification systems are mostly characterized by a narrow spectrum of detectable agents and an insufficient sensitivity to measure toxic / contagious amounts of agent (Decotessc D.7.2, chapter 6.6), also most detectors show a considerable cross sensitivity to harmless substances. Moreover, they do produce false positive results. To compensate these lacks, the operators need a very good knowledge (=experience) of the agents and the devices used to identify them. Operators have to be particularly knowledgeable about the limitations of tools they are using to avoid producing wrong results. Already in the ESRIF report (p.145- 146) it is mentioned that for B and C an alternate possibility would be to replace the detection of material/agents with the detection of their effects/properties: toxicity in the case of chemical or virulence for biological.
Since it is quite evident that there is no single detection technology for all threats, integration and networking of sensors will play an important role in all scanning equipment deployed at borders or other transit points. Furthermore, inspection equipment will have to integrate all sensors both from the hardware side and from the point of view of signal analysis (data correlation, data fusion algorithms, imaging and 3-D reconstruction techniques, artificial intelligence). Another important aspect of improvement could be the development of specific detection architectures (for airports, seaports, border checkpoints, free passenger flow systems like railway stations, public assembly points).

A16.2 Description of the objective

Development of portable multi-threat sensors, which can be used by first responders to have real-time situation awareness when approaching a scene of incident with unknown threats. Measurement results should give risk categorization and identification of the contaminated area rather than identification on threat agents. (e.g. green-yellow-red reading to inform on safe environment). Ideally, detectors will be embedded in daily-use equipment.
Development of new instrumentation will require the parallel development of international standardization and, by consequence, testing and validation procedures. (D.7.2, chapter 5.5).
Time frame: for C/R: 2016; for B/C/RN/E: 2016

A16.3 Products, capabilities and services

- Mobile and portable rapid CR detectors (timeframe: until 2016)
- Mobile and rapid B detectors to detect the degree of hazard (2016)
- Integrated rapid CBR detectors outdoor (2016; based on systems under development in the military domain)
- Alert system for first responders (secured network) (2016)
- Integrated detection systems (X-ray, E-vapour detectors; etc.) to for fast and reliable detection of suspicious IEDs, bombs (2016)
- Detectors capable of detecting traces of E (gas/solid) without contacting suspicious objects (2016)

A16.4 R&D

The technological readiness of existing detection systems is extremely different for B C/E and RN. Nevertheless, combined R/C detector systems are already on the market. The same is true for C/E, which often use the same analytical principles (e.g. IR or RAMAN-spectroscopy; D.7.2, chapter 6.6). B detection is still not mature enough; especially mobile real-time detection equipment needs to be developed. Therefore, the integration into multi-threat sensors is not feasible within a timeframe of several years (> 2020). In addition, the detection principle for B-threats (including PCR for the identification of B-agents) is completely different from any of the other detection methods, so a combination into one piece of equipment does not seem straightforward. If at all, at the scene a detection of IEDs/bombs carried out by EOD services is made by x-ray to detect the detonator / metal parts of the bomb. Sufficiently sensitive E-detectors are currently not available.

- Development of mobile, real-time B detectors for first responders. Fast, affordable, genome sequencing in combination with immediate comparison with extensive sequence databases. (time frame: 2020)
- Further R & D towards detection of suspicious aerosols to facilitate stand-off B detection. (2020)
- For indoor use modification of technology will be required both for mobile CR detectors as well as for B and combined CBR detection systems (time frame: CR: < 2016; B/BCR: > 2020)
- Develop technical solutions integrating B to CR detection (> 2020)
- Development of trace E detectors for gaseous and/or solid traces above items or surfaces. Detectors should also be usable for traces of C-agents in parallel.
  For detection of hazard: Develop living-cell detectors, which indicate toxicity rather than compounds (ESRIF WG6_WP4_final p.9). This requires a database for the prediction of toxicity by molecular and submolecular properties; also it requires a novel screening system for cyto- and pharmacotoxic effects for all cell-lines) (time frame > 2020)
- For B, develop detection systems for virulence (time frame: 2020)

A16.5 Related issues and difficulties

Concerning detectors based on pathogenesis and toxicity there is a direct link to health issues, so ethical considerations are necessary in parallel with detector development and possible use of such systems.

These systems are not easily affordable

There may be a false sense of security created – no detector system can detect EVERYTHING – there is always a risk of not detected threats.

False positives – for non-experts it is extremely difficult to make a decision on the correct reaction to a false alarm. Only experts can identify a false alarm. Then more sophisticated detection (specialized to one threat) are necessary to make additional measurements or support by improved automated systems.

A16.6 Relation to other Topics

Topic 6 (deployment of equipment): such kind of multithread detector systems would be a real improvement toward user-friendliness. Categorization of threat would allow non-expert FRs to make use of the detector information. The interpretation of the detector reading is easy – the interpretation of the measurement is done by the detector itself (indicating threat level already).

Topic 7 (limited cooperation (inter)national): would speed up the development of such sensors

Topic 10 (lack of stand-off detectors): integration of such sensors could be the basis for a multi-threat detection system

Topic 17 (real time threat assessment): categorization would mean kind of real-time threat assessment, so a multi-threat sensor could support to close the Topic 17

Topic 22 (safe sampling without FRs on risk): If FRs are equipped with a multi-threat sensor, they would have a real-time information on the site, where sampling is safe (where sampling for the threat substance is suitable / not very helpful…)

Topic 23 (tools for crisis management): positive relation: good tool for FRs on scene to carry out rescue operations. For the crisis management centres very precise information about identified substances and concentrations is needed in order to make knowledge-based decisions. The outcome will be a threat categorization, but as an input it is not enough.

References:

Decotessc1 D7.2 / Ehlerding, A. et al. (2012): Decotescc1 Deliverable Report D.7.2 – Gap Analysis. Classification Level: Secret.
ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form: http://www.esrif.eu/documents/esrif_final_report.pdf
ESRIF_WG6_WP4 (anonymous) (2008): Outlining CBRN R&D achievements to fill mid- and long-term capability gaps WG 6 on CBRN. Available in electronic form: http://www.esrif.eu/documents/esrif_additional_material.zip

Annex 17 Real time situation awareness: instant threat detection, data processing, analysis and dissemination (Topic no. 17)

A17.1 Introduction

Today's societies face a highly dynamic threat from CBRNE terrorism. Letters filled with anthrax, shoe bombers, suicide attackers in city centers, on airports, and in metro systems: the threat is constantly evolving.
Detecting and identifying a threat requires a constant and continuous analysis of situations (in general). Situation awareness and information are key aspects for real time threat detection and identification. This goes for before, during and after an incident. First responders for instance would benefit from improved real time situation awareness, including hazard assessment. An example of this is fast (preferable on-site) prediction of the area that will be affected when a cloud of chemical substance has been released; this will allow first responders to take the appropriate countermeasures.

Real time situation awareness faces several fundamental challenges:

- Situation awareness requires a complete understanding of the *normal* situation to determine whether anything is *deviating*. This holds, for instance, for detecting abnormal behaviour: What kind of behaviour is an indicator an impending attack? Is this kind of behaviour specific or is it also observed in non threatening situations? Detecting and identifying potentially threatening CBRNE substances has a more or less similar challenge: How to detect these substances in an environment of which the (air) composition is variable and not exactly known? The fact that the threat is constantly changing enlarges the challenge for real time threat detection and identification.
- The use of sensors will lead to an enormous amount of information. This needs to be processed, stored and analysed in time to give authorities a chance of preventing an actor from executing its attack. To be useful in the response phase (after an attack) fast data processing is even more important. The amount of the information and the limited time avalable will pose a severe challenge for information systems.
- An additional challenge is fusing data coming from different kind of sensors: cameras, CBRNE detectors or even information obtained by animal (e.g. dogs) or humans. Reliability of the information system will be essential. Too many false positives and/or negatives undermine a system's value to situation awareness. These aspects are especially significant for B agents and to a large extend for C substances, because biological and chemical threats are difficult to discern from natural or normal substances in ordinary situations. R, N and E substances are, generally spoken, better detectable.

When developing a system for real time situation awareness, it is important to define the scope of the assessment. Do you want to assess the CBRN security situation for an entire country (or even the entire EU), or for a smaller region, perhaps only a certain building? This question is closely related to the type of data that will be used. The type of data that will be used needs to be determined (including the required accuracy, refresh rates, etc). This can involve visual data (cameras that register abnormal behaviour, as mentioned before) and detection of C, B, R/N or explosive substances, but also other aspects like scanning for suspicious texts posted on the internet, or using databases about criminal activities or epidemiological data. The intelligence community should be closely involved when developing a system for situation awareness.

Real time situation awareness enhanced by connected databases of various data is fundamental for protecting civilians and vital infrastructure against CBRNE threats. Its importance goes beyond the aspect of preventing the occurrence of an attack, which is of course the main goal, but a real time

situation awareness system also guides and improves first response and recovery activities: a thorough understanding of the situation will lead to a better approach.

A17.2 Description of the objective

The EU should have a common system for real time data collection, fusion, processing, analysis and dissimination (reporting). In this approach all aspects are linked as a chain: without real time detection capabilities, sufficient data processing capacity or expert analysts the chances of a timely and adequate action will decrease. This system will integrate various sources of information, for instance from databases of intelligence services, police records or border control agencies.

The goal is to deliver the whole system in 2019, ending with the common protocol for information use. The start will be in 2013 with a description of system requirements for real time detection, processing and analysis. Potential end users have to be determined. In 2015, a working prototype of relevant components is delivered, including algorithms for large amount data fusion and processing, followed by an integrated system prototype in 2017.

A17.3 Products, capabilities and services

Real time situation awareness will be based on different products, capabilities and services, which should be intergrated (chained) for an optimal result.

- The first step is to determine the exact scope. What should be the exact capability of the real time awareness system? What are the subjects of investigation, what information is needed at what time? What should be the result? What is the relation to other parts of the CBRNE counterterrorism system-of-systems?
- The second step is to determine how to collect, store, analyse and spread the information. Furthermore, partners have to be identified: suppliers of raw information and users of assessed information. (Cross-border) Formats and communication protocols need to be set.
- The next step in creating real time situation awareness is a system capable of detecting suspicious behaviour and (aerial) substances and other relevant aspects deviating from the ‘normal’ situation. The system will consist of multiple sensors (in the broadest sense of the word), each with its own specialty. All data need to be processed in order to share it.
- A reliable 24/7 decision support tool should be developed. A suitable division of roles between human and machine should be established: computer for the analysis and experts for interpretation, decision making and communication. The tool needs to be fed by sensor output and fused information from other sources and various databases adequate countermeasures.
- The period right after an accident needs special attention. Is it possible to identify the current and near future hazard, to assess if it is likely that more related incidents will happen? Sensor information, intelligence and information from the incident location need to be fused and interpreted. Is it possible to deploy (disposable) sensors very fast within the incident area?

A17.4 R&D

The first object of R&D will develop a systemic framework in which the different chains of detection, fusion/processing and analysis are integrated. This framework is the starting point for creating several capabilities:

- Determine indicators for CBRNE terrorism.
- Real time threat detectors. These sensors can be divided in two groups. One focussing on recognizing substances in differing areas or locations. The second group of sensors will be about detecting suspicious behaviour of terrorist actors.

- Algorithms for data fusion and processing. While sensors will create a huge amount of data, manpower might be scarce. Algorithms are needed to counter information overload and integrate data coming from different kind of sensors.
- Algorithms for data analysis. R&D in algorithms supporting analysis is needed to distinguish threatening and normal situations. Even so, the system should be adjustable in order minimise the chance on false alarms or newly emerging threats.
- Research which parts of the detection, fusion/processing and analysis chain can also be automated or where a man-in-the-loop is required.
- Research in the field of decision support tools. What kind of information is essential for decision making and needs to be prioritised? How is this information best presented?
- Secured and robust network for communication. The chain of detection to analysis will require R&D for optimal solutions to ensure that communication networks will work at all time and are protected against manmade threats (cybercrime and terrorism).

A17.5 Related issues and difficulties

Deploying sensors, information fusion, data storage are aspects which can be at odds with privacy and ethical issues. A network of sensors used for detecting suspicious behaviour and substances will touch daily life, especially when deployed in public areas. This matter will be even more urgent when data about individuals may be integrated.

A political issue will be the reliability of the real time situation awareness system. A system which cries wolf too often is a risk factor for those who bear political responsibility will be high. Unnecessary countermeasures can be costly and undermine public trust in political authorities.

On a different level, access to potentially (very) sensitive data is another point of discussion. Although unlimited sharing of data is seen optimal for assessing threats, some restrictions might be needed to make sure that classified information does not fall in wrong hands. This is especially an important point regarding information coming from intelligence services.

Determining indicators for CBRNE terrorism could provide some difficulties, especially for CBRN. Because the EU has very little experience with terrorist attacks involving CBRN, it will be difficult to determine which factors indicate the preparation of an attack involving CBRN.

Lastly, a system for real time situation awareness should be approached as an interconnected chain of processes and activities. Optimizing one of the links will not lead to an optimal process. For instance, focussing solely at detection without attention for analysis and dissemination will cause an overload of unprocessed information; in a worst case scenario one would discover that relevant information was available before an incident took place, but waiting to be processed.

A17.6 Relation to other Topics

A common system for real time data collection (detection), fusion and processing, analysis and dissemination is linked to several other Topics. While this is primarily about detecting a threat, good tools for crisis management which supports first responders and crisis management authorities is clearly linked (Topic 23: tools for crisis management). It is important to have mutual insight in all involved organizations about their locations, activities, plans, etc. The situation awareness is further complemented with integrating information about infected people and their whereabouts (Topic 15: affected people). Mechanisms for reporting losses of CBRNE material (Topic 14: reporting lost material) are a good of example of a source of information which will support situation awareness.

Clearly, integrating information about detection or crisis management tools etc. touches upon Topics (Topic 1&2: structural and integral approach), which address shortcomings in cooperation between multiple organisations in dealing with terrorist threats.

Annex 18 Design of personal protection equipment with more durable and multifunctional materials which are comfortable for natural gestures (Topic no. 18)

Note: The content of both Topics no. 6 and no. 18. closely relate to each other. Therefor some of the text in the Topic descriptions is the same.

A18.1 Introduction

Protect first responders in a CBRNE scenario is a complex task due to the multiple combination of CBRN-E threats or HAZMAT materials. The personal protection equipment (PPE) has high requirements due to its important role; minimize casualties and maximise effectiveness.

Actually, it is well know that the military sector has been working on protection equipment to prevent troops from contamination during a potential warfare where chemical and biological agents are involved. The transfer of knowledge and equipment from the military to the civilian sector could help the EU to cover the lack of durability and multifunctionality in PPEs.

Some first responder collectives, firemen or police, are more familiar with the use of heavy and complex equipment in case of incidents, natural or man-made. Such heavy equipment could reduce their mobility during their presence on the scenario, which is important for carrying out their job.

A main concern when developing wearable PPE is to make it multifunctional (due to the potential presence of unexpected or unidentified threats or hazards) and to develop a user-friendly equipment at the same time. There are evidences that the first responders involved in the October 2001 anthrax attacks were contaminated despite the use of special PPE.

Many CBRN PPEs are based on the concept of big overpressure balloons with arms and legs. An important problem of the actual PPE is related with their low permeability to external HAZMAT that entail severe limits to their manoeuvrability and the feeling of a “boil in the bag” suit. The first responders perceive low information of the hazards around them and it is difficulty to exchange objects or fluids with the exterior; both facts make their work more complex, mainly for healthcare service. This list of requirements should be completed with the needs related to the decontamination process, which has to be carried out under specific conditions.

The actual PPE available systems and technologies are described in section 5.2.2.1 of DECOTESSc1 deliverable D6.2. Big gaps between the different threats or hazardous materials are identified in this section. The maturity of PPE for Nuclear or Radiological threats is greater than for Biological ones or some chemical non conventional/industrial hazard materials where hazmat suits have not been demonstrated at all.

A18.2 Description of the objective

Development of easy to use and lighter garments for first responder protection (PPE); including aspects such as, manoeuvrability concepts, lightweightness and durability, preservation of the normal vital conditions (avoid quick dehydration, etc) and new materials with multifunctional character to fulfil the overall spectra of a CBRN-Emergency.

The efforts on PPE should be carried out at different levels. One important effort should be done on the improvement of equipment in the sense of improving user-friendliness, comfort, and their correct

use, without forgetting the development of new materials to cover as much as possible all HAZMAT incidents, or the improvement of the breathing systems to cover CBRN. Other aspects to cover are the integration of an alert system to inform the user about the status of the environment or additional functionalities like decontamination capabilities. This objective should be complemented by the development of protocols to test PPE, about how to use the personal protection equipment and the definition of common standards.

The timeframe proposed to develop more efficient, durable and lighter PPE for Chemical or Biological or Nuclear and radiological equipment is 3 years. In case of PPE to protect first responders in a multi-threat event, the required time scale is 4 extra years.

A18.3 Products, capabilities and services

1.- Precise biodosimeter for Biological threats to inform the first responder about the level of contamination.

The improvement of actual dosimeters in terms of the transmission of alerts to the operation center or exposure level to the first responder is a necessary development. Industrial actors in cooperation with first responders and R&D institutions should join efforts to improve present biodosimeter to add new functionalities. The timeframe propose is 5 years.

2.- Multifunction and standardized personal protective clothing (mobility, lighweight, multithreat, communication, etc)

The standardization of clothes and their functionality increase could help the EU in the optimization and mobilization of resources in terms of share capabilities in potential CBRNE events. R&D in cooperation with industry and End-users should work together to achieve this goal in the next 5 years.

3.- More effective and lighter breathing systems.

The development of lighter equipment should carry out in the next 5 years by the cooperation between the research community and industry to provide such new products to the European Market.

4.- Training courses and protocols of how to use garments for the overall security chain actors.

All European community concerned actors, from authorities to developers, have to work in the achievement of a European Training Curricula for CBRNE events. The proposed timeframe is 7 years.

5.- New and effective materials and their manufacturing process for all PPE including multihazards.

To work in the development of new materials for PPE also means developing of new material processing technologies. These tasks should be driven by industry in cooperation with the R&D community. The time frame for achievement of this task is more than 5 years.

A18.4 R&D

The future of PPE will be based on new materials in conjunction with nanomaterials that will show new properties and increase the security of first responders and ease their rescue tasks; focussing the challenges on integration of new functionalities, additional information about the surrounding, communication, comfort, durability, manoeuvrability and more efficient equipment (mask, smart

filters, lither dosimeters, etc). The combination of these new functionalities will be assisted by training, protocols and standardizations processes.

- Development of precise and lighter CBNR dosimeters to identified the exposure level and roughly the character of the HAZMAT exposure. (>2016)
- Development of standard protocols for the correct use to permit the Europe to share equipment and personal in an easy way in case of crisis. (2018)
- Addition of functionality on the garment elements. (>2016)
- Development of new communication capabilities (online monitoring). (2018)
- Development of advance materials to cover the overall spectra of HAZMAT (>2016)
- Development of the breathing systems in the PPE (2016)
- Design of new concepts, joints for the clothes components (2018)
- Definition of common protocols about how to use and how to test for the garment within the overall EU. (2018)
- Definition of standards of new materials, cloths and equipments in terms of preferred means of demonstrating equipment conformity with the basic health and safety requirements. (2018)
- Development of multi-hazards PPE. (2016)
- Development manufacturing process of new materials. (>2016)
- Training course. (2018)

A18.5 Related issues and difficulties

- Acceptance of uniformity.

The unwillingness of national or local authorities to accept uniformity could be due to two main factors. The first one is related to the obligation to share information or technology and the second to the economic impact of the acquisition of new PPE.

- Standardization concerning threat, ergonomic aspects, etc.

From the standardization point of view, there are two main aspects regarding PPE that should be difficult to carry out: the level of ergonomicity of personal protection equipment and the material specificity to certain substances or compounds.

- Legal: How is it tested?

A key question on the improvement of PPE is the definition of the test validation because of the potential lack of adequate testing facilities, equipment or risk assessment of the potential consequences in humans during or after testing.

- Acceptance of test data

The acceptance of PPE test results by authorities or end-users could be difficulty due to the lack of experience and methods to compare or corroborate test data.

A18.6 Relation to other Topics

The design of multifunctional PPE with enhanced durability is a key factor for the recovering phase and the relationship with other Topics such as Topic 17 (real time threat assessment). Online threat assessment with updates in order to not always use the worse case equipment) or Topic 10 (stand-off detectors) is due to the need of PPE equipment on the sensors validation phase. Aspects like the multi-

threat protection and/or detection (Topic 16: detection systems) is a general shortcoming that needs to be covered by R&D activities. Also, the development of user-friendly equipment or the design of equipment where prior experience is not required for its use (Topic 6: deployment of equipment) are aspects related to the present Topic. Finally, the development of new sampling procedures or equipment is connected to the implementation of personal protection equipment.

References

Decotessc1 D6.2 / N. Brousse-Ducrocq et al. (2010): Decotescc1 Deliverable Report D.6.2 – State of the Art description.

Protective Materials for Emergency Responders. Dr. Sergey Gordeyev, NanoObservatory
http://www.observatorynano.eu/project/filesystem/files/Protective%20Materials%20for%20Emergency%20Responders%20UPLOAD.pdf

ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form: http://www.esrif.eu/documents/esrif_final_report.pdf

European Standards
http://www.hse.gov.uk/foi/internalops/fod/om/2009/03.htm

Annex 19 Accurate determination of acceptable residual levels concerning people, infrastructures and ecological effects (Topic no. 19)

A19.1 Introduction

A release of CBRN material can contaminate spaces and locations causing health and environmental risks. The following recovery phase may include decontamination of the affected site and restoring the environment as far as practicable to normal use. The need and extent of the site clean-up will depend upon the incident location, the types and amounts of substance used, their persistence and the severity of contamination. On the other hand, it is also possible that the contaminants will dissipate naturally over time and decontamination is deemed unnecessary. In either case, exposure to low levels of CBRN agent may occur after the affected infrastructures have been brought back into operation. Therefore reliable assessment of the potential risks caused by residual contamination is needed before declaring the contaminated locations safe. For this assessment, information on the exposure levels and health impacts are crucial.

The health impacts are commonly estimated by measuring contaminant concentrations in different media and estimating the uptake by different routes of exposure. The primary routes of exposure are inhalation, ingestion of food and water, or by absorption through tissues (incl. external radiation dose from gamma-emitting RN).

In order to determine how the likelihood and severity of adverse health effects are related to the exposure to an agent, a dose-response relationship is used. Typically, as the dose increases, the measured response also increases. The nonthreshold model implies that there is no amount below which an agent poses a zero risk, although the probability of adverse effects may be very low. On the contrary, a threshold model implies that there is a definitive threshold below which no adverse effects will occur. Both the dose at which response begins to appear and the rate at which it increases with dose depends on the agent, the kind of response, individuals, exposure routes, etc.

Knowledge of safe residual levels would help the authorities to define when it is acceptable to use again contaminated infrastructures and products from the contaminated area. EU should therefore be able to determine acceptable residual levels for CBRN agents concerning people, infrastructures and ecosystems.

A19.2 Description of the objective

The objective is to increase knowledge of potential hazards caused by residual contamination and possible impacts of each hazard. This information can be used to determine acceptable residual levels concerning people, infrastructure and ecological effects.

The more specific objectives have been identified as:

- Understand the migration of released harmful material in the environment and importance of possible routes of exposure
- Increase knowledge of long-term health effects of exposure to low-levels of harmful agents
-
- Understand the environmental consequences of CBRN releases
- Improve cross-sectoral cooperation for knowledge sharing with organizations dealing with CBRN related issues.
- Improve the use of existing data on long-term effects of CBRN low level exposures

In the short term it is possible to combine the existing data of CBRN long term health and ecological effects. Especially for the ecological effects there is a need for further research which will take more than five years. In short term it is possible to create connections to organizations in other fields but creating real cooperation might take 3 to 5 years.

A19.3 Products, capabilities and services

To define acceptable residual levels not only concerning people and infrastructure but also ecological effects the following capabilities should be provided by the EU member states in the next years:

- Understanding of transport and transfer rates of various harmful agents in the environment
- Ability to predict the exposure of humans or ecosystems to the residual contamination in a specific medium (air, water, surfaces etc)
- Ability to determine harmless negligible dose levels to humans or ecosystems from exposure to toxic agents or radiation
- Assessment of long-term research data on CBRN agent accumulation in humans, animals and plants, and other relevant ecological compartments (foodchains, soils, aquifers etc.), and effects on ecosystems for basis of decision making
- Understanding of required decontamination efficiencies to reduce exposures to acceptable levels
- Cross sectoral communication in CRBN aspects with parties from other sectors such as chemical industry, services for cleaning accidents and restoration, contamination control technologies, health and safety agencies dealing with toxicology, etc.
- Acceptance criteria for residual levels: The criteria should clearly define guidelines how to judge safe enough residual levels. The criteria are based on the effects of harmful substances on humans, infrastructure and ecosystems.

A19.4 R&D

For increasing the knowledge of acceptable residual levels concerning people and infrastructure and ecological effects there is a need to:

- Develop and refine models to predict the transport and fate of released harmful materials in built and natural environment
- Evaluate relevant toxicological studies to develop dose-response models
- Develop reliable risk assessment models to evaluate the long-term effects of exposure to low doses of CBRN on humans, animals and plants.
- Determine the acceptable long-term exposure levels due to residual contamination in different media
- Study the degradation of various CBRN agents in infrastructures and ecosystems
- Study the combined effects from different CBRN exposures: harmful agents can interact producing synergistic effects where the combined effect is greater than that of each agent separately.
- Identify appropriate biological indices of exposure for possible monitoring of exposed persons
- Develop network and means to share knowledge between parties in CBRN field and in other relevant sectors
- Define common EU criteria for acceptable residual levels of harmful substances

In addition to health hazards posed by current agents there is also a need to consider new and emerging threat agents whose properties are not yet known. The risk assessment models should be readily upgradable to address these threats.

It may also be necessary to take into consideration the effects of combined exposure. A multiagent exposure can result from the simultaneous release of two or more different agents, or perhaps more likely, due to occupation or personal habits. For example, industrial workers are often exposed to much higher levels of chemicals and therefore have a greater risk of developing disease from multiple exposures than the general population.

A19.5 Related issues and difficulties

While the allowable dose limits for ionizing radiation are well established e.g. by IAEA and ICRP, there is frequently lack of publicly available data especially for biological agents and human subjects. In addition, interspecies extrapolation from animal studies of dose-response relationships causes uncertainties into the dose-response analysis. Therefore determining acceptable contamination levels for bioagents is extraordinary challenging.

Another difficulty with some biological agents is to prove complete decontamination of a location while the absence of an agent is impossible to verify.

Legal and ethical issues can be caused if un-foreseen complications appear among exposed persons after a long time period, even if accepted residual limits have been followed. It may be difficult to identify the cause and the responsible party that will compensate damages.

Toxic by-products can be formed during cleaning procedures and degradation of the CBRN agents. These toxic by-products can cause unexpected health and environmental hazards.

The language used by experts in communication with the public may not be properly understood. Possible un-foreseen effects after a long time period will ruin the public's trust to responsible authorities, which is hard to regain. Acceptable residual levels may not be agreed by the population because public opinion may accept only "nothing left" without understanding e.g. the role of background exposure.

A19.6 Relation to other Topics

Topic 15 (affected people) and Topic 17 (real time threat assessment): determination of contaminated zone. This means determination and characterization of the used agent, contaminated area, contamination level and possibly affected number of people, infrastructure and ecosystem.

Topic 10 (stand-off detectors) and Topic 16 (detection systems): accurate detection systems. There is a need for improved systems to detect and identify various CBRN agents in very small concentrations and in various matrices.

Topic 8 (alert state), Topic 9 (communication with population) and Topic 25 (leadership in EU): Communication failure leading to lost trust to the authorities. Lack of strategies for the communication with the population (e.g. for gaining or keeping credibility of authorities concerning the effectiveness of recovery measures).

Annex 20 Effective procedures for handling mass casualties from CBRNE incidents (Topic no. 20)

A20.1 Introduction

In EU, many hospitals are already running near or at full capacity. Thus, they may not be capable to efficiently handle mass casualties of a large scale CBRNE emergency. The critical issues include necessary diagnostics, number of hospital beds, trained staff, and medical equipment or supplies. There is also lack of antidotes and vaccines if facing a large number of affected people in a short timeframe.

The medical chain also includes emergency care on site by ambulance services. An unresolved issue is triage after a chemical, explosive, biological or detectable radiological incident since in some member states the doctrine is such that medical personnel is not allowed in the hot zone and therefore triage may not be properly performed.

Depending on the type of incident and agent involved the admission and treatment of patients may differ largely. In explosive and most chemical events the effects appear immediately and there will likely be a flow of patients to nearby hospitals within a relatively short time period after an incident, putting pressure on triage, emergency transport, and intensive care resources. On the other hand, with biological agents the verification of exposure at the incident site is practically impossible. Because the time from exposure to the appearance of symptoms in infected persons takes much longer (days) it is possible that the victims will seek aid after the incubation period. There will therefore be wider peak period, and the victims may be geographically more dispersed. The pressure may be on longer-term demands on hospitals, isolation facilities, and the workforce. With radiological agents the time between exposure to radiation and the onset of the initial symptoms may be an indicator of how much radiation was absorbed, as symptoms appear sooner with higher doses of exposure. In each case it is anticipated that many persons will develop symptoms even with no exposure so that psychosocial issues must also be addressed in the potentially exposed population.

A20.2 Description of the objective

The objective is to significantly improve the capabilities and capacities to deal with an unexpected flow of mass casualties resulting from sudden or relatively slowly evolving CBRNE incidents. The cornerstone to this is the ability to rapidly enhance medical capacity to care for a large numbers of victims. More specific objectives have been identified as:

- improving the local, national and EU-level capacity for treating a large number of affected people in unexpected incidents
- improve knowledge sharing and on-line access to information in a case of a CBRNE incident
- new and improved antidotes, vaccines, and medical equipment available in adequate numbers
- develop alternative logistic plans for rapid deployment of stockpiles from various locations
- rapid deployment of sufficient medical treatment
- improving the identification of non-hurt people and their management
- improving communication between authorities and the public to better inform public about treatment/decontamination they can start themselves, e.g. take shower, destroy contaminated clothes etc. This also reduces the peak burden on hospitals
- improving the capabilities for large-scale triage and alternative sites for medical treatment
- enhancing cooperation between organisations in CBRNE emergency management, covering both civilian and military organisations

- enhancing cooperation between organisations in CBRNE emergency management, covering both civilian and military organisations

In short term, it is possible to solve issues that hinder the current cooperation and capacity sharing in CBRNE emergency situations. Increasing the capacities includes investments on necessary equipment and agreements on sharing the capacity between EU member states.

In medium and long term, research is required for development of new antidotes and vaccines and diagnostics.

A20.3 Products, capabilities and services

For improving the capacity to treat a large number of affected people in sudden incidents, EU member states need to increase their medical care capacities for CBRNE. The following services should be provided by the EU member states in the next years:

- Adequate number of competent CBRNE professionals;
- Alternative facilities for medical and other treatments of affected people;
- Adequate number of essential medical equipment;
- Adequate diagnostic capacity.

There is a need for flexibly increasing the number of trained staff on demand and keeping up their skills. This means identification of current professionals as well as educating new ones. For tracking the professionals, it is essential to keep a record on those professionals capable of CBRNE care at various tasks required. At the moment, member states may have some records of their own, but an EU-level database does not exist. For the database, a common view of required medical expertise needs to be agreed for categorisation, in order to enable the sharing of professional staff between member states in a case of a crisis.

For ensuring the availability of CBRNE professionals, related education and training should be organised in a systematic manner. This includes the possibilities to utilise education and training facilities in other member states.

Plans for the use of alternative facilities for medical and other treatment, including transportation, are essential. These may include e.g. identification of alternative locations or plans for using field hospitals. The plans must also include actions to assure the availability of alternative locations or field hospitals in a short timeframe, like through agreements with the facility providers.

There is also a need to assure the adequate number of essential medical equipment as well as basic items like hospital beds to treat a large number of affected people. Accordingly the capacities for short and long-term diagnostics within EU should be tracked for shared use, and improved when missing capacities are identified.

The information of available facilities, medical equipment and diagnostic capacity should be integrated into the existing EU-level database CECIS under MIC. Through MIC procedures, the CBRNE capacities will be better accessible by all member states.

To provide an access to specialist information, there is a need to ***set up a knowledge center*** on those specialists with a specific required expertise. The knowledge center will be a virtual one which can be reached trough phone or internet. The knowledge centre will provide CBRNE information on request 24/7.

New ***procedures to share antidotes, vaccines and treatment capacity*** need to be agreed between EU member states. Relevant stakeholders include both public and private bodies that can provide medical products and services on a short notice. Related agreements with product and service providers should be reached within a year or two.

It is likely that after an incident the number of unexposed individuals requiring psychosocial support is far greater than the number of persons who are physically injured. Therefore rules and practical ***procedures for handling "non-hurt" people*** are required to enable the fair and efficient identification and further care of people not affected by CBRNE agents. These procedures will include rapid diagnoses and means for psychosocial aftercare. Some of basic procedures already exist, but there is a need to expand rapid diagnostic capabilities to treat a massive flow of people. There is also a need to further develop practices for psychosocial aftercare in cooperation with psychological and behavioural experts. The development will take 3-5 years.

Improvement in the availability of ***field hospital facilities and large scale triage*** will be achieved through systematic development of cooperation between CBRNE and e.g. military and rescue organisations. This will be reached both at EU and member state level to enable the sharing of capacities nationally and cross-border operations.

A20.4 R&D

For improving the treatment of a large number of affected or "worried-well" people, there is a need to develop:

- New capabilities that will improve response including diagnostics, accommodation, treatment and transportation;
- Rapidly deployable, mobile, modular and autonomous field hospitals with supportive care capacity
- Training of medical professionals with CBRNE expertise;
- Common curricula for CBRNE medical training in EU for supporting the cross-border sharing of medical professionals in a case of a CBRNE incident;
- a knowledge centre for 24/7 information sharing and expert support
- a network of training facilities throughout EU;
- EU-level procedures and protocols on sharing the civilian and military capacities in a case of a large scale CBRNE incident
- Procedures to share antidotes, vaccines and critical medical equipment rapidly;
- New antidotes and vaccines;
- New/improved medical tools for quick and easy treatment and fast diagnostic techniques;
- Methods to efficiently identify and differentiate affected and non-affected people;
- Guidelines and procedures on how to treat in a psychological manner those people affected and possibly affected;
- Technologies and procedures to improve triage and emergency care at the incident site
- And review current practices worldwide from natural disasters and safety incidents within e.g. chemical or nuclear industry, and incorporate best practice that could be applied to CBRNE attacks.

A20.5 Related issues and difficulties

Handling of mass casualties in a short frame of time raises ethical issues while treating a large number of affected people with limited resources. Rush and difficult working environment may decrease the quality of treatment of the victims. Also the treatment of other patients may be deteriorated. Cultural differences may also cause challenges in treating the people while required procedures like undressing may not be accepted and followed.

Long term aftercare may cause economical and societal problems to the affected victims. Planning for efficient CBRNE aftercare and individual recovery may be learnt from military side.

It is apparent that high cost of developing rarely used drugs discourages commercial pharmaceutical industry R&D without military or governmental support. There may also be ethical barriers to controlled testing of drugs with sick people, which makes it slow to get new drugs accepted.

- Legal acceptance of e.g. new antidotes to enable best protection and care of citizens;

A20.6 Relation to other Topics

Topic 7 ((inter)national cooperation): Collaboration between countries and authorities in order to share existing CBRNE capabilities and capacities would improve the availability and efficient use of national and cross-border resources. Predefined cooperation structures would also shorten time for action. Improve knowledge sharing and on-line access to information in a case of a CBRNE incident by improved national and cross border cooperation structures.

Topic 18 (adequate PPE): Improve the availability of personal protective equipment for medical staff.

Topic 17 (real time threat assessment): Develop real-time communication between various stakeholders to improve situation awareness and real-time threat assessment. This includes receiving on-line information on situation to enable the prediction of e.g. how many more casualties will come in within an hour.

Topic 9 (communication with population): Credible communication with population requires improvements also in the identification of non-hurt people and their management.

Topic 15 (affected people): for the planning of response and recovery activities there is a need for fast identification of affected people. Fast and reliable information on the number of affected people is necessary to get an idea on the size of an incident as input for the decision support.

Annex 21 Capabilities for decontamination of electronics, rough and/or porous surfaces (Topic no.21)

A21.1 Introduction

Decontamination is defined as the procedure of cleaning surfaces, devices or also the human body in order to remove contaminations by hazardous materials (e.g. infectious particles, chemicals, radioactive compounds). For its realization mainly chemical substances are used and in some cases also physical interference might be applied. Decontamination media are chemical substances or nanoparticle compounds to eliminate or to modify the dangerous level of threats; however which might also damage the surface itself and the electrical equipment. For B (and some of C) threats other means like radiation (i.e., UV, Gamma) can be used to disintegrate or modify the threat substances (kill bacteria/virus by disrupting macromolecules such as DNA). A further option for B-agents might be the sterilization by heat and/or vapor.
Other mechanical treatment, such as washing off, might cause stress to any surface. Especially for porous media the threat substances can penetrate into deeper layers and would therefore be well protected against simple mechanical treatment. Applying such approaches, problems may arise by the disposal of enough liquid products for decontamination or detoxification, especially when large surfaces have to be decontaminated.
Another strategy would be the avoidance of any contamination by applying inert surface modifications. New developments of nanotechnology offer options for the modification of surfaces in order to allow easier decontamination or even self-decontamination by neutralizing hazardous materials.
The strategy used for decontamination is strongly dependent of the type and function of the contaminated device or surface. For critical infrastructure methods must be applied that guarantee a damage-free decontamination. Depending on the importance of this infrastructure the possibility of easy decontamination should be considered already in the construction phase. In case only a small number of computers need to be decontaminated, there are methods available to recover the functioning of the electronic device and remove threat substances. For large scale contamination, the problem is still unsolved, as the costs for decontamination might be much higher than the replacement of the electronic devices. Possibilities for data recovery have to be established.

Description of the objective
Major goal of decontamination is the remove or neutralization of threat substances from surfaces, equipment or other infrastructure. Therefore the best suited method for the contaminated target must be identified and developed. In order to reach the goal, several aspects have to be considered:

- Electronic devices are sensitive to immersion or wet treatment
- Substances might be difficult to remove from porous substances
- Neutralization is possible, if the used agents can penetrate the surface
- Success validation procedure has to consider the risk factors

A21.2 Products, capabilities and services

The main target group identified out of the objectives of this gap is the workers involved in recovery of affected places or contaminated products. Further target groups are the first responders, when decontamination is necessary for safe rescue of victims and the policy maker in order to raise awareness of new technologies and methods.
For the different threat substances (C/B/RN) different methods for decontamination will be necessary. Therefore different products and services need to be established:

The major product in order to fulfill the objectives is the development and establishment of tools for safe decontamination. Such tools should be accompanied by the establishment of defined methodologies or routines or procedures for safe cleaning and/or decontamination or detoxification.
On the other hand the development of materials for reduced contamination effects (e.g. nano-materials) should be envisaged; another related strategy is the establishment of structured surfaces that are easier to decontaminate.
In order to ensure complete decontamination of all surfaces that might have been affected a simulation tool for modeling the spread of agents (ideally combined with real contamination tests with subsequent decontamination demonstrations for its development) would be appreciable. Such simulation software might be combined with tools for the visualization of contamination to guide decontamination measures (linking sensors to software tools)
In different European countries different regulations and technologies are applied. Thus the communication of available methodologies for decontamination of electronics and porous surfaces or their invention should be encouraged. In order to achieve the best suited solution a ranking of the most suited methods depending on the targeted application should be carried out.

A21.3 R&D

Each threat substance has a certain dose of in order to be harmful to humans. Therefore the knowledge about thresholds or limiting values (e.g. maximum permissible value) is necessary for developing a decontamination strategy as well as guiding a decontamination procedure. Based on legal regulations, toxicological basic knowledge and other sources of information suitable (achievable) threshold values have to be defined.
Subsequent to decontamination the whole procedure and the achievement of safe levels has to be assessed. Therefore such assessment strategies depending on the type of threat agent have to be established also regarding defined threshold levels. The possibility of a combination of different decontamination methods to reach the predefined level of cleanliness has to be considered.
A further strategy to facilitate decontamination or even to avoid the necessity of decontamination measures is the development and application of materials with low or even zero contamination properties. The use of non-contaminating surfaces has to be standardized and promoted. Such new materials would be the nano-technology based surfaces with antibacterial character, or e.g. super-hydrophobic surfaces for all types of threats.
At last also the decontamination team needs to be specially trained in order to be able to apply new methods concerning the procedures necessary for gaining best success. Such trainings and exercises of the whole decontamination process must also include a check for the achievement of successful decontamination. Further the lessons learned from previous events (real attacks or training situations) should be included in such educational courses.

A21.4 Related issues and difficulties

- From the legal perspective the persons or groups who take responsibility to give “limit values” need to be defined and also the responsible persons or groups for risk management and success assessment.
- Economical and financial issues have to be considered before starting response measures. The responsible persons have to be aware to the high risk, but also of the low probability of events; Potential attack targets usually have high economical values and need to be recovered (airports, subways etc.).
- Detection of small amounts of contamination is often difficult. In order to check the effectiveness of a decontamination process, it is necessary to use very sensitive detection devices to obtain reliable information on the remaining hazardous substance. Precise measurement well above the detection limit is necessary. A definition of the toxic level that the equipment and surfaces can have without affect people has to be established.

- From environmental point of view the correct disposal of used chemicals and washing water has to be ensured. Impairment of normal sewage processing has to be expected; therefore a specialized treatment of wastewater or similar liquids is appreciable. Measures for a limitation of spread of waste water (liquids) have to be established.
- In order to consider economic effectiveness a cost-benefit analysis might often give the result that a comprehensive decontamination is more costly than the demolition or disposal of an infrastructure.
- The public acceptance of the success of decontamination might be difficult to obtain. Many people will have more trust in the demolition and reconstruction of a building than the reuse of infrastructure after decontamination.
- A high investment in the improvement of decontaminability of infrastructure or electronics may not be cost-efficient in comparison to the low probability of an incident needing decontamination.

A21.5 Relation to other Topics

Topic 20 (medical capabilities)

Topic 19 (residue level): residual values for infrastructure, people and the ecological effects. Setting correct limiting values depends on ecological/toxicological considerations, but also on the capabilities, which are necessary to prove the success of decontamination (measurement above detection limit). Technical capabilities must be in place to reach the limiting value by available decontamination methods.

Topic 13 (standards for infrastructure): lack of minimum standards for security relevant infrastructure. The easy decontamination of surfaces should be an issue for the design of infrastructure / surfaces.

Annex 22 Minimizing of first responder risk during the safe sampling collection (Topic no. 22)

A22.1 Introduction

As second step of the response phase after helping the victims, an important task, the collection of samples, has to be carried out. This crucial task is carried out by police or medical services and is required for the identification of agents used on the attack, the attack procedure, the identification of the terrorist group, the spread of contamination, exposure, dose, etc. Their job is disturbed because some evidences could be destroyed, modified or else disappears because of their degradation.

The protection of first responder during the sampling process has to be analysed at the overall sampling process: sampling strategy definition, collection, transportation, extraction and analysis. The different nature of CBRNE threats and hazardous materials and their different media of transmission (surfaces, liquids, airs) involve a different strategy for collecting samples. For vapour samples, the most important need, due to their volatile nature, is to store them appropriately until they can be analysed. Other aspects to consider are the definition of the sample size and location to get representative idea of the overall scene, how many samples to collect and from where. Also, the development of specific methods and methodologies definition in the collection of evidences from different surfaces is required. Transport of the evidence and sample preservation from degradation require harmonization of protocols to achieve a good degree of standardization in Europe.

A big gap exists in the time required for collecting the samples especially regarding their appropriate handling to preserve them. Also, protection of first responders from the risk to contaminate themselves because of lack of information, correct equipment or experience is vital. To avoid this, the development of robotic instruments for remote sampling or the improvement of protection equipment is crucial for ensuring secure manipulation of evidence.

The sample collection method is strongly dependent on detection systems used at the scene; the development of faster, easy to use, efficient or instantaneous sensors is a main challenge to achieve during the next years. The correct sample manipulation and quick identification of the threat have to be carried out by experienced responders. The recognition of symptoms of the victims (haemorrhages, blister, temperature…) could help to identify threat, to stop person to person transmission and to define the contaminated area. The experience should be achieved within specially targeted training exercises. A potential solution to help first responders with sample collection is the creation of a specialized team inside police or governmental agencies with the focus on sample collection.

Actually, the evidence collection after a CBNRE attack does not cover aspects such as safety of all personnel involved in the event, information on the hazard level to first responders, specific equipment including communication systems or improved clothing for faster operations.

A22.2 Description of the objective

Due to the complexity of sample collection, there is a need to develop tools, procedures and equipment to close this gap. More specifically, the objective is to develop simulation tools to investigate sampling strategies, decontamination procedures, protocol harmonization of protocols for sample manipulation at all levels, new training strategies and novel and/or better equipment for various aspects such as remote sampling and information transmission, more precise and faster detection systems to support sample collection, stand-off detection technologies, sample containers and more comfortable garments and equipment for first responders.

A22.3 Products, capabilities and services

1) Simulation tools
Each CBRNE event depends on many variables, so there are no two equal ones. Knowing before hand what the best possible sampling strategy is can be very important. Because of this, it is necessary to develop a software based tool for finding out which is the most effective one for each CBRNE event. The time-frame for this tool is 2016.

2) Procedures and protocols
The sample collection chain depends on many different aspects such as the nature of the hazardous material or the means of propagation as well as being composed of several different steps such as sampling strategy definition, collection, transportation, extraction and analysis. All of these have a direct link to the safety of the first responders. In order to minimize such risks it is necessary to harmonise protocols and procedures that will also require specific EU policies, especially for sample collection, preservation and transport and introduce procedures where necessary as is the case, for example, for the decontamination of items used by first responders. The time-frame for these products is 2017 to 2020.

3) Training
There are crucial aspects that rely on the first responders' experience such as the manipulation of samples, the quick identification of the threat or the recognition of symptoms of the victims. It easy to imagine that an incorrect definition of the contaminated area can have very serious consequences in terms of spread of the infection which can make the difference between a serious but contained threat and a disaster. Much of this experience should be possible to acquire with specially targeted training exercises. Thus, the establishment of training strategies involving all actors and targeting at the complete sampling chain from collection to analysis and result distribution is important. The time-frame for these services is 2020.

4) Equipment
Much of the safety of first responders will depend on the equipment they have available foir carrying out their work. Developments in novel automatic remote sampling equipment and remote identification of contaminated areas by technology integration into UAVs are very important. The time-frame for these products is 2018.
Nevertheless and for the foreseeable future, it will be still necessary for first responders' presence on-site. To increase safety in this case, more precise, lighter and faster, ideally real-time, sensors, dosimeters and detection systems, including stand-off, are required in order to provide basic information about the level of toxicity and the dangerousness of the threat. The time-frame for these products is 2016 to 2018.
Other important products that need development are appropriate sample containers to guarantee the custody chain and avoid sample or personnel contamination, more comfortable garments and equipment for first responders as well as improved communication between civil and military control centres. The time-frame for these products is 2016 to 2017.

A22.4 R&D

The most important needs on R&D for sample collection are:

- Improvement of remote and automatic system for sample collection. (2016)
- Improvement of simulation tools for identification of the sampling strategy. (2016)
- Improvement or development of dosimeters (CB 2016 and RN 2014)
- Development of sample containers (CB 2020)

- Development of decontamination protocols (CB 2020 and RN >2020)
- Development of low cost and easy to carry sensors for CB agent identification (CB 2016 or more)
- Biodosimeter development for virus, bacteria and spores (B 2016).
- New materials for cloths in order to increase protection (e.g. hands, face or eyes.) (2014)
- Embedded electronic in the textile for first responder location, communication and monitoring (2014).
- Ergonomic improvement of garment to help on task such as manoeuvre instrumentation (2016).
- Multi-disciplinary courses (2020).
- Standards and policy definition by governments and EU (2020).

A22.5 Related issues and difficulties

Decontamination of of tools and garments:
The issue in this case is to know what is the decontamination level since this is not defined and much less agreed upon by Eu countries.

Standardization of procedures between different actors (police, military, medical, …):
It may be difficult to convince the military and different countries to share between them the necessary information to achieve this objective.

Ergonomic aspects:
The problem is that usually improvements in ergonomic aspects of protection suits will result in a lower protection level for first responder. Again, where to draw the line may be an issue.

Use of monitoring instead of sampling:
Monitoring systems may not have the necessary level of precision and a counter test in case of need will not be possible.

A22.6 Relation to other Topics

Since risk minimisation of first responders is at issue in this Topic, there is a direct relation to Topics that address safety issues from the point of view of equipment, such as Topic 16 (detection systems) and 18 (adequate PPE), and from the point of view of capabilities as is the case of Topic 17 (real time threat assessment).

References

[1] Nick Castle et all. *What is the optimal position of an intubator wearing CBRN-PPE when intubating on the floor: A manikin study*. Resucitation 2011, to be published.

Decotessc1 D6.2 / N. Brousse-Ducrocq et al. (2010): Decotescc1 Deliverable Report D.6.2 – State of the Art description.

Protective Materials for Emergency Responders. Dr. Sergey Gordeyev, NanoObservatory
http://www.observatorynano.eu/project/filesystem/files/Protective%20Materials%20for%20Emergency%20Responders%20UPLOAD.pdf

ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form: http://www.esrif.eu/documents/esrif_final_report.pdf

CHEMICAL, BIOLOGICAL, RADIOLOGICAL OR NUCLEAR (CBRN) DETECTION: A TECHNOLOGICAL OVERVIEW (2005)
http://www.senato.it/documenti/repository/lavori/affariinternazionali/nato/167CivileJoplingEN.pdf

Annex 23 Good tools for crisis management for the accurate prediction of hazard (CBRNE) (Topic no. 23)

A23.1 Introduction

In general, crisis management is the process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public. In CBRN crisis management, understanding the situation is a key priority for FRs. There are many new technologies at hand to increase the situational awareness. New sensors facilitate more accurate visualisation of a situation, while C2 (command & control) infrastructures now rely on the compilation of a growing amount of information. The user interface can be tailored for specific use of FR on-site or more sophisticated applications for remote commanders (PDA, blackberry, laptops, dedicated CC radio equipment, etc.). Consequence management to overcome CBRN attacks and hoaxes requires development of more effective and reliable detection and identification capabilities, including detection networks, data fusion, distribution of signal output and decision support tools (p. 21-22, ESRIF report).
Concerning the accurate prediction of hazard, refined dispersion modelling and tools for predicting the transport of agents in the biosphere / atmosphere as well as indoor situations are needed (D.7.2, chapter 6.3). Especially for complex in-door situations, there is only scarce number of tools available, mostly based on computational fluid dynamics. At present, sophisticated models require a complex set of input parameters (e.g. meteorological conditions, signature of landscape, soil type) and are usually classified by national authorities, state-of-art examples are given in D.6.1. For in-door modelling information on the building design and ventilation systems are crucial input data. Especially the dynamic development of the threat situation in terms of hazard dispersion over large areas, availability of FR staff on site, number of victims to be treated etc. needs to be predicted and visualized (D.7.2, chapter 6.3) by consideration of real-time (measurement) data inputs in order to continuously refine predictions.

A23.2 Description of the objective

The objective is to develop user-friendly and comprehensive software/hardware solutions for the accurate prediction of CBRNE hazard by integration of various information and visual representation as decision support with direct linking to command and control systems and the possibility of communication between the command centre and first responders on-site. User-friendly output devices like PDA, blackberry or laptops, tailored to the need of the respective stakeholder group need to be taken into account for comprehensive crisis management systems. Systems need to be applicable to all kind of scenarios (indoor/outdoor; urban/rural, complex infrastructures etc.) and cover prediction in a wide sense.

A23.3 Products, capabilities and services

- Fast and comprehensive situation awareness by collection of all necessary information (detector data, weather data, epidemiological data, early warning systems, threat assessment/intelligence data), sampling and analysis to verify a threat and provide input for decision support. For in-door releases: info about building (plan, area, volume ventilation system). (2016)
- Availability of simulation tools to process real-time data and all the input data and produce maps and integrated information for decision support. Evolution of the incident, spread of contamination in complex infrastructures, in-door dispersion etc.)(Feed into command & controls systems; 3-D representation of results and visualization of evolution of events in space and time). (2016)

- Decision support tool (incl. software, sensors etc., experts) for comprehensive situation awareness (making use of collateral data, sensor data, intelligence info etc.) – simulate spread of diseases (B) or contamination (C, RN) and plan countermeasures (vaccination, treatment, limitation of contamination) and organizational response (prepare hospitals, set up isolation tracts, decontamination units etc.). (2016)
- Establishment of a Command & Control centre on National level and software systems to coordinate the operation from a central point and keep communication with all involved stakeholders (2015)
- Ensure permanent availability of the crisis management systems by regular training the validation on realistic training scenarios (not only desktop studies but field exercises). (2015)
- Organization of regular exercises including many (all) stakeholder groups, especially the public and representative mass media (broadcast radio, television, online (internet) newspapers) to raise awareness for correct behaviour in CBRNE incidents. (2015)
- Establishment of short-cut communication networks to link all relevant first responder organizations plus intelligence and other relevant parties (e.g. decision makers) to each other on regional command level. (2016)

In the recently started Integrated Project "PRACTICE", which proposes a comprehensive toolbox for CBRN incident management, many of these products will be developed. For all these points, a basic version can be developed within a timeframe of 5 years/ until 2016.

Specific to threat agents (products, capabilities):

- Develop and implement networks of stand-off detection systems (B: 2020; C, RN: 2016)
- Develop harmonized protocols for sampling and detection (by trained FRs) of threat agents in suspicious regions; exclude general public – verification of threat (B: 2016, C, R: 2013)
- Availability of adapted decision support systems to be applicable for "small-scale" incidents (e.g. dirty bomb) and in-door as well as complex urban scenarios. (2016)
- Software for localization (backtracking) of the origin of the B-threat and identify potentially affected people. Prediction of spread of disease in time and space (2016)
- Central Contact point to register incidents of unlikely diseases (e.g. radiation syndrome), conspicuous cases from hospitals and medical services (family doctor, general practitioner) and raise awareness for lumped incidences of diseases. (2013)
    - Database of symptoms and diagnostic indicators and state-of-art treatment for relevant B-threats (2013). This can be done at European level in collaboration amongst Member States.
    - Register of findings of unauthorized transport and handling of radioactive sources/materials;
    - Publication of any lumped incidents of radiation symptoms (2013)
- Awareness building on all levels of the health system to register any suspicious case promptly and consult Central Contact Point to detect anomalities (2013)

A23.4 R&D

ESRIF WG6 on CBRN (WP4) and also Decotessc1 Gap Analysis (D.7.2) defined following needs for research:

- Integration of information coming out of detection networks, intelligence, and dispersion modelling. Integrated information (CBRN situational awareness) must be fed into decision support tools and integrated into command and control.
- Develop modelling capabilities for attack simulation and intervention planning taking place at numerous incident sites (in/out-door, urban, sub-urban, rural, industrial, infrastructure).
    - Fast forecasting of incident propagation;
    - Health evolvement of exposed persons;

  - Dispersion modelling tools in urban environments and complicated in-door situations, as well as complex critical infrastructures such as airports, harbours, and big events; plus experimental validation of model output quality to verify validity of chosen boundary conditions and parameterization.
  - Development of 3D maps of high-level targets and tools for data integration to provide visual representation of complex information.
- Develop tools to calculate the impact (also higher order) of CBRN attack employing metrics other than casualties (e.g. psychosocial impact or economical impact)".
- Testing and verification of simulation tools by experiments with life agents (or stimulants) under realistic outdoor conditions
- Development of improved decisions support tools usable by FRs on-site (making use of real-time detector measurement)

A23.5 Related issues and difficulties

- Legal/Ethical: responsibility for untrue, wrong predicted values / hazards; e.g. triggering an unnecessary evacuation decision;
  Wrong predicted values cause wrong decisions for command & control → threatening the health of FRs (e.g. too long operational times; wrong PPE selection).
- Economical: wrong decisions can be expensive; responsibility for carrying costs of unnecessary interventions
- Time delays to start intervention operations due to lack of clear responsibilities for decision making (dramatic increase of damage in terms of lives and costs)

A23.6 Relation to other Topics

Topic 5 (realistic training): Only if people using a decision support tool are trained, the interpretation of results can be done with self-confidence and mistakes are minimized. Also, only with training it is possible to carry out the tasks in a minimum of time and avoid any delay in the response. (User-friendliness of DSS-software can be improved).

Topic 6 (deployment of equipment): the task of information collection for situation awareness can only be carried out by first responders coming to a scene (in many countries voluntary staff with a limited level of specialized training), if they have access to user-friendly detectors. Today, only experts can handle the available detection equipment as it needs specialized education not only to carry out the measurement but also to interpret the instrument reading.

Topic 8 (alert state): although it is always a risk to spread information on possible threats to a large number of people (producing unnecessary fear / panic) this allows to detect real threats very early and implement countermeasures immediately (esp. for B-threats early detection can safe a large number of lives, if the outbreak of a pandemic can be avoided).

Topic 10 (stand-off detectors): at the moment stand-off detectors for C/RN/E threats are available but far from being cheap enough to allow a spatially comprehensive deployment. For specific kind of infrastructures, it could be a very big benefit to have such instruments available. Input from stand-off detector networks to crisis management tools can be a real improvement for situation awareness and decision making.

Topic 15 (affected people): Only if such tools for identification of victims are available, the respective information can be used for crisis management to limit the number of highly affected victims (by early treatment or application of countermeasures; e.g. decontamination)

Topic 16 (detection systems): such systems are a crucial ingredient for crisis management. Only with comprehensive and fast information on the extent of hazard FR can enter an incident scene and start response actions on site.

Topic 17 (real time threat assessment): this is an important kind of input data for a crisis management tool (situation awareness, selection of countermeasure actions).

References

D.7.2 / Ehlerding, A. et al. (2011): Decotessc Deliverable Report D7.2 – Gap analysis. Classification Level: Secret

ESRIF (European Security Research Innovation Forum, eds.) (2009): ESRIF Final Report. ISBN 978-92-79-13025-0; 323 pp. Available in electronic form: http://www.esrif.eu/documents/esrif_final_report.pdf

ESRIF_WG6_WP4 (anonymous) (2008): Outlining CBRN R&D achievements to fill mid- and long-term capability gaps WG 6 on CBRN. Available in electronic form: http://www.esrif.eu/documents/esrif_additional_material.zip

Annex 24 Standardisation and Certification of CBRNE detection equipment (Topic no. 24)

A24.1 Introduction

The detection of CBRNE threatening materials and the assessment of their hazardousness is nearly exclusively obtained by the use of detection equipment. To ensure that a CBRNE threatening material of a specific kind and hazardousness can be properly evaluated and identified it is essential to know the capabilities and performance of the used detection systems. Because generally many different detection systems and equipment is deployed even for the detection of the same threatening material it is necessary to have comparability between these systems. When purchasing and using the equipment it is also of immense importance that it fulfils the requested capabilities and requirements. Not least there are national differences concerning the requested properties and requirements for the detection equipment. Therefore it is often the case that there is no comparability of the specifications of the equipment or the results obtained from the performed measurements. Taking all these things into account it becomes obvious that a standardisation of the CBRNE detection equipment is essential. E.g. regarding the standardisation of E detectors the commonly used ECAC Testing Methodology (ECAC CTMs) for testing and approving for example metal detectors or explosives bulk or liquid explosives detectors for their usage at airports may serve as good starting point to set-up a suitable testing and evaluation scheme for other than airport scenarios. ECAC CTM's include always a set of benign samples together with explosives samples to be able to analyse the false alarm rates of the tested detectors.

A24.2 Description of the objective

The main objective is the development and implementation of harmonised standards for CBRNE detection systems and related equipment on EU-wide level. For this purpose the creation of a certification system and the production and harmonisation of CBRNE related standards are required. The European Committee for Standardization (CEN) should therefore unify and combine all standardisation related issues concerning CBRNE. Accreditation of CBRNE testing facilities, organisation of information exchange or the continuing development of standards is a prerequisite to achieve comparable and reliable information on detector capabilities. The timeframe for achieving the objective is about 5 to 10 years.

A24.3 Products, capabilities and services

1) Harmonised standards for CBRNE detection systems and related equipment on EU-wide level

The main instrument for achieving comparability between different detections systems or related equipment is the standardisation of the detection systems, testing procedures, the equipment which is required for the tests and the documentation and exchange of testing results. For achieving a coherent standardisation there is the necessity of having standards for the related equipment and procedures based on realistic incident scenarios. For an effective work these standards must be harmonised between the different countries on a European level. For E detectors also ECAC specific procedures may be adapted. The related timeframe is about 5 to 10 years.

- Standards for sample collection:
  Many of the detection systems need to collect samples before they can perform measurements. This can be done by taking samples from the soil, air, water or by taking swipe samples. Because

the measuring results depend in most cases on the way how the samples were collected the sample collection itself must be standardised.

- Standards for testing samples:
  For the performing of standardised tests there is a need for production and use of standardised testing samples. The design and characteristics of these testing samples should be based on realistic incident scenarios and reflect real possible CBRNE detection tasks.

- Development of common testing methodologies for the scenario-specific testing of available and future E detectors including development of suitable testing samples for current and future threat materials (trace surface contamination samples, vapour samples, study ageing / stability of samples etc.)

- Standards for testing procedures and protocols:
  The standards for testing procedures and protocols should also include a scenario based approach. These standards ensure that the tests which are performed by the testing facilities are comparable with each other. The usage of standardised testing procedures effects also an improvement of the quality assurance.

- Standards for detectors themselves:
  The standards for the detectors themselves are a set of requirements for the detectors to pass a certification. These standards set minimum requirements concerning hardware, software, manuals, false alarm rates, human factor, etc. which are necessary to ensure the fulfilment of the capabilities and requirements which are requested by the end-users.

- Procedures for the exchange of test results:
  These standards include standardised reports, information exchange procedures and reporting guidelines.

2) EU-wide accepted certification of equipment related to CBRNE detection

The EU-wide accepted certification would be granted by a European CBRNE certification organisation and should be based on the tests results which were performed by accredited manufacturer-independent testing facilities. The requirement for this kind of accreditation of a testing facility would be the usage of all the EU-wide CBRNE standards and compliance with accepted accreditation procedures like ISO 9001 and ISO 17025. The certification will be accompanied by a labelling system. Furthermore EU- and national law should ensure that only certificated equipment should be used for CBRNE security purposes by the end-users (border security, first responder, monitoring systems, etc). ECAC-like common testing procedures may also be adapted in EU27. The related timeframe is about 5 to 10 years.

3) EU-CBRNE-Certification organisation

For the exchanging of information, enforcement, coordination and development of standardisation related issues there should be an EU-CBRNE-certification organisation with the following tasks and sub-sections. Regarding airport security also the ECAC should be involved. The timeframe for the creation of the following organisations, platforms and forums is about 5 to 10 years.

- An organisation which grants the CBRNE certificates. This organisation would tender tests, collect the test results and decide about successful awarding of certificates.

- A communication platform and network for the information exchange between end users, testing facilities, decision makers and manufacturers. This platform should especially enable an exchange of information between the decision makers and testing facilities.

- A forum for the continuing development of CBRNE standards. Participants of this forum should be the end users, testing facilities, decision makers and manufacturers which are involved in the field of CBRNE security. This could be covered by the CEN.

- An organisation for accreditation of CBRNE testing facilities or at least an organisation which coordinates the accreditation processes performed by national accreditation bodies. This organisation will approve the accreditation and supervise (or coordinates the supervision by national bodies) the testing facilities to proof compliance with the standards for CBRNE detection systems and related equipment.

A24.4 R&D

In the following are described the necessary research and development steps which are needed in order to reach the above mentioned capabilities. It must be taken into account that there are already related and ongoing or recently finished projects and results obtained by these projects: e.g. CREATIF and follow-on projects or ITRAP+10. The research and development should take place in cooperation with these projects and also with exiting standardisation organisation like ISO/IEC, ANSI, CEN, ECAC, etc.

- Investigation on already existing standards. The first step of the development of harmonised standards on EU-wide level is an investigation on the already existing standards. Based on the results of this investigation it should be verified if the standards are adequate for the purpose they are made for. This verification should also include the analysis of possible harmonisation between the different standards. The timeframe for this investigation is about 1 to 2 years.

- Investigation on existing organisations concerning standardisation issues. For the formation of an EU-certification organisation there is a need for an investigation on existing communication platforms, standardisation organisations (e.g. ISO/IEC, ANSI, ECAC etc) and ongoing research concerning standardisation issues. A verification of the possible harmonisation, cooperation or fusion of the investigated organisation is also essential. This could be supervised or done by the CEN itself. The timeframe for this investigation is about 1 to 5 years.

- Research on the capabilities and requirements for the CBRNE detection systems. These capabilities and requirements must be based on what the end users need to perform detection task and therefore on realistic and detailed detection scenarios. The timeframe for this research is about 2 to 3 years starting subsequent to the finished investigation on existing standards and organisations respectively subsequent to the finished development of realistic detection scenarios.

- Research on the question what testing samples are realistic enough for the development of adequate standards. The timeframe for this research is about 2 years starting subsequent to the finished investigation on existing standards and organisations respectively subsequent to the finished development of realistic detection scenarios.

- Research on what are the most effective and practicable ways of sample collection. The timeframe for this research is about 2 years starting subsequent to the finished investigation on existing standards and organisations respectively subsequent to the finished development of realistic detection scenarios.

- Research on what are the best methods for the testing of CBRNE detection systems. The timeframe for this research is about 2 years starting subsequent to the finished investigation on existing standards and organisations respectively subsequent to the finished development of realistic detection scenarios.

- Development of adequate standards for sample collection, testing samples, testing procedures and protocols, detectors themselves and for the exchange of test results based on results from investigation on existing standards and research on standardisation related issues. The timeframe for this research is about 2 years starting subsequent to the finished research on the capabilities and requirements for the detection systems, the question what testing samples are realistic enough, the most effective and practicable ways of sample collection and the best methods for the testing of CBRNE detection systems.

- Development of realistic and detailed detection scenarios with quantitative data for the geometry, samples, available time, minimum detection limits, detector overload, etc. The timeframe for this development is about 1 to 3 years.

- Development of testing samples for future threat materials including stability analysis and aging of samples (surface and vapour samples)

A24.5 Related issues and difficulties

- Motivation of manufacturer:
  Due to marketing issues or legal aspects like patents there is the problem that the manufacturer could be unwilling to allow to share the testing results.

- Protectionism:
  Because often countries want to protect the companies which produce detectors in their country they may be reserved against EU-wide standards or an EU-standardisation organisation.

- Motivation of state authorities:
  Problems with acceptance of EU Standards (testing done in one country does not imply that any other country will accept the results) can result in the non-acceptance of a certification organisation.

- Political and bureaucratic problems:
  The EU-certification organisation could be unwelcome due to political and bureaucratic issues.

- Use of certificated equipment:
  The demand (by EU- and national law) of using only certificated equipment for CBRNE security purposes by the end-users could be not executable due to legal problems or political willingness.

A24.6 Relation to other Topics

Topic 7 ((inter)national coopertaion): Relation to limited national and international (structures for) cooperation/collaboration and sharing of (classified) information/knowledge/best practices. Similarities are concerning the exchange of information and the cooperation on international level.

Topic 25 (leadership in EU): Relation to Topic in leadership within the EU, such as the lack of an EU coordinating body, for keeping uniform rules for measures and for information. Similarities are concerning the installation of coordination organisations, the willingness for cooperation on EU level and EU-wide standardisation and synchronisation of measures in general.

Topic 3 (focus worst case): Too much focus on worst case scenarios and limited validation of scenarios and threat assessment. The standardisation of testing samples and the detectors themselves should be based on realistic incident scenarios and therefore is dependant on the development of such scenarios for threat assessment.

Topic 13 (standards for infrastructure): The standards for security relevant infrastructure and the standards for the CBRNE detectors themselves should be based on the same realistic incident scenarios.

Topic 10 (stand-off detectors): Effective detection of threatening CBRNE material.

Topic 22 (safe sampling): minimizing of first responder risk during the safe sampling collection.

Annex 25 Increased coordination and unambiguous responsibilities within the EU for CBRNE-crisis management (Topic no. 25)

A25.1 Introduction

There are today a number of organisations, institutions and actors dealing with counter-terrorism and crisis management both belonging and not belonging to the EU. However, there is a need for increased coordination and clarified leadership within the EU in order to improve the work on crisis management and counter-terrorism.

The EU has a structure for crisis management (where crisis also includes incidents caused by nature such as flooding, earthquakes, forest fires etc.). If there is a major crisis the Member States (MS) can cooperate through the Crisis Coordination Arrangements (CCA), which is activated in case of incidents demanding unified EU policies and political cooperation. The CCA concerns how the EU institutions and MSs cooperate on a strategic and high political level in Brussels in case of crisis. For more detailed information see D6.2. The CCA is currently under reviewing process (to be finished by the end of 2011). A reason for why the CCA and its added value was questioned was that it has never been activated (only the Alert Mode has been activated and this happened during the Mumbai attacks in 2008).

If there is a crisis where unified EU policies or political cooperation are not needed but the disaster-stricken country needs help with resources and expertise within the civil protection and rescue area, it falls on the table of the Community Mechanism of Civil Protection. The Community Mechanism for Civil Protection is a platform for resources available within the EU and plays a co-ordinating role by matching offers of assistance to the needs of disaster-stricken countries. The assistance provided to the affected country is coordinated by the Monitoring Information Centre (MIC). Since its establishment in 2001, the Mechanism has been activated more than 100 times. More information is found in D6.2.

Crisis management is a national concern within the EU and is mostly dealt with by the MSs own national crisis management plans or by bilateral agreements. It should be stressed that in case of assistance, e.g. by the Community Mechanism of Civil Protection or by bilateral agreements, it is the receiving country who is the leader of the operation.

A25.2 Description of the objective

The objective is to have the coordination and cooperation between all EU measurements working in a satisfying way for all types of possible CBRNE-crises. The actors within the structures for coordination should have clear responsibilities and the cooperation should include and work in all parts of the security cycle. It should exist both political and operational cooperation on high level as well as on lower level.

A25.3 Products, capabilities and services

- A coordination centre or coordination structure for enhancing the coordination, both operational and political, is needed.
- The coordination needs to be exercised. Exercises of CCA, or future coordination centre, needs to be performed regularly.

- The result of the reviewing process regarding the CCA needs to be considered. The responsibilities and cooperation between CCA (or other future coordination centra) and other agencies within the EU need to be clarified.

It should be noted that the EU has internal structures and bodies for crisis management. Many reviewing processes have taken place after incidents and these have pointed out the problem of coordination [3, 8]. What is needed is a clarification of coordination and leadership for the different institutions/bodies and structures within the union but also increased cooperation with bodies working with crisis management not belonging to the EU.

A25.4 R&D

- For the coordination centre to be a dynamic and fast responding EU structure for cooperation in case of major crises there is a need for fast information exchange between participating personnel. This has been pointed out in exercises of CCA[9]. New technical systems for sending text messages are needed or other corresponding communication tools. During exercises of the CCA there have been problems of delays when sending text messages, this can cause great problems in urgent situations.
- The need for standards regarding leadership and coordination for bilateral agreements between MSs should be evaluated.
- Analyze the optimal solution for EU crisis management. Is the optimal solution the structure that exists or should it be changed?
- The knowledge of every MS's ability to react on a CBRNE-terrorist attack should be used in the development of a coordination plan.
- An inventory of different actors dealing with crisis management not belonging to the EU could be carried out and suggestions of how to coordinate these with EU bodies.

A25.5 Related issues and difficulties

Legal: The standardization of the crisis management should not conflict with national law.

Political: Crisis management is a national concern and it is the disaster-stricken country that is responsible within its own boarders. EU can never take over a political organ or administrations within a MS. If EU should start to get involved in the responsibilities of the disaster-stricken country, the MSs could feel that they are loosing national sovereignty to the EU, which could create conflicts within the society.

Economical: Reorganisation does not have to be costly, but can instead save money. Coordination of what already exists and clarifying the tasks in case of an incident does not necessarily mean increased costs. Some reviewing processes may be needed, but there should be an overlook of existing knowledge and structures before a new institution or body is created.

A25.6 Relation to other Topics

If the coordination, cooperation and leadership between different actors of CBRNE-crisis management in the EU would be enhanced also the following Topics should be bridged:

Topic 1+2 (structural and integral approach): By enhancing the link to other domains and learning about their knowledge the total result of counter-terrorism measurements could improve. The knowledge about who is responsible for what in different domains could benefit the counter-terrorism response since there would be an increased ex-change of knowledge. If the connection between the

phases of the security cycle could be improved this would improve the leader structure at the same time.

Topic 7 ((inter)national cooperation): In order to have a good coordinated leadership in case of an major CBRNE-incident within the EU there is a need for structures for sharing information, best practices and cooperation.

Topic 8 (alert state): If the public should be aware of the different alert states and there would be a greater involvement of the society the structure and leadership in case of an incident would be enhanced.

Topic 9 (communication with population): If the public feels that the communication to them from the authorities is reliable and sufficient the public is willing to trust the authorities and this strengthens the leadership of the authorities.

Topic 12 (responsibilities): The leadership in case of cooperation needs to be unambiguous, the responsibilities of different operators need to be cleared out, this would strengthen the whole coordination and sort out questions regarding leadership.

References

1. Sundholm, K., Defence Counsellor *Interview with Ms. Sundholm working at the Permanent Representation of Sweden to the EU*. 2011.
2. Olsson, S., ed. *Crisis Managment in the EU*. 2009, Springer: Stockholm.
3. Lönberg, S., Deputy Director, *Interview with Ms. Lönberg working at the Crisis Management Coordination Secretariat, Prime Minister's Office (Stockholm)*. 2011: Stockholm.
4. Larsson, P., *EU-CCA och dess konsekvenser för svenska myndigheter*. 2008: Sweden. p. 27.
5. Larsson, P., *EU:s kriskoordineringsarrangemang (EU-CCA) ur ett svenskt perspektiv*. 2006, Swedish Defence Reaserch Agency: Stockholm. p. 56.
6. Barnier, M., *For Europe civil protection force:europe aid*. 2006.
7. *EU Emergency and Crisis Coordination Arrangments in Brussels (CCA) - Challenges for the future*. 2009, Council of the EU: Brussels. p. 6.
8. *Outcome of the workshop on the CCA: Challanges for the future*. 2009, Council of the EU: Brussels. p. 6.
9. *EU Emergency and Crisis Coordination Arrangments in Brussel (CCA) - CCA exercise 2009 (CCAEX09) - Final Evaluation Report*. 2009, Council of the EU: Brussel. p. 12.
10. *The Stockholm Programme - An open and secure Europe serving and protecting the citizens*. 2009, Council of the EU: Brussels. p. 82.
11. *EU Action Plan on Enhancing the Security of Explosives*. 2008, Council of the EU: Brussels. p. 18.
12. *Report and revised Manual on EU emergency and crisis coordination Endorsement*. 2007, Council of the EU: Brussels. p. 72.