
| | |
|---|---|
| **Title :** | **WP4 – System Description** |
| **Number :** | **Deliverable D4.2** |
| **Authors :** | Sebastian Chmel (Fraunhofer INT)<br>Hermann Friedrich (Fraunhofer INT)<br>Veronique Berthou (JRC)<br>Michalis Christou (JRC)<br>Olaf Schumann (Fraunhofer INT)<br>Herbert Wiesinger-Mayr (AIT) |

| | |
|---|---|
| **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), Inames-Tecnalia (ES), Seibersdorf (AT) |

# Summary

This report describes the results of Work Package 4 (WP4) "System Description" of the project DECOTESSC1, a phase 1 demonstration project which was announced in the 2nd call regarding the research topic security within the specific programme "Cooperation" of the of the 7th Framework Programme for Research, Technological Development and Demonstration Activities (2007-2013) by the European Commission.

Within DECOTESSC1 project Work Package 4 deals with "System Description" and refers to the thorough understanding of the system-of-systems' structure. The accomplished objectives of this Work Package are the definition of the field of work, especially the area where the strategic roadmap will lead, thus facilitating the work on the following Work Packages 5, 6 and 7 of the project by creating the appropriate structure and harmonizing the different steps of the analysis. Furthermore the description of the system was performed in such a way that it can be a starting point for data bases, communication, evaluation of current work and for future work by aggregation of subtopics, wise simplifications, concentration to essential points and identification of possibly important topics which have been neglected up to now.

Using a multidimensional approach, a Multidimensional Taxonomy System (MTS) was developed, in order to provide a comprehensive and broad overview to the subject. With the help of a MTS it is possible to define an enormous number of topics with only a limited number of terms. The CBRNE-MTS system was developed following an extensive compilation of definitions and taxonomies given in previous projects or identified by security-related committees and corresponding to a number of quality criteria. The report includes the definitions and explanations of the used terms and their relations in the MTS based on the CBRNE-related projects and reports witch were found most important for the purpose of the present work and which are listed and shortly described. A discussion of possible applications of the CBRNE-MTS is added. Furthermore interfaces of the area of CBRNE threat and countermeasures with other security-related themes were identified and discussed, for example, related to topics such as crime fighting, disaster control, or environmental protection.

# Table of contents

# 1 Introduction

## 1.1 Project background

This report describes the results of Work Package 4 (WP4) "System Description" of the project DECOTESSC1, a phase 1 demonstration project which was announced in the 2nd call regarding the research topic security within the specific programme "Cooperation" of the of the 7th Framework Programme 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. The latter are considered to be incidents that threatens and causes 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. This includes 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 present project a thorough understanding of the system-of-systems' 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. A gap analysis will 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 4: Scope and goal of the report

Work Package 4 "System Description" is one of the first tasks within the project and refers to the thorough understanding of the system-of-systems' structure. The main objectives are:

- The field of work is to be defined, especially the area, where the strategic roadmap will lead. This will facilitate the work on the following Work Packages of the project and help to harmonize the different steps of the analysis.
- The system description is done in a way that it can be a starting point for
  - data bases, communication and evaluation
  - current work and future work by aggregation of subtopics, wise simplifications, concentration to essential points and identification of up to now neglected but possibly important topics

In order to fulfil these purposes the area of CBRNE threats and countermeasures including research and development had to be described with respect to its formal structure and range. This means that it had to be clarified what topics belong to the area and how they can be ordered. Manifold aspects had to be addressed like the CBRNE prevention, response or recovery, furthermore operational, technical, political and social issues and so on.

Using a multidimensional approach, a Multidimensional Taxonomy System (MTS), a comprehensive and broad overview over the subject is provided. With the help of the MTS it is possible to define an enormous number of topics with only a limited number of terms. These are sorted in sets, called dimensions, which are intended to be set up in a way that single topic fields can be defined by an unambiguous and manageable bunch of items - one item out of each dimension. The description

system may serve as a base for proper aggregations, simplifications, for clarification and concentration to essential points. In addition possible interfaces with other security-related themes were identified.

The Work Package 4 (WP4) "System Description" was divided into five tasks:

- Task 4.1: Compilation of definitions and taxonomies given in the framework of previous projects or identified by committees like ESRIF, by public authorities and others.
- Task 4.2: Rearrangement of the compiled concepts and set up of the Multidimensional Taxonomy System (MTS) for all identified subjects.
- Task 4.3: Identification of interfaces with other security-related themes.
- Task 4.4: Discussion of the MTS by the Core Group and the Expert Group
- Task 4.5: Final modification of the MTS and definition of terms.

It is a strategic concept of DECOTESSC1 that the work will be primarily done by the Core Group of consortium partners. In addition, to achieve all the challenging objectives, on top of the efforts of the Core Group, the needs of the various stakeholders (government representatives, local authorities, users with different think-tanks, universities, RTOs and industry (including SMEs)) are considered by direct interaction. In the case of WP4 "System Description" all the Core Group members and about 90 experts out of the expert group in total were involved via email and phone. Finally, a workshop was organized at the Joint Research Centre (JRC) in Ispra, Italy to validate the findings with respect to the system description, to discuss the structuring of the area of CBRNE threats and measures and to agree on definitions. The 33 participants were representatives of the Core Group members and experts from different EU countries, representing end users, local and government authorities, security technique manufactures and so on. During this workshop the results of WP4 were reported and discussed, especially the definitions of relevant terms, the arrangement of the multidimensional taxonomy system and its implications for the further proceeding within DECOTESSC1. Also further possible impact of the MTS was discussed (see chapter 4).

The report is organized in the following way: in chapter 2 the concept of a Multidimensional Taxonomy System (MTS) in general is explained and the criteria for designing such a system are outlined. Subsequently, in chapter 3 the methods that were used to get information and to elaborate the CBRNE-MTS are described and finally the CBRNE-MTS itself is presented together with the definitions and explanations of the used terms. Furthermore, drawbacks and possibilities of the system are discussed in chapter 4. Interfaces with other security-related themes are depicted in chapter 5. An overview on projects and reports with definitions and taxonomies that were taken into account while elaborating the MTS for CBRNE topics and an abbreviations and acronyms list can be found in the appendices A and B.

# 2 Principles of a Multidimensional Taxonomy System

Prevention, detection techniques, crisis management, interoperability, social issues, medical treatment, evacuation plans… a multitude of terms hints to themes that are important for a thorough understanding of the field of CBRNE threat and the system of countermeasures as well as a substantiated planning of future actions or research and development. As outlined in Annex A there are different taxonomies and definitions of terms in use to describe aspects of the overall situation, but no generally accepted taxonomy. The present system description given by the Multidimensional Taxonomy System (MTS) including the definitions and explanations of terms is supposed to clarify the subject of the project, its extension and complexity as well as the various interactions to the scientific community, the industry and the stakeholders. Further possible applications of the MTS are outlined in chapter 4.

The principle of the MTS can be described as follows (cf. [Chm10]): The whole area of interest, in our case comprising the CBRNE threat and countermeasures, is divided into numerous parts, called MTS cells. A MTS cell is defined by several aspects, where each aspect is an element of a set of aspects, here called dimension. The dimensions are defined in a way that a MTS cell can be clearly determined by a bunch of aspects, where exactly one aspect has to be taken out of each dimension. Table 2.1 shows as an example two dimensions, "Threatening Material" and "Target". The dimension "Threatening Material" comprises the aspects "Chemical Agents", "Biological Agents" and so on. The dimension "Target" comprises the aspects "Transportation", "Public Authorities" and so on. The table is arranged in a way that each MTS cell is represented by one table element. This illustrates that the dimensions have to be defined in a way that every combination of aspects, where each aspect is out of a different dimension, determines a reasonable MTS cell. Furthermore, the aspects should have as low overlap as possible to ensure unambiguousness. As an example one MTS cell is marked: It refers to the theme "attack with nuclear material on a transportation system". In this way the complex area of CBRNE threat and countermeasures can be clearly structured – where obviously more than two dimensions should be taken into account (see chapter 3).

| Threatening Material / Target | Chemical Agents | Biological Agents | Radiological Material | Nuclear Material | Explosives |
|---|---|---|---|---|---|
| Transportation | | | | MTS cell | |
| Public Authorities | | | | | |
| Economy | | | | | |
| Basic Services | | | Topic | | |
| Cult Places | | | | | Topic |
| Gathering of People | | | | | |

Table 2.1: Two dimensions of the MTS defining 30 MTS cells (table elements)

The aspects can be further subdivided into sub-aspects, but it has always to be checked if the substructure is covered (or should be covered) by another combination of aspects taking into account

all the dimensions. The number of aspects (or sub-aspects) needed to describe a MTS cell is equal to the number of dimensions. So the restriction of the number of dimensions makes the description system manageable – in spite of the fact that a huge number of MTS cells are covered. Any conceivable topic in the area of CBRNE threat and countermeasures should be describable as (a) a part of a single MTS cell or (b) a part of an aggregation of MTS cells (see as an example the two dashed boxes in Table 2.1).

As a further refinement of a MTS it is thinkable that single MTS cells on their parts can be structured in a multidimensional way, which was not done in the present case for the CBRNE-MTS.

Clearly, the number of MTS cells defined by one aspect out of each dimension might become far too large to be examined in detail, even if the number of aspects and dimensions is manageable. Therefore simplification is needed. This can be done by aggregation and neglecting. MTS cells can be aggregated in the sense that aspects or sub-aspects within each dimension can be aggregated. For example a lot of aspects of the dimension "Geographic Location" could be aggregated under "Europe" or all of them under "World". This can be done in all cases where there are no big differences between the countries concerning the combination of aspects out of the other dimensions. On the other hand, if legal issues are in the focus of interest (dimension "Perspectives" in the CBRNE-MTS, chapter 3.2) it might not be reasonable to consider all countries together without any distinction. Similar considerations hold for other aggregations. In this sense it is meaningful to check all aspects out of all dimensions that define a certain topic before aggregation is performed. Instead of general aggregation of aspects within one dimension a topic-dependent aggregation is in order. In a similar way topic-dependent neglecting of certain dimensions might help to simplify the complexity of the MTS. It should be noted that all the dimensions in the MTS are supposed to be defined in a way that they all are present when a topic is defined, even if no attention is paid to the one or the other dimension. Aggregation and neglecting are not part of the set up of the MTS, but ways of working with the system, albeit a division of aspects into sub-aspects might suggest a certain aggregation.

For a clear definition of a MTS cell it is important that the relations between the aspects out of different dimensions are determined. If for example a MTS cell is defined amongst others by "Research and Development" (dimension "Readiness Level") and "Organisational Means" (dimension "Means"), it is not clear on a first glance if the subject of interest is "organisation of research and development" or "research and development on the field of organisational means". Such ambiguities have to be avoided by defining the relations between aspects out of different dimensions. Related explanations for the CBRNE-MTS can be found in chapter 3.3.

After all that has been said so far, the following quality criteria for a good MTS could be identified:

- Completeness: The field of interest has to be covered as completely as possible by the MTS cells. That means that ideally any arbitrarily chosen topic out of the field of interest can be sorted in one single MTS cell or in an aggregation of single MTS cells.
- Unambiguousness: It should be possible to sort any topic out of the field of interest in an unambiguous way in one single MTS cell or in an aggregation of single MTS cells.
- Minimized aspect and dimension overlap: The aspects or sub-aspects within a dimension should have as low overlap as possible (to ensure that each topic can be attributed with as few aspects and as unambiguously as possible). The same holds for dimensions.
- No constraining aspects in one dimension: The aspects out of one and the same dimension should be real alternatives in the following sense: if a topic is defined with respect to a certain dimension by one aspect out of this dimension it should not be possible to constrain this topic by adding another aspect out of the same dimension (AND) – rather to extend the topic by this (OR). If aspects belong to different categories, which could be applied together to constrain a topic, they should better be distributed to different dimensions.
- Clear Relations: The relations between aspects or sub-aspects out of different dimensions should be defined as clear and unambiguous as possible.

- Self Consistency: Every combination of aspects or sub-aspects, where at least one aspect/sub-aspect is taken from each dimension, should describe a reasonable MTS cell.
- Manageability: The number of dimensions should account for a reasonable structuring but should be kept low enough to allow an effective use of the MTS. The same holds for the number of aspects in each dimension, where the use of the MTS is not restricted so strongly by a big number of aspects as it would be by a big number of dimensions.
- No concentration: The MTS should be constructed in a way that the relevant topics out of the field of interest are disseminated into many different MTS cells. It is not at all necessary to have a homogenous dissemination, but if the concentration of the relevant content on a few MTS cells is to extreme, then the use of the MTS is restricted. In this case a sub-structuring seems advisable.

For a good, comprehensive and useful MTS it is obviously desirable that all the quality criteria are fulfilled. In practice this will not always be possible. How strict a criterion can and has to be fulfilled depends on the situation in which the MTS is to be used. E.g. the completeness-criterion might lead to a high number of dimensions and aspects where on the other hand due to the manageability-criterion the number of dimensions should be kept low. It depends on the specific use of the MTS how many dimension and aspects are considered as "manageable". In case of need aspects could be summarized and details could be taken into account as sub-aspects. Summarizing of dimensions might seem possible, too, but might also lead to inconsistencies and violate the no-constraining-aspects-criterion in a way that the MTS cannot be used any more reasonably. In general, it should not cause logical problems, if the last three criteria are not fulfilled (Self Consistency, Manageability and No concentration), and therefore they might be considered as less important.

One might add familiarity as a further quality criterion: the persons who are supposed to use a MTS might prefer to find the terms they are familiar with in the system, as dimensions, aspects or sub-aspects. This might cause a higher acceptance rate of the MTS by the stakeholders. However, it will not always be possible to design a MTS with familiar terms which fulfils all above quality criteria in a satisfactory way. Furthermore, even in professional circles the meaning of widely used words is not uniformly defined and different people do understand different things under the same word. In addition, the necessity of clear relations between aspects out of different dimensions might lead to a specific use of certain terms within a MTS, which might lead to misunderstandings. The general rule used within the MTS is: familiar terms are used, unless misunderstandings must be feared. If this holds then it might be valuable to integrate the familiar terms in another way: They can be taken into account in the explanation of the aspects and dimensions or, e.g. in the user interface in case the MTS will be used to structure a database.

The Multidimensional Taxonomy System (MTS) on the area of CBRNE counter measures is a tool to unravel the complexity of the CBRNE counterterrorism system-of-systems. It is also a base for dealing with the complexity through proper aggregations, simplifications, through clarification and concentration to essential points. In this sense it is a tool for the reduction of complexity in order to select those combinations of aspects which seem to be most harmful and should be addressed with high priority.

# 3 CBRNE-Multidimensional Taxonomy System (CBRNE-MTS)

## 3.1 Description of elaboration methods and difficulties

The design of the MTS for CBRNE-topics has been achieved in consideration of definitions and taxonomies given in the framework of previous projects like the PASR projects STACCATO and IMPACT or identified by committees like ESRIF and similar groups. Previous concepts were compiled, checked, complemented, continued or rearranged, where necessary, to add up to a complete picture. At the same time the general criteria for designing a MTS had to be taken into account. The process was accompanied by many discussions with experts via written or oral exchange, especially at the first DECOTESSC1-workshop in July 2010 at JRC in Ispra, Italy (see chapter 1 and [Wie10]).

The compilation of definitions and taxonomies given in the framework of previous projects, identified by relevant committees or used by well recognized authorities was done via literature research and by consulting experts. The documents and sources of information found most important for the purpose of WP4 are listed and shortly described in Annex A.

In parallel the MTS was elaborated according to the ideas and rules explained in chapter 2. The main objective was to describe the whole system of CBRNE threat and countermeasures by a manageable number of terms without ignoring the complexity of the area. Therefore the multidimensional structure was chosen, where each dimension contains a certain set of aspects. These are to be combined mutually to account for the multidimensional volume of the total system (see chapter 3.2).

In order to find most suitable and widely accepted terms the structuring and all the definitions were checked with the literature and discussed with experts. Referring to the quality criteria explained in chapter 2 leading questions for developing the MTS were:

- What dimensions are necessary to define the field of work appropriately?
- How should aspects or sub-aspects be defined within the dimensions?
- How can the relation of aspects out of different dimensions to each other be defined in an unambiguous manner?
- Should a set of the proposed aspects better be aggregated and considered as an aspect with sub-aspects?
- How could the overlap between aspects or sub-aspects within a dimension be kept to a minimum?
- Can a topic, which is defined with respect to a certain dimension by one aspect, be constrained by adding another aspect out of the same dimension? Can this be avoided by distributing the aspects to different dimensions?
- What are the best terms for the dimensions and aspects so that the intended meaning is descript in the clearest way?
- What alternative terms are conceivable and should be taken into account for the explanation of dimensions and aspects?
- Is it possible to simplify the MTS by elimination of a dimension and dispersing their aspects to other dimensions?
- Can aspects or sub-aspects be removed and be handled as a topic, which is defined by a combination of aspects or sub-aspects, where one aspect (or an aggregation) has to be taken out of each dimension?
- Is the MTS self-consistent, i.e. does the combination of one aspect/sub-aspect from each dimension make sense?
- Are all topics and terms that are relevant for our project covered by the MTS?
- What are “other security related themes” that do not belong to the area of CBRNE in general, but should be noted (Work package Task 4.3)?

Questions like these were supposed to assure the MTS completeness and consistence and should help to develop a CBRNE-MTS that fulfils the quality criteria.

To illustrate the way - and also the difficulties - of finding a proper taxonomy system, especially the way of finding aspect definitions for a given dimension, Table 3.1 shows a short overview of the situation for the theme “security chain” - also called security cycle to indicate that the activities start from the beginning, when an incident has occurred and all the chain links have been run through. The table does not demonstrate the use of the terms within the MTS, the intention is in fact to show the different taxonomies used in different sources of information concerning the security chain. For a better overview of the varying structuring of the chain and the different terms used for the classification of its parts, similar expressions are stacked in the same columns. Terms which are linked with a diagonal slash are as well linked in this way in the used documents and therefore are intended to be one single part of the security chain, which means for the table that they are put in the same table element. The arrows express that one of the terms in the table element is used as a separated part of the security chain in some of the other documents. In the two left columns the name of the source and the position in the related document (e.g. page number) is mentioned. This is necessary because even in one and the same document respectively source of information the structuring of the security chain is not always described consistently. The Table 3.1 displays a non-uniform picture. Moreover the meaning and comprehension of the terms for the chain links themselves are not standardized and uniform among experts. Obviously it is difficult to create definitions and to assign the terms to the security chain in a way that every expert is satisfied. In the present context one had to accept the additional challenge to define aspects and dimensions which fulfill the requirements given by the principle of the MTS. The finally adopted definitions for aspects (see chapter 3.3) are inter alia from the documents [CRE10], [EOS09], [ESR09], [OEC03], [CRS10], [PSC05].

| Source | | Aspects | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ESRIF-Final Report | Page 18 | | Prevention | Protection | | Preparing | Response | | Recovery |
| | Page 135 text | Threat assessment | Prevention | | Preparedness | | Response | Mitigation | Recovery |
| | Page 135 figure | Threat assessment | Prevention | | | | Response | Mitigation | Recovery |
| | Page 85 | | Prevention | Protection | | | Reaction/ Mitigation | | |
| EOS-White Paper + ESRIF-Final Report | Page 27 + Page 58 figure | Risk assessment | Prevention/ Mitigation | | Preparedness | | Response | | Restoration/ Reconstruction/ Recovery |
| EOS-White Paper | Page 6/7 | | Prevention | | | Preparation | Response | Mitigation | Recovery |
| OECD. Guiding Principles: Chemical Accident | Page 10 | | Prevention | | Preparedness/ Mitigation | | Response | | Follow-up |
| | Page 15 | | Prevention | | Preparedness | | Response/ Recovery | | |
| CRESCENDO-Workshop | A. Penttinen | | Prevention/ Preparedness | | | | Crisis management | | Consequence management |
| | O. Nederlof | | Prevention | | | Prepare | Respond | | Aftercare |
| | L. Olmendo | Situation | Prevention/ Preparation | | | | Crisis management | | Decontamination/ Restoration |
| TNO Project Terrorisk | | Proaction | Prevention | | Preparedness | | Response | | Aftercare |
| Public Safety Canada – CBRN Strategy | Page 4 | | Prevention/ Mitigation | | Preparedness | | Response | | Recovery |

Table 3.1: Short overview of the situation for the theme “security chain”.

Topics and security-related themes that do not belong directly to the area of CBRNE attacks but are linked in one way or the other were identified. They are not taken into account for the setup of the MTS, but the interfaces with the are of CBRNE threat and counter measures were discussed and are described in detail in chapter 5.

Due to the large number of possible combinations of aspects a complete review if all topic fields, defined by a possible combination of aspects (called MTS cells, see chapter 2) make sense is next to impossible. Thus logic errors might still persist in the CBRNE-MTS, despite the efforts to eliminate such faults. Additionally, while for some dimensions it is quite easy to cover the whole field, e.g. "Geographic Location" or "Threatening Material", for others the completeness requirement imposes a serious challenge. This is most obvious for the "Target" dimension, where terrorists might choose preferably those targets, which were not thought of.

For some dimensions, two or more sets of aspects or sub-aspects are conceivable for the description of the dimension, e.g. the aspect "Transportation" of the dimension "Target" might be subdivided by the mode of transportation (Road, Rail, Air, …) or the transported object (mass transport, passenger transport). The intended use of the CBRNE-MTS might demand different choices; depending of the scope where it is used, different aggregations could be made.

### 3.2 The CBRNE Multidimensional Taxonomy System

In the following the design of the CBRNE-MTS is outlined. As already mentioned in chapter 2 the two dimensions shown in Table 2.1 are obviously not sufficient to define a MTS cell exactly enough for the present purpose. Other items, e.g. referring more specific to the kind of target (airport, public places etc.) or the countries of interest have to be added. In total eight dimensions were considered to be reasonable to determine an MTS cell in the present context: "Level of Action", "Readiness Level", "Security Chain", "Threatening Material", "Target", "Means", "Perspectives" and "Geographic Location". The terms are defined and described in detail in chapter 3.3. An overview of all dimensions and their aspects is presented below. Sub-sub-aspects are not included in the overview but can be found in chapter 3.3. It is also possible for users to add further sub-sub-aspects to the CBRNE-MTS.

The ordering of the dimensions as given in this subchapter does not indicate importance. In a next step, during the application of the CBRNE-MTS, the dimensions can be handled as completely equal (e.g. in a database) or they can be ordered into different levels (e.g. to structure a report). The work approach of DECOTESSC1 is oriented in the aspect "Analysis" of the dimension "Level of Action", i.e. the work packages of DECOTESSC1 coincide more or less with the sub-aspects of this aspect: "Status quo Analysis" and "Trend Analysis" are subjects of work package 6 (WP6), the "Ideal Situation" is subject of work package 5 (WP5) and so on. Thus, the aspect "Analysis" of the dimension "Level of Action" is the main level for the present project. The DECOTESSC1 work package reports on their part will be structured in the first layer according to the "Security Chain": "Threat", "Prevention" and so on. This was decided in the above mentioned workshop (see introduction and chapter 3.1) to stress the system-of-systems character of DECOTESSC1. The other dimensions can serve as guidelines for further structuring.

It should be kept in mind that a single MTS cell is defined by a bunch of aspects or sub-aspects where *exactly* one aspect or sub-aspect has to be taken out of each dimension. An aggregation of MTS cells can be defined in a similar way, where *at least* one aspect or sub-aspect has to be taken out of each dimension. An example for a MTS cell defined by aspects out of eight dimensions is: Status quo analysis (1st aspect, out of dimension "Level of Action") of research and development (2nd aspect, out of dimension "Readiness level") in France (3rd, out of "Geographic Location") concerning the feasibility (4th) of prevention (5th) of a chemical attack (6th) at a public place (7th) with respect to

technology-based techniques, i.e. measurement techniques, communication devices etc. (8th)[1]. This definition by eight items clarifies for example that within this MTS cell the development of technical equipment is considered, not the actual installed equipment. On the other hand, a glance on other aspects may indicate what themes might deserve attention, too: e.g. not just the feasibility of the equipment under development but also political and legal questions may play a role – another MTS cell, defined by changing the aspect "Feasibility" to "Legal Issues".

It is intended that any conceivable topic concerning CBRNE threat and countermeasures is describable as a part (non-strict subset) of a single MTS cell or a part of an aggregation of MTS cells. The related MTS cells have to be defined by at least one aspect or sub-aspect in each dimension. It should be noted that it is not in the intention of the MTS to address single aspects or the dimensions itself as topics.

| **DIMENSION Level of Action** | |
|---|---|
| Analysis (of aspects out of "Readiness Level") | |
| Status quo Analysis | |
| Trend Analysis | |
| Ideal Situation Analysis | |
| Real-ideal-situation-gap Analysis | |
| Strategy (recommendations, requirements…) | |
| Implementation (of aspects out of "Readiness Level") | |

| **DIMENSION Readiness Level (regarding Security Chain activities)** | |
|---|---|
| Research and Development (including experiments, testing, assessment) | |
| Actual designated or executed measures | |
| Guarantee of Operational Capability (maintenance) | |
| Training and Education | |

| **DIMENSION Security Chain** | |
|---|---|
| Threat | |
| Prevention | |
| Preparedness | |
| Response | |
| Recovery | |

| **DIMENSION Means (for Security Chain activities)** | |
|---|---|
| Organisational Means | |
| Technology-based Techniques | |
| Methodological Techniques | |

[1] But, if you choose an aspect from only three dimensions, you implicitly aggregates all other dimensions. For example: Status quo analysis (1st aspect, out of dimension "Level of Action") of research and development (2nd aspect, out of dimension "Readiness level") in France (3rd, out of "Geographic Location") concerning a chemical attack (6th). This topic covers all aspects of the dimensions perspectives, means, target and security chain.

| **DIMENSION Threatening Material** | |
|---|---|
| C | |
| B | |
| R | |
| N | |
| E | |

| **DIMENSION Target** | |
|---|---|
| Transportation | |
| Road | |
| Rail | |
| Subway | |
| Air | |
| Maritime | |
| Public authorities | |
| Political Institutions | |
| Security/Safety Institutions | |
| Judiciary | |
| Military Facilities and Stuff | |
| Gathering of people | |
| Events | |
| Public Places | |
| Economy | |
| Industry | |
| Finance | |
| Basic Services (excluding transportation) | |
| Distribution Networks | |
| Water | |
| Energy Carrier (oil, gas, electricity etc., including pipelines) | |
| Agriculture and Food | |
| Healthcare | |
| ICT and Internet services | |
| Cult Places | |

| **DIMENSION Perspectives (of aspects out of "Readiness Level")** | |
|---|---|
| Feasibility | |
| Political Issues | |
| Social and Psychological Issues | |
| Legal Issues | |
| Economical Issues | |
| Health Issues | |
| Environmental Issues | |

| **DIMENSION Geographic Location (of Security Chain activities)** | |
|---|---|
| Europe | |
| EU | |

| | |
|---|---|
| … | |
| Non EU | |
| Asia | |
| … | |
| America | |
| USA | |
| … | |
| Africa | |
| … | |

### 3.3 Definitions and explanations of terms

In the present chapter all the terms used in the MTS are defined and explained. Also synonyms and similar expressions are given for better orientation. For the correct understanding of the definitions it is important to keep in mind the structure of the MTS:
1. Every aspect or sub-aspect provides only an incomplete description of a MTS cell if it is not combined with at least one aspect or sub-aspect out of each of the other dimensions. Only in few cases such combinations are noted explicitly.
2. Furthermore the definitions refer to the aspects and dimensions as such, including the relations to other aspects and dimensions, and not to the general meaning of the terms. For a proper understanding and use of the CBRNE-MTS it is important to be aware of the relations.

#### 3.3.1 Definition and explanation of the MTS dimensions and aspects

Dimension: "Level of Action"

In this dimension two aspects are collocated, Analysis and Implementation, which describe two levels of action with respect to the area of CBRNE threat and countermeasures:

Implementation

This aspect refers to the realization of the objects that are given by an aspect out of the dimension "Readiness Level". This means the realization of research and development, the realization of actual measures or the realization of training and education – where the realized things are further specified by aspects out of all the other dimensions. The addressed MTS-cell could be for example the implementation/execution (1st aspect) of research and development (2nd) on organizational means (3rd) for response (4th) in case of an attack with chemical agents (5th) at Public Places (6th) in Italy (7th) with respect to legal issues (8th) of this research and development. Or the addressed MTS-cell could be the implementation (1st) of the actual designated or executed measures (2nd) concerning organizational means (3rd) for … with respect to the legal issues (8th) of these measures. This MTS-cell covers amongst others the question what laws are regulating the organisation of response measures in the considered special case.

Analysis

This aspect refers to the action of analyzing, where the direct topic of the analysis in question is given by an aspect out of the dimension "Readiness Level", which in turn is further specified by aspects out of all the other dimensions. The subjects of the analysis in question, the analysts, are experts and specialists who have to be specified from case to case.

The aspect is subdivided into sub-aspects that refer to the scope of analysis, which might range from a mere description of the status quo to a vision about an ideal situation to concrete recommendations and strategy concepts.

The following sub-aspects have been defined:

*Status quo Analysis*

This sub-aspect means: The scope of the analysis is the status quo of the object, which is given by an aspect out of the dimension "Readiness Level", which in turn is further specified by aspects out of all the other dimensions.

*Trend Analysis*

This sub-aspect means: The scope of the analysis is to identify trends, to give an overview on planned or ongoing measures or research projects etc. – depending on the aspects chosen out of the other dimensions.

*Ideal Situation Analysis*

This sub-aspect means: The scope of the analysis is the description of the ideal situation. For example in combination with the aspects "Actual designated or executed measures" and "Response" out of the dimensions "Readiness Level" and "Security Chain" it refers to requirements for perfect response in case of a CBRNE incident.

*Real-ideal-situation-gap Analysis*

This sub-aspect means: The scope of the analysis is the identification of gaps between the reality and the ideal situation where the further details are depending on the aspects chosen out of the other dimensions. It includes in general the ranking of the identified gaps between the reality and the ideal situation.

*Strategy*

This sub-aspect means: The scope of the analysis is to develop a strategy how gaps between reality and ideal state can be reduced. Again, as explained for the other sub-aspects, it might be a strategy for research and development, for the actual measures, for maintenance or for training – depending on what is chosen in the dimension "readiness Level". This includes recommendations, identification of key players and so on.

Dimension: "Readiness Level"

In this dimension aspects are collocated that refer to the question how directly the centre of interest is object of the analysis or implementation. In the CBRNE-MTS the centre of interest are the activities, which are given by an aspect out of the dimension "Security Chain" and which are further specified by aspects out of all other dimensions (except the dimension "Level of Action", which specifies the analysis and implementation and not the activities as explained above). These activities can be more indirectly the object of analysis in the sense that e.g. the direct object is the related research and development or related training.

Within this dimension the following aspects have been defined:

Research and Development

This aspect means: The object of the implementation or analysis (see dimension "Level of Action") is research and development itself, the systematic activity covering all kinds of investigation and assessment, even so the whole innovation cycle from basic research to introduction of new products or realisation of measures including experiments and testing. Actors in these activities are researchers, specialists and experts. The objects of the research and development in their part are to be defined by an aspect out of the dimension "Security Chain" and further specified by aspects out of all other dimensions (except the dimension "Level of Action"). Sub-aspects may be the different branches of research.

Actual designated or executed measures

This aspect means that the object of the implementation or analysis (see dimension "Level of Action") is the actual ability and measures of the actors, where the latter are given by an aspect out of the dimension "Security Chain". The abilities are proved due to activities themselves or can be estimated from the fact that the needed means and qualified actors – be it terrorists or state authorities – exist. The aspect "Actual designated or executed measures" refers directly to the execution, including the regarded means, methods and technology (see dimension "Means").

Guarantee of Operational Capability

This aspect refers to activities aiming at the guarantee of the operability of the realised or designated measures which are given by an aspect out of the dimension "Security Chain" and which are further specified by aspects out of all other dimensions except the dimension "Level of Action". It covers controlling, implementation and maintenance as well as repair and replacement.

Training and Education

This aspect refers to activities aiming at the generation respectively improvement of the state of knowledge and the performance of people for the purpose of securing the proper use of means, measures and technologies. Subjects (trainers) and objects (trained people and purpose of training) of this aspect are given by an aspect out of the dimension "Security Chain" – this means they might be terrorists as well as state authorities. "Training and Education" is indirectly further specified by aspects out of all other dimensions (except the dimension "Level of Action"), It covers preparedness in the sense that it ensures the qualification of the actors in case of an incident.

Dimension: "Security Chain"

In this dimension aspects are collocated which refer to specific activities by different actors in conjunction with a CBRNE incident. They range from preparing measures by terrorists as well as prevention measures by state authorities until restoring measures in the aftermath. These activities are further specified by aspects out of all other dimensions including possible impact areas (dimension "Perspectives"). The only exception is the dimension "Level of Action", which specifies the analysis and not the activities. In some documents where these kinds of activities are described the term "cycle" is used instead of "chain" to emphasize that after recovery new threats will arise.

Within this dimension the following aspects have been defined, where the arrangement of the aspects is inter alia from the documents [CRE10], [EOS09], [ESR09], [OEC03], [CRS10], [PSC05], [IPS05] and the definition of the aspects inter alia from the documents [CRE10], [EOS09]:

Threat

This aspect covers the activities of the terrorists to prepare and execute an attack. Together with aspects out of the dimension "Threatening Material", "Target" and "Means" a threat scenario can be defined in more detail. Subject of these activities is the terrorist. The "threat analysis" or assessment in fact is given by the following MTS-cells: Status quo analysis or trend analysis (1st aspect) of the actual designated or executed measures (2nd) to generate a threat (3rd), where the aspects out of the other dimension have to be specified or are simply aggregated. On the other hand also an analysis of the threat analysis itself can be addressed with the help of the CBRNE-MTS: Status quo analysis (1st) of research (2nd) on the threat (3rd), where again the aspects out of the other dimension have to be specified.

Prevention

This aspect includes all measures aimed at prevention from the occurrence of an incident by looking at preventing that someone can and will carry out an attack. Subject of these activities are among others state authorities and security institutions. This can be achieved e.g. through regulations, local ordinances, legislative measures, intelligence or deterrence measures (see dimension "Means" and "Perspectives").

Preparedness

This aspect includes all measures to prevent an actor of executing an attack and create awareness and resilience in case something happens. Preparedness covers measures that are aimed at reduction of the impact of an incident respectively protection from the incident itself. Subject of these activities are among others state authorities and security institutions. Preparedness is mainly showing the attacker: 'it is useless to attack, because we are protected, physically as well as mentally'. In advance accomplished Preparedness measures should reduce the risk to life and property in the pre and post-disaster environments. This can be achieved e.g. through regulations, local ordinances, legislative measures (see aspect "Organizational Means" in the dimension "Means" or "Legal Issues" in the dimension "Perspectives"), CBRNE intelligence and building practices as well as by means of mitigation projects like engineering and other physical protective measures that reduce or eliminate risk from hazards and their effects (see aspect "Technology-based Techniques" in the dimension "Means")..It should be noted that in some documents (e.g. in ESRIF final report [ESR09], page 58) also general preparing activities like training and education of response are collocated under the term "preparedness" – which is not done in the present CBRNE-MTS, where we follow the definition of J. Wevers et al, Terrorisk (to be published). Rather training with respects to every phase is covered by the aspect "Training and education" in the dimension "Readiness Level".

Response

"Response" includes the sum of decisions and measures taken during and immediately after the incident, including mitigating the impact of the incident after its occurrence. Subject of these activities are first responders, state authorities and security institutions.

"Response" relates to the emergency operation activities conducted during the impact of a disaster and the short-term aftermath. The main emphasis is on the saving of human life, including protection

of first responders, but it also encompasses the protection of assets, the supply of vital goods and services, protection of the environment and reduction of impacts in public.

Recovery

"Recovery" is the process by which communities return to a normal level of functioning. Subject of these activities are state authorities and security institutions.

"Recovery" refers to the coordinated process of supporting emergency or disaster-affected communities in reconstruction of the physical infrastructure and restoration of emotional, social, economic and physical well-being. In the initial stages of this process the emphasis is on the restoration of basic services and facilities and on decontamination of the impact area, depending on the specific situation (see dimension "Target"). However, in the longer term, the impact of reconstruction is crucial; agencies involved at this stage aim to ensure that vulnerabilities are reduced without simply reproducing the existing risk elsewhere.

Dimension: "Means"

In this dimension aspects are collocated that refer to the means that are used to realize the activities, which are given by an aspect out of the dimension "Security Chain" and which are further specified by aspects out of all other dimensions except the dimension "Level of Action". The actor who uses the means is therefore determined by the aspect chosen in the dimension "Security Chain". It might be a terrorist ("Threat") or a state authority ("Prevention", "Preparedness", "Response" or "Recovery".).

Within this dimension the following aspects have been defined inter alia inspired by mostly of all the documents from the literature list:

Organisational Means

This aspect refers to the organisation of the activities or measures as specified by an aspect out of the dimension "Security Chain" and as further specified by aspects out of all other dimensions. It includes the distribution of competencies, relations of state entities (or terror groups), communication structures, personal management, reflection on "lessons learned" and so on.

Technology-based Techniques

This aspect refers to technology-based techniques that are applied during the activities or measures as specified by an aspect out of the dimension "Security Chain" and as further specified by aspects out of all other dimensions.

The MTS cells defined with the help of this aspect include detection, identification and protection techniques, surveillance instruments (monitoring), decontamination, neutralisation and medical treatment, depending on the aspect chosen in the dimension "Security Chain". If the aspect "Threat" was chosen there, then also improvised explosive or nuclear devices are covered (depending on the aspect in the dimension "Threatening Material") as well as vectors (agent distribution systems / means). If the aspects "Prevention", "Preparedness", "Response" or "Recovery" are chosen, then the techniques in question include detection or surveillance techniques, furthermore techniques to preserve or restore the integrity of people and goods (including e.g. the use of dispersion models).

Methodological Techniques

This aspect refers to methodological techniques that are applied during the activities or measures as specified by an aspect out of the dimension "Security Chain" and as further specified by aspects out of all other dimensions. In case the aspect "Response" was chosen in the dimension "Security Chain" e.g. contingency plans are taken into account.

Dimension: "Threatening Material"

In this dimension aspects are collocated that refer to the sort of material that can be in the focus of the activities, which are given by an aspect out of the dimension "Security chain" and are further specified by aspects out of all other dimensions (except the dimension "Level of Action"). The aspects define the material, which is supposed to be used and to cause the main hurtful effect in case of the considered attack.

Within this dimension the following aspects have been defined, where the definitions are inter alia from the documents [CRE10], [IPS05] and [JOP08]:

C (chemical)

Chemical agents are those that are effective because of their toxicity.

If chemical agents are used as propellants, explosives, incendiaries or obscurants they are not considered as a chemical incident, even though the chemicals in them may also have toxic effects. Only incidents whose main goal is to have toxic effects are considered chemical incidents. The chemical action of chemical agents can cause death, permanent harm or temporary incapacity.

B (biological)

Biological agents are means that cause casualties in man and animals or lead to damage to plants or materiel by infecting life forms either with disease-causing microorganisms, replicative entities (including viruses, spores, infectious nucleic acids and prions), naturally produced poisonous substances (bio-toxins) or other harmful biological forms.

The triggered disease may be the result of the interaction between the biological agent, the host and the environment. One of their chief characteristic is their ability to spread disease through humans, animals and agriculture. Microorganisms are living organisms, such as a bacterium, archaea, yeast, fungus or protozoans. They may exist as part of the normal flora (e.g. oral cavity, skin, intestinal tract) without producing disease. Due to unbalance of the interrelationship between the microorganisms or also between the microorganisms and the host resistance, individual forms of microorganisms may overgrow and trigger disease in the host's tissues. Viruses are submicroscopic infective agents that are autocatalytic protein complexes containing genetic information comparable to genes, which allow growth and multiplication only in living cells by using the host's replication mechanisms. Thus they cause various important diseases in man, animals, or plants. Bio-toxins are poisonous substances that are produced naturally (by bacteria, plants, fungi, snakes, insects, and other living organisms) but may also be produced synthetically. They differ from chemical agents by their biological origin that implies biodiversity.

R (radiological)

R materials cover radiological devices resulting in nuclear radiation caused by, artificial dispersion of radioactive material or irradiation.

Radiological materials cause physiological damage through the ionizing effects of neutron, gamma, beta, and/or alpha radiation. Radiological hazards include any electromagnetic or particulate radiation capable of producing ions so as to cause damage, injury, or destruction.

N (nuclear)

N materials cover nuclear weapons and Improvised Nuclear Devises (IND) (fissile materials) resulting in nuclear radiation caused by fallout or irradiation.

A nuclear weapon or IND refers to a complete assembly, in its intended ultimate configuration which, upon completion of its arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and energy release.

E (explosive)

Explosive is a chemical substance or mixture of substances intended to produce an explosive effect in civil applications, military or terrorist applications.

Explosives are categorized as high-explosives (HE) or low-order explosives (LE). HE (include e.g. trinitrotoluene, nitroglycerin, dynamite or ammonium nitrate fuel oil) produce a defining supersonic overpressurization shock wave. LE (e.g., pipe bombs, gunpowder, or aircraft improvised as guided missiles) create a subsonic explosion and lack HEs overpressurization wave. Explosive and incendiary (fire) bombs can be further characterized based on their source. “Manufactured” implies standard military-issued, mass produced, and quality-tested weapons. “Improvised” describes weapons produced in small quantities, or use of a device outside its intended purpose. Manufactured (military) explosive weapons are exclusively HE-based. HE and LE, respectively manufactured and improvised explosion devices cause different injury patterns. Conventional explosives can generate casualties in several ways depending on the type of explosion, secondary effects of the explosion (e.g., building collapse, fire), and the surrounding environment of the explosion (e.g., confined spaces, availability of debris or materials to generate an expanding area of potential injuries).

Dimension: “Target”

In this dimension aspects are collocated that refer to the kind of target that can be in the focus of the activities, which are given by an aspect out of the dimension “Security Chain” and which are further specified by aspects out of all other dimensions except the dimension “Level of Action”. The aspects include objects, locations, facilities or people against which a terroristic act can be directed.

Within this dimension the following aspects have been defined which are inter alia inspired by the documents [PSC09], [BMI05], [BMI09], [ESR09], [CEC04] and [IPS05]:

Transportation

There are five main kinds of transportation sectors for the transportation of goods and passengers (mass transportation), which are road traffic, railway service, subway, air transportation and maritime traffic. “Transportation” includes the means of transportation like vehicles, trains, subway cars, planes

and ships, as well as transportation related infrastructure like roads, rails, tunnels, train stations, airport or harbours. "Transportation" includes also the traffic control systems like e.g. Air Traffic Control for air transportation.

Sub-aspects are: "Road", "Rail", "Subway", "Air" and "Maritime"
Sub-sub-aspects for all sub-aspects are: "Infrastructure", "Traffic" and "Traffic Control"

Public Authorities

Under "Public Authorities" are combined all legislative, governmental or administrative institutions and facilities, the judiciary, security and safety institutions like the law enforcement agencies including penal institutions or fire service, and the Military facilities along with military stuff.

Sub-aspects are: "Political Institutions", "Security/Safety Institutions", "Judiciary" and "Military Facilities and Stuff".

Gathering of People

Gathering of people occur in case of sports, cultural (concerts, festivals) or political (demonstrations) events. It includes also crowds of people at public places like pedestrian zones or shopping malls. However all transportation-related areas are excluded.

Sub-aspects are: "Events" and "Public Places".

Economy

"Economy" incorporates the industrial production of raw materials and goods (inclusive production, storage and handling of dangerous goods, e.g. in the chemical or nuclear industry), provision of services to business and customers (excluding services falling under the definition of "Basic Services" and "Transportation") and the financial sector including banking and stock markets.

Sub-aspects are: "Industry" and "Finance"

Basic Services

"Basic Services" cover all infrastructure installations which are crucial for the life and well-being of citizens except all other aspects of the dimension "Target". "Basic Services" include "Distribution Networks" (inclusive related facilities) for water and energy carriers like gas, oil (including pipelines) or electricity, "Agriculture" inclusive food supply, the whole healthcare-related sector and "ICT and Internet Services" systems (Information and Communication Technology).

Sub-aspects are: "Distribution Networks", "Agriculture and Food", "Healthcare" and "ICT and Internet Services"

Cult Places

"Cult Places" cover all locations and facilities inclusive related personnel with symbolic significance like monuments, landmarks, religious (churches) or cultural (museums) facilities and locations as well as cultural assets.

Dimension: "Perspectives"

In this dimension aspects are collocated that refer to the considered impact of the subject of interest. The latter is given by an aspect out of the dimension "Readiness Level" and further specified by aspects out of all dimensions (except the dimension "Level of Action").

Within this dimension the following aspects have been defined which are inter alia inspired by the document [CEC06]:

Feasibility

Regard of the possibility of the realisation of the subject of interest without attending to any influence on political, social, psychological, economical, health and legal issues.

The question of interest is merely: Can it technically be done?

Political Issues

Issues concerning general political conditions and political impact of the subject of interest.

This may cover inter-state regulations and agreements like for border-control or lobbying activities by different government agencies of non-government-organizations, for example.

Social and Psychological Issues

Issues concerning general social conditions and social or psychological impact of the subject of interest.

Depending on the aspects out of the dimension "security chain" topics like the trade-off between security vs. freedom and privacy, the refusal of a technique from the majority of the society and religious, ethic or psychological aspects are addressed.

Economical Issues

Issues concerning general economical conditions and economical impact of the subject of interest.

Here all topics that deal with the impact on the economy are addressed, like the total cost of ownership of a technique under investigation or the implications for the overall economical system of a country or region.

Legal Issues

Issues concerning general legal conditions and legal impact of the subject of interest.

This may cover incompatible laws for the achievement of a specified goal or Intellectual property rights, for example.

Health Issues

Issues concerning general health conditions and health impact of the subject of interest.

Environmental Issues

Issues concerning the general environmental conditions and environmental impact of the subject of interest.

Dimension: "Geographic Location"

In this dimension aspects are collocated that refer to the geographic location where the activities, which are defined by an aspect out of the dimension "Security Chain", take place. The proposed division into continents and countries suggests itself and is self explaining. In this dimension aggregation might be especially useful during application of the MTS - depending on the MTS cells, defined by all the aspects out of the other dimensions, of course.

Within this dimension the following aspects and sub-aspects have been defined:

Europe
- EU-countries
  - 1 Austria
  - 2 Belgium
  - 3 Bulgaria
  - 4 Cyprus
  - 5 Czech Republic
  - 6 Denmark
  - 7 Estonia
  - 8 Finland
  - 9 France
  - 10 Germany
  - 11 Greece
  - 12 Hungary
  - 13 Ireland
  - 14 Italy
  - 15 Latvia
  - 16 Lithuania
  - 17 Luxembourg
  - 18 Malta
  - 19 Netherlands
  - 20 Poland
  - 21 Portugal
  - 22 Romania
  - 23 Slovakia
  - 24 Slovenia
  - 25 Spain
  - 26 Sweden
  - 27 United Kingdom
- Non-EU-countries
  - …

Asia
- …

America
- …

Africa

…

Australia

…

### 3.3.2 Related terms that are not CBRNE-MTS aspects or dimensions

The following list shows some terms of interest which are not used as labels for aspects or dimensions of the CBRNE-MTS, but nevertheless indicate important topics and are implicitly present in the CBRNE-MTS:

Mitigation
Risk Assessment
Deterrence
Crisis Management
Critical Infrastructure
Vulnerability
Human Factor
Multiple Attacks
Security Cycle
Threat Cycle
Disaster Life Cycle
Protection
Prepare
Preparation
Reaction
Post-Incident Intervention
Emergency Management
Aftercare
Follow-up
Consequence Management

In the cases where the listed terms define topics, that are part of one or more MTS-cells (i.e. they are covered by a combination or aggregation of aspects of the different dimensions, see chapter 3.2), it is clear that they cannot represent simply a single aspect or a dimension. In other cases the terms are not used because they are just similar to the ones used for aspects or dimensions in the CBRNE-MTS and a choice had to be made for the one or the other reason. Furthermore unambiguousness and avoiding of misunderstanding were considered as important for a smoothly use of the CBRNE-MTS. For example the term “Critical Infrastructure” is not uniformly used by experts with respect to its coverage: A general definition of Critical Infrastructure e.g. from [CEC04] is: Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments. But depending on the sources of information the coverage of the term “Critical Infrastructure” differs considerably: In some documents it comprises only two aspects out of the dimension “Target”, in some documents more or even all (confer [PSC09], [BMI05], [BMI09], [ESR09], [CEC04] and [IPS05]). To avoid misunderstanding the term “Critical Infrastructure” is therefore not explicitly used in the CBRNE-MTS.

# 4 Possible Applications

During the compilation of the presented MTS within the framework of the DECOTESSC1 project, care had been taken to design the taxonomy system in a way that it could possibly be employed for many different applications. This section describes these considered applications and gives a brief guidance of the envisioned MTS uses.

## 4.1 Definition of the field of work and the subject of the project

During the definition of dimensions and aspects care has been taken that all possible CBRNE related topics could be categorized by the MTS which in turn allows the use of the MTS itself for defining the whole field of work. This would then be defined as the union of all possible combinations. Thus a much more accurate definition of CBRNE related topics could be given as all topics are explicitly listed in a very compact way and it is ensured that no topic is omitted, as long as the MTS is defined in a proper way. Also the complexity of the whole field of work is nicely visualized by the huge number of possible aspect combinations. Moreover the subject of the DECOTESSC1 project follows from the definition of the field of CBRNE related treads and gives the possibility to narrow the subject of the project by the identification of MTS cells or groups which are of no importance; these could be excluded with explicit justification. This ensures that only the most important MTS cells are handled in the curse of the project and allows on the other hand to re-evaluate the reasons for neglecting certain paths if the situation changes and reincorporate them. Furthermore, the existence and usage of the MTS ensures that people don't rely on some commonly-known terms, which are not strictly defined. Using such terms imposes the danger that different meanings are prevalent in the community, which could lead to misunderstandings, seriously hinder discussion and affect the results. Here the MTS greatly improves the situation, as one could precisely define the topic. Thus the MTS could be used as one management tool to optimize the value of the results obtained by the project.

## 4.2 Structuring of reports

The structure of the MTS, namely its dimensions with the contained aspects, allows for a clear and consistent structure of reports. The dimensions could be ranked by importance and the aspects are then used as the paragraphs and subparagraphs where certain aspects might be neglected or aggregated as needed. The depth, to which the dimensions are used to partition the report, could be chosen depending on the overall requirement, complexity of the report and also the increasing number of subparagraphs with increased number of employed dimensions. Using all eight dimensions as structuring levels is most probably unfeasible, but for large and complex reports using three or four dimensions might be practical.

If two or more reports need to have the same structuring, e.g. for comparing their results, the MTS could very easily be employed to create a consistent outline with minimal effort. The users only have to agree on the dimensions to use as structuring levels, their ranking and the possible neglection or aggregation of certain aspects. In the DECOTESSC1 project, the WP5 and WP6 will generate a requirement description and a state of the art description, respectively. The results of these two work packages will then serve as input for the WP7 gap-analysis. Here the MTS will be used to synchronize the report outlines for WP5, and WP6 which will further on facilitate the generation of the WP7 gap analysis.

### 4.3 Compilations of database

One of the most obvious applications of the MTS is the labelling of database-entries like reports, papers and books with one or a set of some aspects from each dimension, i.e. identify the topic of the object and label it accordingly. These labelled objects are in turn compiled to a database. Such a system would allow the retrieval of database-entries based on the combination of aspects from one, several or even all dimensions. This includes simple searches for all objects that possess one aspect of a specific dimension or also complex searches, where objects are retrieved that do or do not exhibit certain aspects from multiple dimensions. For special applications even sophisticated boolean combinations of the aspects might be allowed. For large databases this would allow a statistical evaluation that could identify topics, which are well covered among the stored objects (e.g. final reports of EU projects) or which are not handled at all. This would allow for an intensified search for objects of the not or less frequent handled topics. If such a topic is considered to be an important one, this identifies a gap, which finally might lead to the setup of a project addressing specifically this gap.

### 4.4 Identification of important topics and gaps

As indicated by the section concerning the compilation of a database, the MTS could be employed for the identification of important topics and gaps. The starting point might be the quantifiable evaluation of some kind of database, already structured by the MTS or, if such a database is not available or not well suited for this task, the knowledge of an expert. The MTS then allows a systematic search for gaps or important topics by evaluating all possible aspect combinations through the dimensions. Because of the large number of possibilities, wise simplifications have to be made. For instance, all topics dealing with detection technology are certainly independent of the country as the technology itself will be available in every European country. But at the same time, it might be the case that the technology is the same, but different expertise and training among different countries exists, which need to be analysed and might constitute a gap. Here the systematic search via the MTS explicitly raises the question if aspects could be aggregated or neglected, simply by the action of neglection and aggregation in itself. Keeping records of the reasons and assumptions for neglection and aggregation, an inherent quality control process is implemented.

### 4.5 Realizing complexity of field

One special use of the MTS is the visualization of the complexity and extent of the field of CBRNE related topics. In the present version, the MTS consists of 8 dimensions with over 50 aspects. Neglecting all sub-aspects and the aspects of the dimension “Geographic Location” the CBRNE-MTS yields a total of 31.500 different MTS cells. These numbers clearly shows how large the field of CBRNE related threads is. Some of these MTS cells are probably not or at least not at this time of for the current task of great importance, but only a systematic evaluation of all MTS cells ensures that no important one is missed.

# 5 Interfaces with other security-related themes

## 5.1 Crime fighting

Definition of crime

Crime may be defined as deviant behaviour that violates prevalent norms and standards which describe the coexistence of human individuals and normal behaviour. General crime definitions might change due to the complex realities and its dynamic shifts regarding social, political, psychological and economic conditions. Thus individual human societies may define crime differently. Therefore crime is the breach of law or general rules which can provoke the prescription of a conviction by governing authority. In case informal relationships and sanctions prove insufficient to establish and maintain a desired order, a government may introduce a stricter system of social control. Crime may be categorized in property crime, public order crime and violent crime. For a crime the following elements must be present: actus reus (guilty act), mens rea (guilty mind), harm, causation, concurrence, legality and punishment.

*Organized crime:*
Organized crime is defined by activities that require considerable skills in planning and organization as well as extended networks of participants, and are organized in infinitely variable ways. Therefore it is part of criminal behaviour known as group delinquency. It is a complex phenomenon, one that is difficult to distinguish from organized gangs and mafias.

*Illegal trafficking:*
Illegal trafficking is the covered transportation of persons and goods over a prohibited border such as international border between states, out or into a building including a prison. The act is illegal in case of violated prevalent rules or laws. Motivations for illegal trafficking include the illegal trade such as drugs, goods or the immigration and emigration. Further classification implements financial and non-financial terms. Non-financial motivations comprise the transport of banned items over a security checkpoint or the removal of classified documents from a government or corporate office. Illegal trafficking can be classified by the type of transported being or good and its intention. Goods are trafficked in order to supply demand for this ware or service, which is illegal or heavily taxed (e.g. illegal drugs, weapons, cigarettes…). Human beings pass over borders by people smuggling or human trafficking. People smuggling can be made as service to those wanting to illegally migrate and the involuntary trafficking of people. Trafficking in human beings involves that the trafficked victim is coerced in some way in the country of origin. The victims do not agree to be trafficked, thus they are tricked, lured by false promises or forced into it.
Another form of illegal trafficking is the smuggling of wildlife in order to cover demand for exotic species.

*Forensics and attribution:*
Forensics is the involvement of different scientific disciplines (e.g. molecular biology, biometry, informatics, analytical chemistry …) in order to answer questions of interest to a legal system. Its applications rely on an effective relationship between scientists, police, lawyers and other forensic specialists. New scientific developments lead to rapidly changing opportunities for giving of evidence such as DNA analysis. Methodical gathering and analysis of evidence is used for establishment of facts that can be presented in a legal proceeding. Though crime scenes and laboratories are perhaps, most often associated with forensics, there is also computer or network forensics, forensic accounting, forensic engineering and forensic psychiatry, among other specialized fields that are today an integral part of forensics.

Interfaces between CBRNE terrorist attacks and crime

The interfaces exist in the field of prevention related issues. During the preliminary stages of the preparation of attacks the terrorists are often involved in crime activities in order to acquire needed equipment (e.g. explosives, firearms, chemicals). They can also be involved in illegal trafficking in order to enter the countries in which they plan to perform the attack or e.g. by travelling to countries which are known for having terrorist training camps. In the field of forensics there is a huge overlap between normal crime and terror related crimes because mainly the same security and safety institutions are involved in criminal prosecution.

## 5.2 Disaster control

Definition of disaster

A disaster is an unexpected natural or man-made catastrophe of substantial extent causing significant physical damage or destruction, loss of life or sometimes permanent change to the natural environment. It includes unforeseen events causing great loss, upset or unpleasantness of whatever kind.

*Natural disaster:*
Natural disasters are nature borne, but can appear as man-made as well (e.g. snow slide, land slide, …) Natural disasters usually build up in a very short time giving low or even no time space for avoidance or preparation. The affected geographical areas can be huge and consequently the number of affected people may be large (e.g. bush-fires, floods or also the climate change).

*Man-made disaster:*
A man-made disaster is a threat or a crisis, which have parts of human intention, negligence, or error, or involving a failure of a man-made system. These disasters can be systematically categorized in social disasters, which include war, terrorism, civil disorders, crime and arson as well as in technical disasters, which includes industrial hazards, power outage, fire, hazardous material (such as CBRNE), and transportation (e.g. aviation, railroad, space) as well as economic disasters, which include enterprise bankruptcy as well as humanitarian crisis. The process of disaster control includes tools that apply to different missions using different technologies depending on the nature of the crisis. The appropriate methodology depends on the phase within the disaster management and also the type of incident. Man-made disasters are intended destructive acts perpetrated by individuals or groups.

Interfaces between CBRNE terrorist attacks and disaster control

As a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken for minimizing the effects of a disaster. Typically, disaster recovery planning involves an analysis of processes and continuity needs; it usually also includes a significant focus on disaster prevention. The crisis management includes the following challenges: management of the incident scene, crowd management and evacuation, search and rescue of victims, psycho-social support, communication of technical issues and information provisioning, implementation of coordinating mechanisms and procedures, crisis logistics, political sensitiveness, training and exercises. Therefore there are superior interfaces between terrorist attacks and disasters. Mostly of the response and recovery related means, precautions and activities are equal for both cases. Health protection, the involved facilities and institutions (like fire fighters, police etc.), action plans and training activities have thereby the most important interfaces for terrorist attacks, other man-made disasters and natural disasters.

### 5.3 Environmental protection

Definition

Environmental protection are the active measures for protecting the environment and its natural resources, on an individual, organizational or governmental level for the advantage of the natural environment and humans who live in it. Environmental protection includes any activity to maintain or reinstate the value of the environment through avoiding or reducing the emission of pollutants or reducing the presence of polluting substances in the environment. It may consist of changes in characteristics of goods and services, changes in consumption patterns, changes in production techniques, treatment or disposal of residuals in separate environmental protection facilities, recycling, and prevention of degradation of the landscape and ecosystems.

Interfaces between CBRNE terrorist attacks and environmental protection

Interfaces can be identified at all levels of terror threats from prevention, to detection, rescue and recovery. Protection and recovery which is mainly focused on human issues might be extended by the further aspect in order to involve complete environment with its living organisms. Further innovative tools for threat detection and prevention may be applied for the environment protection also in everyday life as well. Further aspects include the awareness during production and application of tools and methods concerning CBRNE threat issues. Several aspects of protection and control may be applied in similar manners using the same equipment and methods. Measures for improving air quality and also the protection of water resources may be evaluated using equal approaches to threat detection. Further reciprocal benefits may be achieved regarding different actions on climate change prevention and the assurance of the safety and applicability of chemicals.

### 5.4 Cyber-Crime and cyber security

Definition of cyber crime

Cyber crime may be defined as unlawful acts wherein the computer is either a tool or target or both. Thus it includes any crime where a computer is involved and in most cases several ones are connected to a network, in which the computers may be an instrument for the realization of a crime. Therefore no clear distinction between cyber and conventional crime might be defined. A net-crime refers, more precisely, to criminal exploitation of the internet. The issues concerning cyber crime involve hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Cybercrime also includes stealing millions of dollars from online bank accounts and non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. One of the most prominent known cyber crimes might be identity theft, where criminals use networks to steal personal information from other users.

*IT-virus:*
A computer virus is a program or a programming code which replicates by being copied or initiating its copying to another program, computer boot sector or document. Thus it can copy itself and infect computers as well as spreading from one computer to another when a user sends it over a network or the Internet, or carries it on a removable medium. In general there are three main classes of IT viruses: file infectors, system or boot record infectors, and macro viruses. Computer viruses are part of a taxonomy with malware as a higher order. Malware is the short name for malicious software, designed to infiltrate a computer system and includes a variety of forms of hostile, intrusive, or annoying software or program code. Thus Malware includes worms, trojan horses, spyware, dishonest adware, crime ware, most root kits, and other malicious and unwanted software.

Interfaces between CBRNE terrorist attacks and cyber crime

Cyber crime may be the base for terrorist attacks in all forms and at all organisational levels. Thus internet can be used as source of information as well as communication platform and can be a tool for organisations in order to realise their plans as well as a target for cyber crime itself. Because of the low age of this technology organisations and governments are quite unprepared to such sorts of attacks. Thus on a continental level, both governments and other organisations would be encouraged to prevent such activities including espionage, financial theft, cross border crimes. The computer may also be used as a tool for crime in order to harm a person or an institution, where the damage manifests in the real world. Usually these attacks focus on different weaknesses and are leading to mainly psychological and intangible harm. Such crime existed very long time, however the new tools increase its potential pool of victims and makes it more difficult to trace.

## 5.5 Space security

Definitions

Space may be defined as an unlimited three-dimensional expanse in which all material objects are located. In this context it is the place beyond our planet's atmosphere taking place between the celestial bodies of the universe. The density is normally negligible although cosmic rays, meteorites, gas clouds, etc., can occur. It can be divided into cislunar space (between the earth and moon), interplanetary space, interstellar space, and intergalactic space. Considering the humankind state-of-the-art of technology development, the space relevant to be considered concerning threat may be constrained to cislunar space, however also more projects discovering space beyond this limit are carried out. The involvement of space in espionage, security and commercial related themes increases the requirement of security-related definitions and actions. Thus Space security may be defined as the secure and sustainable access to, and use of, space and freedom from space-based threats.

*Security of aerospace missions:*
Because of the multiple use of space and wide range of space actors, a comprehensive and holistic outlook is necessary to achieve a reasonable understanding of space security and security of aerospace missions. The protection of communication links to and between satellites as well as to other aerospace missions is a major concern next to the protection of vulnerable space ground stations. Protection of space missions and satellites against some direct threats which lead to destruction is a high concern for ground stations but also for space missions, which however require sophisticated technology for an attack. Strategies for avoidance of large damage are mainly obtained through radiation hardening, system redundancy, and greater use of higher orbits. Additionally space systems may offer important support for military functions such as: communications, navigation, early-warning, reconnaissance, surveillance, imaging, and remote-sensing. In this context these systems could allow the realization of operations with speed, precision, and economy of force.

*Satellite security:*
The number of satellites and other objects in earth orbit has been continuously growing and because of its high speed in orbit, space debris can endanger space assets. In addition, satellites require an orbital slot and a portion of the radio frequency spectrum in order to effectively carry out their functions in orbit and ensure communication. The expansion of satellite applications harbours a growing demand for scarce radio frequency spectrum. Similarly, the growing demand for orbital slots has resulted in increased competition between satellite operators.

Interfaces between CBRNE terrorist attacks and space security

Space has become an important centre of social, economic, and military power. However, the dynamics of space security are still poorly understood. Space is a fragile environment and the resources of orbital space are limited. A further future topic will be the balance of the competing applications of civil, commercial, and military interests against the need for sustainable use of space that will ensure its utility for future generations. A potential threat is that satellites and other space systems may be damaged or even destroyed by electronic, explosive, kinetic, or directed energy weapons. Capabilities to attack ground stations and communications links are increasingly available to a broad range of actors. Direct attacks on satellites require sophisticated capabilities which are not widely available. This would need well improved technologies which could be present but negated by means of deception, denial, or disruption. Enabling technologies for space-based capabilities are being pursued by several states in the context of civil and military programs.

### 5.6 Health care system

Definitions

*Health care system:*
The key players of health care specially educated persons working autonomous (e.g. medical practitioner) or are employed at organisations that provides healthcare services (e.g. hospital). Such organisations might be a profit-oriented company or a non-profit organisation including charity based financing or a governmental entity. Organisations employing people providing health care are also known as health care providers. The goals for health care systems are good health for the citizens in the region, responsiveness to the expectations of the population, and fair financial contribution.

*Ambulance:*
An ambulance is a specially equipped automobile or other vehicle such as airplane, ship or motorcycles for carrying the sick or wounded to a hospital or other health care facility. An ambulance may also provide medical treatment directly at the place of the patient.

*Medical facilities:*
A medical facility is a place where practices for curing or healing of patient are carried out routinely. Such facilities provide rehabilitative, restorative and nursing care to patient or residents which require assistance with activities or routine activities. Parts of them are long-term care facilities including classical hospitals, nursing homes, rehabilitation facilities, inpatient behavioural health facilities, and long-term chronic care hospitals. Medical facilities range from small clinics and group practices to large hospitals which also have emergency rooms and trauma centres.

*Medical treatments:*
Medical treatment is the realisation of a surgery, the administration of a drug and other like substances or any other medical procedure carried out under supervision of a registered medical practitioner. This definition does not include diagnostic tests or advices that do not lead to a treatment. The treatment usually follows the diagnosis.
A preventive therapy is a treatment which is realised to avoid a medical condition to be manifested. This includes the vaccinations in order to prevent infectious diseases. A supportive therapy does not cure or treat the disease but is applied in order to alleviate pain.

Interfaces between CBRNE terrorist attacks and health care system

A possible threat may be an attack with means which cannot be treated with existing medical supply or also when medical treatment is not available at the time and place of requirement. Medical facilities

may be the target for attacks with explosives or other means that hinder the use of medical facilities. Other threat might be the circumvention of facility supply with infrastructure needed such as an electricity cut or a breakdown of communication channels. A further target may be the employees of medical facilities and other medical practitioner in order to complicate or hinder the treatment of patients or also of victims from different threats.

## 5.7 CBRNE Safety

Definitions

Whereas security deals with terrorist attacks and intended disasters, safety focuses on risks arising from unintended events initiated by natural occurrences, hardware failures, other internal events or interruptions (such as fire or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). Therefore safety measures implies e.g. regulations and techniques for storage and handling of CBRNE material, training of safety personnel, emergency and monitoring plans or measures, resulting in protection of workers, the public and the environment from undue CBRNE materials. There is a strong connection with disaster control and environmental protection issues. Safety is of paramount concern in today's high technology environment. There are many situations in witch extreme attention to safety systems is essential to achieve proper operating conditions, to prevent accidents or mitigate accident consequences. Some of those situations are e.g.: nuclear weapon detonation safety, nuclear reactor safety, mass transit transportation safety, hazardous materials transportation and handling safety. In each case, specific safety systems, human control, and administrative procedures are needed to give a high level of assurance against accidents and disasters. In an overview sense, safety concepts can therefore be divided into different broad approaches like general safety, operational safety and passive safety.

Although there are many similarities between safety and security there are also many issues standing in contrast with each other:

- Differences in the State's involvement: In occurrence of a security incident the state is directly involved in identifying a threat and may need to provide support in response to a terrorist act, but has no similar role in connection with a safety incident.
- In the field of security relevant information is traditionally kept more confidential than in the field of safety.
- Security personnel typically have a military or police background, whereas general safety staff is more typical of the general population, albeit with an emphasis on engineering or expertise in the maintenance or operation of machinery
- There are also circumstances in which actions to serve one objective can be antagonistic to the achievement of the other. For example, the introduction of delay barriers for security reasons can limit rapid access to respond to a safety event.
- The management of a crisis resulting from a terrorist act may demand the involvement of different and possibly more state bodies than one arising from a safety event. In addition to services to minimize the consequences of the event, the response to a terrorist event may involve law enforcement agencies, bomb disposal services and judicial authorities.

Interfaces between CBRNE Safety and Security

Nevertheless there are also a considerable overlaps between CBRNE safety and security. Safety and security have common purpose - the protection of people, society and environment. In both cases e.g. the protection is mainly achieved by preventing the release and spread of dangerous material. Because in both cases abnormal situations need to be detected early and acted on promptly to avoid consequent detriment, extensive emergency planning should be in place in the event of the failure of prevention,

protection and mitigation systems. Also in the field of training an education on detector systems there is a huge overlap because of the similarity of the used detection and monitoring techniques and equipment.

# 6 Summary

Within DECOTESSC1 project Work Package 4 deals with "System Description" and refers to the thorough understanding of the system-of-systems' structure. The objectives of this Work Package are:

- To define the field of work, especially the area where the strategic roadmap will lead, thus facilitating the work on the following work packages 5, 6 and 7 of the project by creating the appropriate structure and harmonizing the different steps of the analysis.
- To describe the system in such a way that it can be a starting point for data bases, communication, current evaluation work and future work by aggregation of subtopics, wise simplifications, concentration to essential points and identification of possibly important topics which have been neglected up to now.

This work package has been a basic step of the methodology, providing a systematic and sound structure for the description of relevant issues in the area of CBRNE threats and countermeasures including research and development. It had first to clarify what topics belong to the area and how they can be ordered. Aspects such as CBRNE prevention, response and recovery, operational, technical, political and social issues, etc., had to be defined, ordered and addressed.

Using a multidimensional approach, a Multidimensional Taxonomy System (MTS) was developed, in order to provide a comprehensive and broad overview to the subject. With the help of the MTS it is possible to define an enormous number of topics with only a limited number of terms. These are sorted in sets, called *dimensions*, which are intended to be set up in a way that single topic fields, called MTS-cells, can be defined by an unambiguous and manageable bunch of items - one item out of each dimension. The MTS system may serve as a basis for proper aggregations, simplifications, for clarification and concentration to essential points. In addition possible interfaces with other security-related themes were identified.

The CBRNE-MTS system was developed following an extensive compilation of definitions and taxonomies given in previous projects or identified by security-related committees and corresponding to a number of "good quality" criteria – including completeness, unambiguousness, minimisation of overlaps, clear relations, self-consistency, manageability and dissemination. The different CBRNE aspects and sub-aspects are organized around eight dimensions:

- Level of Action, including analysis (State-of-art, trend, etc.) and realization
- Readiness Level (e.g. R&D, Ability, Training and Education)
- Security Chain (Threat, Prevention, Preparedness, Response, Recovery)
- Threatening Material (C, B, R, N, E)
- Target (e.g. Transportation, Public Authorities, Gathering of People, Economy)
- Means for attack related activities (Organisational Means, Technology-based Techniques, Methodological Techniques)
- Perspectives (e.g. Feasibility, Political Issues, Social Issues, Legal Issues, Economical Issues)
- Geographic location (e.g. EU, different Member States, non-EU)

The CBRNE-MTS has been developed by the core group of DECOTESSC1 partners and discussed in detail with an expert group of 90 experts, who have been consulted through email and telephone and whose comments have been incorporated in the final MTS. Furthermore, a workshop organised by the JRC at Ispra, Italy, with the presence of 33 experts representing end-users, manufacturers, industry, academia and authorities, has also validated the findings and the proposed structure.

The limitations and possibilities of the proposed system are discussed in detail. Within the DECOTESSC1 project, these include the clear and unambiguous definition of the field of work and

the subject of the project, the common structuring of the reports, compilations of database elements, identification of important topics and gaps, and the possibility it offers the users to understand the complexity of the subject. Interfaces with other security-related themes were also identified and discussed, for example, related to topics such as crime fighting, disaster control, environmental protection, cyber-security, space security, health care system, and safety..

The CBRNE-MTS is intended to serve as guidance for the further work within the DECOTESSC1 project. In addition it offers the possibility that future research programmes and coordinating activities use it (perhaps in a modified way) as a framework to deal with the complex area of CBRNE threat and countermeasures, e.g. designing a common data base for CBRNE EU project documents. In that way it could help to focus new projects to more specific topics and avoid double work without neglecting the context, because the relations and the related projects could be easily identified.

# 7 References

[AIR07] AIRSECURE (Risk-based detection and filtration system for airports against airborne chemical, biological and radiological hazards), 2007

[ASS07] ASSRBCVUL (Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis), ASSRBCVUL - Final Report, 2007, *restricted*

[BIO08] BIO3R (Bioterrorism Resilience, Research, Reaction – Supporting Activity promoting co-Operation to assess the Bio Threat and organise a collective and comprehensive response for EU Society and Citizens' Biosecurity)

[BMI05] BMI (Federal Ministry of the Interior of Germany), Protection of Critical Infrastructures – Baseline Protection Concept (Recommendation for Companies), 2005

[BMI09] BMI (Federal Ministry of the Interior of Germany), BMI-KRITIS - Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (National Strategy for Protecting Critical Infrastructures), 2009

[CEC04] Commission of the European Communities, Communication from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 final, 2004

[CEC06] Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, 2006

[CEC09] Commission of the European Communities, Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, COM (2009) 273 final, 2009

[Chm10] S. Chmel, Structuring and Sorting – Thoughts to a multidimensional Taxonomy System and Related Quality Criteria, in preparation

[COP10] COPE (Developing a common operational picture between regional and national authorities, first responders etc.), 2010

[COR09] CORPS (Cross sector observations of threat perceptions and research priorities for biological homeland security in Europe), 2009

[CRE09] CREATIF (Network of Testing Facilities for CBRNE detection equipment), http://www.creatif-network.eu/home.html

[CRE10] CREATIF, Glossary to define common language and delimitations for testing, evaluation and certification of CBRNE detection equipment, Deliverable Report D.1.1, 2010

[CRS10] CRESCENDO (Coordination Action on Risks, Evolution of Threats and Context Assessment by an Enlarged Network for an R&D Roadmap), Presentations at Workshop CBRN-E, Brussels, 2010, http://www.crescendo-project.org

[DEM10] DEMASST (Demo for mass transportation security), Strategic Roadmap for Phase 2, DEMASST Final Forum D6.5, 2010

[DHS09] US Department of Homeland Security (DHS), National Infrastructure Protection Plan (NIPP), 2009

[DoD03] DoD Architecture Framework Working Group, DoD Architecture Framework Version 1.0, Deskbook, 2003

[EDA05] EDA (European Defence Agency), EDA Technology Taxonomy

[EOS09] EOS (European Organisation for Security), EOS – White Paper, Towards a harmonized EU civil protection, 2009

[ESA06] ESRAB (European Security Research Advisory Board), Meeting the Challenge: the European Security Research Agenda, Luxembourg: Office for Official Publications of the European Communities, 2006, - ISBN 92-79-01709-8

[ESR09] ESRIF (European Security Research and Innovation Forum), ESRIF Final Report, 2009, - ISBN 978-92-79-13025-0, http://www.esrif.eu/index.html

[ESS06] ESSTRT (European Security: High Level Study on Threats, Responses and Relevant Technologies), ESSTRT Final Report - New European Approaches to Counter Terrorism, 2006

[FEM08] FEMA (Federal Emergency Management Agency), National Response Framework (NRF), FEMA Publication P-682, 2008

[IMP05] IMPACT (Innovative Measures for the Protection Against CBRN Terrorism), IMPACT WP100, deliverable D100.1 - A Representative Set of Planning Scenarios, 2005, *restricted*

[IPS05] IPSC (Institute for the protection and Security of the Citizen), Research Strategy Paper - Emerging Technologies in the Context of "Security" -Issued in the Framework of Science and Technology Foresight, 2005

[JOP06] U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 3-41 (JP 3-41), Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management, 2006

[JOP08] U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 3-11 (JP 3-11), Operations in Chemical, Biological, Radiological and Nuclear (CBRN) environments, 2008

[JOP10] U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 1-02 (JP 1-02), DoD Dictionary of Military and Associated Terms, 2010

[OEC03] OECD (Organisation for Economic Co-operation and Development), OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response, Second Edition, OECD Environment, Health and Safety Publications, 2003, - (97 2003 10 1 P) ISBN 92-64-10181-0 – No. 53021 2003

[PAT07] PATIN (Protection of air transportation and infrastructure), 2007

[PSC05] Public Safety Canada (formally known as PSEPC: Public Safety and Emergency Preparedness Canada), The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada, 2005. - ISBN 0-662-68927-5, http://www.publicsafety.gc.ca/index-eng.aspx

[PSC09] Public Safety Canada (PSC), National Strategy for Critical Infrastructure, 2009, - ISBN: 978-1-100-11248-0, http://www.publicsafety.gc.ca/index-eng.aspx

[SEN06] SENTRE (Strategic research plan for security technology research), Security Network for Technological Research in Europe, Strategic research plan for security technology research, 2006

[STA11] START (National Consortium for the Study of Terrorism and Response to Terrorism), http://www.start.umd.edu/start/

[STC08] STACCATO (Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities), STACCATO Final Taxonomy, Deliverable D1.2.2, 2008

[STR08] STRAW (Security Technology Active Watch), D1.1 – Security Technology Watch List, 2008

[VIT06] VITA (Vital Infrastructure Threats and Assurance), Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at EU-level, Deliverable D1.2, 2006, http://vita.iabg.eu/

# Annex A Compilation of CBRNE-related projects and reports taken into account in elaborating

The objective of the present compilation was the identification of commonly used classifications and terminology as a base for the CBRNE - Multidimensional Taxonomy System (MTS). For this attention was paid mainly to European documents. The most important documents for our purpose are listed and shortly described below.

1. **ESRIF** (European Security Research and Innovation Forum), ESRIF Final Report, 2009., http://www.esrif.eu/index.html ([ESR09])

ESRIF was established in September 2007, based on a joint initiative of the European Commission and the 27 EU member states and lasted till December 2009. ESRIF consisted of 64 members from 31 countries (member states and associated countries) and was assessed by more than 600 experts from industry, public and private end-users, research establishments and universities, as well as non-governmental organisations and EU bodies.

The main purpose of ESRIF was to analyze the medium and long-term challenges (up to 20 years) that Europe faces. These range from natural disasters to organised crime and man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects. As the result of the work ESRIF has defined a European Security Research and Innovation Agenda (ESRIA) that identifies and roadmaps key capabilities and research needs in line with the main work results in the field of the security cycle, countering different means of attack, securing critical assets and securing identity, access and movement of people and goods.

2. **STACCATO** (STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities), STACCATO Final Taxonomy, Deliverable D1.2.2, 2008 ([STC08])

STACCATO (started on 15th January 2007 as a European funded supporting activity under the Preparatory Action for Security Research (PASR) and had a duration of 16 months. It was a follow up activity of SeNTRE (Security Network for Technological Research in Europe) which was a supporting activity funded under PASR 2004. STACCATO aims at proposing methods and solutions for the creation of a security market and a structured supply chain in Europe.

In line with ESRAB (see next bullet) recommendations, it will go beyond research needs and gap analysis already undertaken through efforts supported by PASR, by identifying implementation measures. STACCATO's objectives were to:

- Map existing competencies in the EU-27, highlighting particularly the role of SMEs in order to integrate their innovation potential and examine ways to effectively undertake a coordination of the European Security and Technological Industrial Base (STIB);
- Propose a methodology for Technology Watch;
- Analyse the conditions and propose recommendations to develop a common European Security Equipment Market (ESEM), by identifying common needs, taking into account regulatory issues and coordinating with regional, national, international and EU security research programmes.

Part of the project's achievements were to establish a stakeholder platforms/network, to coordinate with existing or planned research programmes in Europe; and to develop a comprehensive and

detailed database to support the competence mapping of the European STIB. The objective of this database was to structure the participating stakeholders according to their scientific, technological, industrial and/or service support competences.

3. **ESRAB** (European Security Research Advisory Board), Meeting the Challenge: the European Security Research Agenda, Luxembourg: Office for Official Publications of the European Communities, 2006. ([ESA06])

To develop a longer-term perspective in the field of security research, a Group of Personalities (GoP) was set up. The group was composed of high-level industrialists, Members of the European Parliament, and representatives of international organizations and research institutes. In March 2004, they presented their report to the President of the Commission, entitled 'Research for a secure Europe' in which they recommended the formation of a European Security Research Advisory Board (ESRAB) to draw the strategic lines for European security research and to advise on the principles and mechanism for its implementation within the Commission's seventh framework programme for research and technology development (FP7). Furthermore, they proposed that the board focus on two principal objectives: meeting society's needs through the definition of clearly defined customer (end-user) needs and raising the global competitiveness of the European technology supply chain. ESRAB was formed in April 2005 and signalised Europe's intent to make a significant contribution towards addressing security research and technology needs. It brought together demand articulators and research and technology suppliers in a 50-person-strong board of high-level specialists and strategists with expertise in the field of security research including: public authorities, industry, research institutes and specialist think tanks. In addition, five Members of the European Parliament and representatives from 14 European Commission services participated in the workings of the board. The board delivered its report on September 2006. ESRAB focused on four mission areas: protection against terrorism and organized crime, border security, critical infrastructure protection and restoring security in case of crisis. From the analysis of these four security missions, capability requirements were described, grouped into functional areas, and then supporting technologies identified. As part of the findings, ESRAB has produced a strategic framework to structure the research content covering both technological and non-technological aspects giving priorities to activities which offer a high potential to deliver European Added value. ESRAB also recommends that multi-disciplinary mission-oriented research should be undertaken covering capability development, system development and systems of systems demonstration. Technology development should include new and emerging technologies to address security-specific breakthrough technologies. ESRAB also recommends the creation of a European Security Board designed to turn the current patchwork of security related activities and policies into a coherent and synchronized series of roadmap.

4. **DEMASST** (DEmo for MASS Transportation security), Strategic Roadmap for Phase 2, DEMASST Final Forum D6.5, 2010 ([DEM10])

DEMASST is a Phase 1 demonstration project within EU's Seventh Framework Program for Research and Technological Development (FP7). The major goal of the project is to produce a roadmap definition for the Phase 2 demonstration program Security of Mass Transportation, which will promote large scale integration, validation and demonstration of new security systems of systems going significantly beyond the state of art.

DEMASST takes on the dual challenges of analysis and networking necessary to define and achieve commitment for the strategic roadmap for the Phase 2 Demonstration project. "Mass transportation" in the context of the security terminology used in the European Union is mostly oriented towards urban public transportation, such as metro, tram, commuter train, city busses and inter-modal, critical

nodes, including those connecting long-distance transports with urban transport systems. The approach of DEMASST is thus a broad range of public transport but focusing on rail in megacities.

DEMASST develops a highly structured approach to the demonstration program built on identifying the main security gaps and the most promising integrated solutions, utilising sufficiently mature technologies, for filling them. In the type of Concept Development & Experimentation approach proposed the experiments must be designed and analysed so as to be maximally informative.

Given the vast variation in mass transportation systems an effective demonstration program must also identify synergies between demo tasks and use less costly methods than full scale demonstration whenever that helps a broader awareness.

DEMASST proposes to build the methodological infrastructure for this. But an optimal demo project design does not stop with finding scientific answers: the issue of turning demonstration into innovation is top on DEMASST's agenda. And this approach will have utility also beyond transportation. The project was carried out between January 2009 and April 2010. The final report is under the review of the European Commission.

The second phase of the demonstration project will probably start at January 1, 2011 under the name SECUR-ED.

5. **DoD Architecture Framework Working Group**, DoD Architecture Framework Version 1.0, Deskbook, 2003 ([DoD03])

The Department of Defense (DoD) Architecture Framework (DoDAF) defines a common approach for describing, presenting and comparing DoD enterprise architectures and facilitates the uses of common principles, assumptions and terminology. The DoD Architecture Framework 1.0 was published in 2003 (and the version 1.5 in 2007), and its principal objective is to ensure that architecture descriptions can be compared and related across organizational boundaries including joint and multi-national boundaries. The purpose of the DoD Architecture Framework Version 1.0, is to provide guidance for describing architectures. It establishes data element definitions, rules, and relationships and a baseline set of products for consistent development of systems, integrated, or federated architectures. These architecture descriptions may include Families of Systems (FoSs), Systems of Systems (SoSs), and net-centric capabilities for interoperating and interacting.

The DoDAF is a reference model to organize the enterprise architecture (EA) and systems architecture into complementary and consistent views. The DoDAF defines a set of products that act as mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of an architecture description through graphic, tabular, or textual means. It is especially suited to large systems with complex integration and interoperability challenges, and is apparently unique in its use of "operational views" detailing the external customer's operating domain in which the developing system will operate. While it is clearly aimed at military systems, DoDAF has broad applicability across the private, public and voluntary sectors around the world, and represents only one of a large number of systems architecture frameworks

6. **EDA** (European Defence Agency), EDA Technology Taxonomy ([EDA05])

The European Defence Agency was established under a Joint Action of the Council of Ministers on 12 July, 2004, "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and

Defence Policy as it stands now and develops in the future". The European Defence Agency, within the overall mission set out in the Joint Action, is ascribed four functions, covering developing defence capabilities; promoting Defence Research and Technology (R&T); promoting armaments co-operation; and creating a competitive European Defence Equipment Market and strengthening the European Defence, Technological and Industrial Base. All these functions relate to improving Europe's defence performance, by promoting coherence. A more integrated approach to capability development will contribute to better-defined future requirements on which collaborations - in armaments or R&T or the operational domain - can be built. More collaboration will, in turn, provide opportunities for industrial restructuring and progress towards the continental-scale demand and market, which industry needs.

To ensure that R&T efforts are aligned with agreed capability needs, the Agency has developed a series of CapTech networks. Each of them focuses on a particular military domain and the technologies associated with it. It also brings together a network of experts drawn from Member States, industry, research institutes, academic institutions and agencies (International, European and National). They are grouped under information acquisition and processing, guidance, energy and materials, and environment systems and modelling; corresponding technology taxonomy has been developed by EDA.

7. **EOS** (European Organisation for Security), EOS – White Paper, Towards a harmonized EU civil protection, 2009 ([EOS09])

EOS was created in July 2007 by European private sector suppliers and users from all domains of security solutions and services to develop a consistent European Security market. EOS has 2 millions employees over 12 European countries representing all major sectors: defence, civil security, ICT, energy, transport, finance, services and research. EOS' main objective is the development of a consistent European Security Market and a sustainable European Security Model that satisfies political, social and economic needs through the efficient use of budgets and the implementation of available solutions in priority areas. EOS actively supports:

- the development of civil security & resilience systems and related services with innovative European approaches that can be used in the global security market,
- the effective implementation of existing and future solutions and services by developing interoperable and consistent architectures, interfaces, innovative methodologies and/or common procedures, best practices, pilot projects, etc.

In 2009 EOS published its Position Paper on "EOS Priorities for a Future European Security Framework" together with 8White Papers with common recommendations for EU on: Border Surveillance, Border Management, Civil Protection, ICT Network Security, Civil Aviation Security, Surface Transport Security, Supply Chain Security, Energy Infrastructures Security & Resilience.

The European Union regularly suffers from natural and man-made disasters, the social and economical consequences of which may adversely affect its growth and competitiveness. There is evidence of a growing vulnerability to disasters due to the worsening conditions of climate change, the increased probability of a CBRNE accident, a pandemic or similar wide impact health threat, which will have a large impact on human life, ecosystems, political and social stability, the economy and infrastructure. EOS is proposing to the EC and, where possible, to the different MS, to implement the following main recommendations.

To face these challenges, the EU is strongly advised to improve EU global governance to achieve a stronger coordination between local/national and EU activities in order to enhance the European Civil Protection Policy. The deployment of such policy should be facilitated by the creation of a pan-

European Advisory Forum for Crisis Management and Civil Protection. To enhance regional cooperation for sharing best practices, interoperability of procedures with increased solidarity improved training and simulation, the EU should support cooperation between MS and first responder organisations. First responders and industry are called to develop cost-effective technologies for the prevention, early detection and response to CBRNE threats, and the EC is further advised to develop a common EU Risk Assessment methodology for increased interoperability of Civil Protection operational techniques, procedures and systems. It should also create an EU Programme on Civil Protection to improve prevention, preparedness, response and remediation from natural and manmade disasters and crisis situations, while supporting the development and implementation of common / similar procedures and interoperable resources across MS (emergency communications, first responders' tools). Finally, EU Civil Protection stakeholders should support the development of societal issues, i.e. the involvement of civil society in preventing and responding to crises, the adequate involvement of media, and enhanced medical support for victims and first responders.

8. **IMPACT** (Innovative Measures for the Protection Against CBRN Terrorism), IMPACT WP100, deliverable D100.1 - A Representative Set of Planning Scenarios, 2005, *restricted* ([IMP05])

IMPACT was one of the PASR 2004 projects carried out in the period December 2004 – December 2006, with the participation of 20 partners from 10 Member States under the coordination of TNO. The starting point of IMPACT is that current European capabilities to detect and respond to the types of CBRN threats are modest and the responsibility in Europe for responding to terrorist incidents is spread among many organizations, making it necessary to unify much of the current response capability while at the same time, setting standards and establishing guidelines for European nations to address coordination of their response to terrorism. The objectives of IMPACT are to lay the foundations for an integrated European CBRN counter terrorism research and acquisition programme. This programme should be used to validate, assess and demonstrate innovative technological capabilities, operational concepts and procedures to assist in preventive and suppressive crisis management.

The approach of IMPACT is based on five pillars: the threat and further prevention, protection, responding to and recovering from an event. An important outcome of the project was a representative set of planning scenarios, which – together with the CBRN agent database – allowed a more in-depth understanding of the threats and set the requirements for addressing them. The elaborated scenarios covered a wide spectrum of threats and events:

- use of chemical agents (chemical weapons)
- use of Toxic Industrial Chemicals (TICs)
- use of Biological agents
- use of Radiological agents
- attack to nuclear facilities
- hoax attack
- one combined attack scenario (mixed radiological and chemical)

In the representative scenarios, the agent, the actor, the means of execution and the evolution of the event are described and 1st, 2nd and 3rd order effects are estimated, while counterterrorism measures are proposed.

Furthermore, analysis of the role of first responders throughout Europe has been performed in the project and proposal for a first responder's doctrine was written. System requirements for the response team as well as on C, B and R/N detection, physical protection, decontamination and sampling were formulated. An overview of current and emerging detection techniques for C and R/N agents was

provided, while current capabilities for detection of B agents were assessed. In summary, The IMPACT project approached the CBRN counterterrorism in an integrated way.

9. **STRAW** (Security Technology Active Watch), D1.1 – Security Technology Watch List, 2008 ([STR08])

STRAW is a support action under the Security Research theme that aims at providing a European Service of Technology Watch on Security Technologies. The project started in October 2008 and has a duration of 20 months. The concept of STRAW is to bring together the defence and security research industry by a neutral coordination to ensure the awareness of underpinning technologies that make possible the implementation of civil security applications. There are two ongoing initiatives on technology taxonomy within EU, one from the industry and another from military community. STRAW aims at harmonizing both under the umbrella of an European Technology Watch in order to advise public authorities, EU security research community and public at large on emerging technologies.

STRAW vision is to support research activities and policies under Security theme supported by the following objectives:

- Collection of data from the different entry points, managing the quality, relevance, reliability, sensitiveness and innovativeness of the data provided on available technologies, with a view to create a network of contact points responsible for managing data entries.
- Combination of the different entries using a Taxonomy Mix Approach.
- Performing of a segmentation of information receivers and customise the right information for each segment in order to forecast the likely security technology information to be used in the relevant areas.
- Deliver the information using the most efficient channels in order that the users could efficiently and effectively meet the challenges resulting from global technological changes.
- To create a panel of security experts to monitor the network implementation and advise the EC, MS etc.

Within the project a number of different taxonomies have been explored. This exploration undertook a common definition and scope of the “security” concept and how the associated elements (players, technologies and terms) are structured according to different approaches. These include ESRAB, ESRIF, STACCATO and the U.S. Department of Homeland Security. As result, the STACCATO (Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities) Taxonomy has agreed to be the most appropriate one for STRAW. The taxonomy is split into 7 main sections each comprising 3 hierarchical levels. No hierarchy is assumed between the main sections, however there is a gradual shift in focus of the sections from technologies to missions. The main Mission capabilities identified are the following:

- Ensure Identification and control of goods and people
- Ensure and Maintaining Law and Order
- Protection of citizens (goods and people)
- Avert and foreseen Catastrophes
- Control and surveillance of areas
- Protection of areas and infrastructures
- Protection of networks
- Crisis management
- Control of disarmament/ fight against proliferation

10. **ASSRBCVUL** (Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis), ASSRBCVUL - Final Report, 2007, *restricted* ([ASS07])

ASSRBCVUL is a Coordination Action that was carried out in FP6 with the participation of 6 EU and one non-EU partners, under the coordination of TNO. The project was concluded in May 2007. The purpose was to assess the technological, social, economic and psychological vulnerabilities of the modern societies that make up the EU to radiological, biological or chemical terrorism with the view to assist in developing preventive and suppressive crisis management strategies.

The approach chosen for this project is risk assessment and management. After the description of the model, the threat is assessed that RBC agents pose to EU society in the possibility of their deliberate release by terrorists. The next step is assessment of the vulnerability of EU society towards deliberate release of RBC agents, with policy measures necessary to prevent and mitigate the effects of attacks coming next. Further, a set of planning scenarios are described, which could be used for the assessment of EU's RBC terrorism vulnerability. The scenarios are used to assess the potential for success (and/or failure) of specific policy measures. Finally, assessment of the policy and counter measures is performed, on a scenario based risk assessment culminating in the definition of a set of damage profiles, while analysis of policy and counter measures on an EU and Member State level is carried out.

11. **START** (National Consortium for the Study of Terrorism and Response to Terrorism), http://www.start.umd.edu/start/ ([STA11])

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a U.S. Department of Homeland Security Center of Excellence, tasked by the Department of Homeland Security's Science and Technology Directorate with using state-of-the-art theories, methods, and data from the social and behavioural sciences to improve understanding of the origins, dynamics, and social and psychological impacts of terrorism. START, based at the University of Maryland, College Park, aims to provide timely guidance on how to disrupt terrorist networks, reduce the incidence of terrorism, and enhance the resilience of U.S. society in the face of the terrorist threat.

START researchers use a variety of approaches in their projects, ranging from analyses of statistical data to in-depth examinations of individual case studies, from survey-based analyses to reviews of public documents, and beyond. This range of methods will help to provide both a broad and deep understanding of the dynamics of terrorism and terrorists, allowing for more effective counter-terrorism measures.

Amongst the most interesting activities of START are the activities of WG3: Societal Responses to Terrorist Threats and Attacks. This Group provides scientifically derived insights on perceptions of, preparations for, responses to, and recovery from terrorist attacks, focusing on the domestic US setting. Investigators mine existing databases and literature to develop timely guidance on what is already known. Concurrently, WG3 conducts original research on issues that are poorly understood: risk perception and communication; household and community preparedness for terrorist attacks; likely behavioural responses by the public to a future terrorist attack; social and psychological vulnerability to terrorism and weapons of mass destruction; and strategies for mitigating negative psychological effects and enhancing resilience in the face of the terror threat.

12. **CRESCENDO** (Coordination Action on Risks, Evolution of Threats and Context Assessment by an Enlarged Network for an R&D Roadmap), Presentations at Workshop CBRN-E, Brussels, 2010, http://www.crescendo-project.org ([CRS10])

CRESCENDO is an on-going FP7 research project started in July 2009, with a duration of 24 months. Building on the experience of the PASR SeNTRE and STACCATO projects, the 2 year CRESCENDO Coordination Action intends, under the lead of CEA, to respond to the request of the users and the experts who attended these first workshops to continue working together and to enlarge their activities. They raised concerns on how to improve the innovation process, how to create a real European security market and how to strengthen European competitiveness by closing the loop between academia, industry, including SMEs and the users.

CRESCENDO focuses on the following objectives:

- Operation of an enlarged security network comprising public stakeholders, industries, SMEs, RTOs, think tanks and academia in the EU 27, with a specific focus on the new Member states, as well as in the Associated Countries
- Deeper analysis of the environment: Evolution of societal security (threats and risks). Policies, regulation and standardization analysis in order to define processes for harmonized, ubiquitous, clear and unambiguous, regulations, policies and standards.
- Recommendations for a Comprehensive Innovation Process aiming at identifying the best possible structure for the security supply chain, i.e. the European Security and Technological Industrial Base (STIB)
- A strategic R&D Roadmap aiming at supporting the EC, ESRIF working groups and EU Member States in preparing European and national research programmes
- Consolidation and continuous dialogue and recommendations for future development and acquisition programmes at European and national levels paving the way towards a European Security Equipment Market (ESEM).

CRESCENDO will gather homogeneous communities of experts and users, to address the FP7 missions through workshops and interviews coordinated by CEA, with the main RTOs, industries and related associations as partners.

13. **OECD** (Organisation for Economic Co-operation and Development), OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response, Second Edition, OECD Environment, Health and Safety Publications, 2003 ([OEC03])

The Guiding Principles, which have been prepared under the auspices of the OECD Working Group on Chemical Accidents, have been developed in co-operation with other international organisations active in the area of chemical accident prevention, preparedness and response, including ILO, IMO, UNECE, UNEP, UNOCHA (UNEP/OCHA Joint Environment Unit) and WHO.

The objective of these Guiding Principles is to set out general guidance for the safe planning, construction, management, operation and review of safety performance of hazardous installation in order to prevent accidents involving hazardous substances and, recognising that such accidents may nonetheless occur, to mitigate adverse effects through effective land-use planning and emergency preparedness and response. These principles provide advice related to the role and responsibilities of public authorities, industry, employees and their representatives, as well as interested parties such as members of the public potentially affected in the event of an accident, and non-governmental organisations.

Detailed guidance covers all phases of accident risk management, from accident prevention, to emergency preparedness and mitigation, to emergency response and follow-up to accidents with accident investigation, identification of lessons learned and dissemination. In principle, focus is given to fixed installations, while special issues such as transportation or accidents occurring during loading/unloading operations are also covered.

14. **BMI** (Federal Ministry of the Interior of Germany), BMI-KRITIS - Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (National Strategy for Protecting Critical Infrastructures), 2009 ([BMI09])

The BMI is a ministry of the Federal Government and is amongst other things responsible for the internal security, for protecting the public against violence, terrorism, crime and disasters. It is also responsible for identity cards, passports, firearms and data protection.

The "National Strategy for Protecting Critical Infrastructures" (CRITIS-Strategy) aggregates the objectives and the political-strategic approach of the German Federal Republic and is the initial point for continuing the so far reached achievements on a consolidated basis and for further development with the view on new challenges.

The main topics of this document were:

- Previous results of the work over the last years
- Criticality of infrastructure and areas of authority
- Threats, risks and vulnerabilities of critical infrastructure
- Strategic objectives
- National and international cooperation
- Assembly procedures

15. **CREATIF** (Network of Testing Facilities for CBRNE detection equipment), http://www.creatif-network.eu/home.html ([CRE09])

The CREATIF network is dedicated to provide a communication platform for technology users and decision makers, providers and testers to discuss the future development of testing and to support user decisions and product / service development. Stakeholders are invited to exchange their views and knowledge: testing facilities can publish information about their expertise and testing capabilities / facilities in a database on testing facilities within EU-27, an advisory group of selected end-users and industrial experts will be established to integrate their point of view into project deliverables and topical workshops. In these workshops specific themes in the field of certification and testing of CBRNE detection equipment are discussed. CREATIF will ensure a careful examination of existing testing protocols and relevant standards to suggest harmonization of testing in the field of CBRNE detection both on a geographic scale within EU-27 and on a technical level. Possibilities to amend testing protocols by covering human factors and operational / scenario based testing will be suggested. Additional deliverables of the network will be a roadmap for a European certification system for CBRNE detection products & services and a concept on the continuation of the CREATIF network as an autonomous body after the end of the funded project. The CREATIF network of Testing Facilities for CBRNE detection equipment is a European project, financed under the FP7 security theme; it started in February 2009 and is still on-going (duration of 30 months).

16. **Public Safety Canada**, National Strategy for Critical Infrastructure, 2009. - ISBN: 978-1-100-11248-0, http://www.publicsafety.gc.ca/index-eng.aspx ([PSC09])

The goal of the National Strategy for Critical Infrastructure is to build a safer, more secure and more resilient nation of Canada. To this end, the National Strategy advances more coherent and complementary actions among federal, provincial and territorial initiatives and among the ten critical infrastructure sectors listed below:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Information and communication technology
- Health
- Water
- Safety
- Manufacturing

The National Strategy fosters the development of partnerships among federal, provincial and territorial governments and critical infrastructure sectors, advances an all-hazards risk management approach, and sets out measures to improve information sharing and protection.

Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. The National Strategy supports the principle that critical infrastructure roles and activities should be carried out in a responsible manner at all levels of society in Canada. Responsibilities for critical infrastructure in Canada are shared by federal, provincial and territorial governments, local authorities and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services – while individuals also have a responsibility to be prepared for a disruption and to ensure that they and their families are ready to cope for at least the first 72 hours of an emergency.

The Strategy proposes that federal, provincial and territorial governments and critical infrastructure sectors collaborate to strengthen the resiliency of critical infrastructure in Canada. It also recognizes that primary responsibility for strengthening the resiliency of critical infrastructure rests with the owners and operators. Enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters.

17. **Public Safety Canada** (formally known as PSEPC: Public Safety and Emergency Preparedness Canada), The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada, 2005., http://www.publicsafety.gc.ca/index-eng.aspx ([PSC05])

The aim of the CBRN Strategy of the Government of Canada is to protect Canada and Canadians by taking all possible measures to prevent, mitigate and respond effectively to a potential CBRN incident.

The CBRN Strategy supports the Government's National Security Policy and supports the Government of Canada's Anti-Terrorism Action Plan announced after September 11, 2001, which aims to:

- prevent terrorists from entering Canada
- protect Canadians from terrorist acts
- bring forward tools to identify, prosecute, convict and punish terrorists
- keep the Canada-U.S. border secure and open to legitimate trade
- work with the international community to bring terrorists to justice.

The CBRN Strategy incorporates both domestic and international elements, and incorporates crisis and consequence management. It is part of Canada's National Emergency Management System and is inclusive of federal departments and authorities, and is coordinated with provincial and territorial governments.

Also enhancing communication between departments, other levels of government, international partners, the media, the private sector and general public belong to the strategy.
The province or territory where a CBRN terrorist event occurs has the main responsibility to manage its consequences. They are also responsible for working with municipalities. If needed, a province or territory can request additional assistance from the federal government. The CBRN Strategy consists of strategic objectives to enhance Canada's ability to mitigate and prevent CBRN incidents from occurring. The objectives will also allow Canada to prepare for, respond to, and recover from, CBRN incidents. Four strategic objectives are necessary to achieve the CBRN Strategy's aim: Prevention and mitigation; preparedness; response and recovery.

The primary governing bodies to guide the implementation of the CBRN Strategy of the Government of Canada, and its objectives, begins with the Assistant Deputy Minister (ADM) Public Safety Committee, which reports through Deputy Ministers to the Cabinet Committee on Security, Public Health and Emergencies. A report assessing the status of initiatives to fulfill the CBRN Strategy's objectives will be provided to the relative governing bodies by Public Safety and Emergency Preparedness Canada (PSEPC) annually.

The Federal/Provincial/Territorial CBRN Working Group and Committee of Senior Officials Responsible for Emergency Management (SOREM) will act as the main coordinating bodies to link federal and provincial-territorial governments as they develop and carry out programs and initiatives in support of the CBRN Strategy. The PSEPC will continue to coordinate the implementation of the CBRN Strategy, providing updates as necessary on initiatives that fulfill the CBRN Strategy's objectives, and reporting to government as required.

18. **U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 3-11 (JP 3-11),** Operations in Chemical, Biological Radiological and Nuclear (CBRN) environments, 2008, http://www.fas.org/irp/doddir/dod/jp3-11.pdf ([JOP08])

This publication, edited by high level US military professionals, describes the Security Environment for Employment or Threat of Chemical, Biological, Radiological and Nuclear (CBRN) Weapons, the CBRN Defense Framework and Sustainment Considerations in a CBRN Environment. It also provides Considerations for CBRN Planning and Operations.

This publication provides doctrine to assist commanders and staffs in planning, preparing for, conducting, and assessing operations in which their forces may encounter chemical, biological, radiological, and nuclear threats and hazards.

The threat of chemical, biological, radiological, and nuclear (CBRN) weapons, including toxic industrial materials (TIMs) pose serious challenges to US military operations across the globe. The worldwide availability of advanced military and commercial technologies (including dual-use),

combined with commonly available transportation and delivery means, may allow adversaries opportunities to develop and employ CBRN weapons without regard for national or regional boundaries.

Nation states and non-state actors alike may have incentives to operate outside of international regulations/agreements, especially when important interests are involved. Even if an adversary does not intend to use a CBRN weapon, the potential existence of CBRN threats and hazards in any operational area creates potential risks.

Adversaries may be of the nation state or non-state actor persuasion and could have local, regional, or global reach. CBRN defence is based on three general principles that specifically address the hazards created by CBRN incidents: contamination avoidance of CBRN hazards; protection of individuals, units, and equipment from unavoidable CBRN hazards; and decontamination in order to restore operational capability. Application of these principles helps to minimize vulnerabilities, protect friendly forces, and maintain the force's operational tempo in order to achieve operation or campaign objectives.

19. **ESSTRT** (European security: High level Study on Threats, Responses and relevant Technologies), ESSTRT Final Report – New European Approaches to Counter Terrorism, 2006 ([ESS06])

The above-mentioned document is the final report of the ESSTRT consortium, which consists of Thales, the International Institute for Strategic Studies, and Crisis Management Initiative. The report takes the form of a set of recommendations on countering terrorism, followed by a summary of the conclusions of a 16-month study carried out by the consortium.

The consortium analyzed threats to European security, and in particular the threat from international terrorism. It examined actual and potential responses to terrorist threats; the technologies that are and could be deployed in support of these responses; the ethical and legislative issues raised by these responses and technologies.

Finally, the consortium drew up a set of recommendations for the Commission and for European governments. European countries can substantially reduce the threat from international terrorism if they adopt a comprehensive strategic approach, according to the ESSTRT Study of European security. The Study finds that Europe could benefit from investment in a wide range of technologies that would bolster protection against terrorist attacks. The Study recommends that individual nations conduct risk-based assessments of Critical National Infrastructures – those assets and activities which, if damaged or destroyed, would affect a country's ability to continue normal life. It recommends that all European countries adopt a range of actions intended to prevent terrorist action, to pursue those responsible, to protect against attacks and to develop resilience against them.

Each country should have a crisis management structure that would regularly rehearse tackling contingencies. The Study suggests these national actions should be backed by a set of enabling capabilities including intelligence information, a strong policy of public communication, and the impact of technological solutions could be considerably enhanced by research on improvements – both in protecting against physical attacks, and in warding off attacks on networked data systems.

In designing and adopting countermeasures ESSTRT has developed and proposes the "Four-fences" model: This is done by considering the "fences" that terrorists may have to cross in order to attack a target. The model is useful because it provides a link between threats and technology: the "fences"

represent the points in the build-up to an attack at which use of technologies may be helpful. The 4 fences considered are:

- Intelligence
- border control,
- general surveillance, and
- target protection

Among technologies that, if advanced and improved, would considerably bolster security measures are:

- Scanners or other methods of detecting weapons or hazardous substances. This would improve security at airports and other travel hubs, for example by better scanning of people and luggage for weapons.
- "Smart containers" should be developed for sea transport and large vehicles, because of the inadequacies of existing scanning technologies for large objects.
- Area surveillance and perimeter/border protection. This would include surveillance of public spaces to detect unusual behaviour, and of remote, unattended borders.
- Personal identification, including biometrics. Though biometrics have been introduced into some personal identification documents, rates of false rejection and false acceptance are too high and could be reduced.
- Fast detection and identification of chemical, biological and radiological substances.
- For networked data systems, technologies should be developed to cope with and recover from attacks, since it is rarely possible to prevent all attacks. The most important solutions are intrusion tolerance and survivability, backup tools and monitoring tools. To protect against human error or malicious intent, high assurance software development methodologies and automated support for network management are needed.

As well as making recommendations on measures to counter-terrorism, the ESSTRT team studied internal security threats to Europe, the responses so far, and technologies relevant to improving security. Finally, the Study suggests a set of criteria – utilising the Four P (prevention, pursuit, protection and preparedness) and Four Fence models – by which governments might assess the effectiveness of counter-terrorist measures.

20. **BIO3R** (Bioterrorism Resilience, Research, Reaction – Supporting Activity promoting co-Operation to assess the Bio Threat and organise a collective and comprehensive response for EU Society and Citizens' Biosecurity) ([BIO08])

BIO3R was one of the PASR 2006 projects carried out in the period 2007–2008, with the participation of twenty partners from eight Member States under the coordination of "Fondation pour la Recherché Stratégique", France. The project aims at contributing to the improvement of the European preparedness in the field of bioterrorism and to a better comprehension of citizens and professionals by tackling three main issues:

- Research, with an evaluation of the state of the art in relation with the risk assessment and the identification of operational requirements, which helped to select priorities for future research;
- Reaction, aiming at the reinforcement of crisis management policies, through improvement of the networking and better integration of public and law strategies at European, national and local levels; and
- Resilience, with the objective to make EU societies stronger and more resistant to aggression, by reinforcing the awareness and the preparation of the EU citizens regarding the biothreat, through access to reliable information, and through education and training, thus by acting on their perception.

The first step within the BIO3R project was the identification of a number of realistic scenarios, leading to threat assessment and the identification of operational requirements. This is completed by an evaluation of the epidemiological modelling capacities in relation with the improvement of bioterrorism preparedness and response. Then available countermeasures were assessed related to the mitigation of the effects of a biological attack, and potential improvements were identified. This part addresses in particular:

- techniques and technologies in the fields of detection, identification, protection and decontamination;
- available/existing prophylactic and curative therapeutic countermeasures.

The project also aimed at contribution to the improvement of resilience and mitigation of threat through a study of crisis management issues and a cross-evaluation of public health policies. The issue of communication and coordination between the involved actors was addressed and contribution was made to the education and training of hospital professionals and first responders through the development of a training kit. Major ethical and legal issues which could arise from the implementation of measures dedicated to the prevention or the response were also identified and discussed.

21. **U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 3-41 (JP 3-41),** Chemical, Biological, Radiological, Nuclear and High-Yield Explosives Consequence Management, 2006, http://www.fas.org/irp/doddir/dod/jp3_41.pdf ([JOP06])

This publication, prepared under the direction of the U.S. Chairman of the Joint Chiefs of Staffs, provides overarching guidelines and principles to assist commanders and their staffs in planning and conducting joint chemical, biological, radiological, nuclear, and high-yield explosives consequence management operations.

The document discusses the CBRNE Consequence Management Environment and distinguishes 3 situations where consequence management can be conducted: When Department of Defense (DOD) leads the operational response in reaction to an incident involving US forces and allies, across the range of military operations; to provide defense support to civil authorities in a domestic response, thus assisting Federal agencies within the US in accordance with the National Response Plan (NRP); or, to provide defense support to a foreign request. Detailed doctrine and guidance of action in each of these situations is provided.

It is stressed that understanding the effects of CBRNE on the population and the infrastructure is essential for the Joint Forces Commander (JFC) to apply the right resources at the right time. Even prior to being formally tasked to assist, the JFC should strive to develop full situational awareness with respect to the incident's cause to better understand the event's impact and to prevent further injury or harm to the civilian population or the responding joint force. According to a clear identification of roles – well-described in the document – he may then get involved in Crisis Management adopting a set of measures to identify, acquire, plan, and employ the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

For a Domestic Emergency, the National Response Plan guides the Federal response to any given emergency or disaster and most joint force CBRNE CM operations will be authorised as a result of the President declaring a disaster or emergency. The National Incident Management System forms the foundation for conducting domestic response operations and provides a consistent approach for Federal, state, local, and tribal governments to work effectively and efficiently together to prepare for,

prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. Domestic response operations consist of the five phases:

- Alert/Preparation/Situation Assessment.
- Deployment (with appropriate resources at appropriate timing).
- Support to Civil Authorities (in planned and synchronized manner)
- Transition of functions to civil authorities; and
- Redeployment.

Similar phases are distinguished in Foreign Consequence Management with the involvement and cooperation of the Hosting Nation's Authorities. In planning for CBRNE Consequence Management the importance of the following factors is highlighted:

- Assessment, together with local, regional and national responders, of the scope and magnitude of the incident.
- Coordination of operations with all involved actors, agencies, authorities.
- Providing logistic support
- Providing health services support
- Decontamination of civilians or military personnel.

22. **U.S. Armed Forces, Joint Chiefs of Staff, Joint Publication 1-02 (JP 1-02),** Department of Defense Dictionary of Military and Associated Terms, 2010, http://www.dtic.mil/doctrine/jel/doddict ([JOP10])

This document sets forth standard US military and associated terminology to encompass the joint activity of the Armed Forces of the United States in both US joint and allied joint operations, as well as to encompass the Department of Defense (DoD) as a whole. These military and associated terms, together with their definitions, constitute approved DoD terminology for general use by all components of the Department of Defense.

23. **VITA** (Vital Infrastructure Threats and Assurance), Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at EU-level, Deliverable D1.2, 2006,, 2006, http://vita.iabg.eu/index.php ([VIT06])

VITA is a project funded by the European Commission under the first call of the Preparatory Action in the Field of Security Research (PASR 2004). It was performed in the period December 2004 – July 2006 by an international consortium consisting of seven partners from six EU countries which were co-ordinated by IABG, Ottobrunn, Germany. VITA deals with the threat of Critical Infrastructures in Europe by natural disasters, manmade disasters and technical incidents, and addressing the protection of such infrastructures via realistic scenario and crisis management simulation, increasing the awareness and a sense of urgency on the need for CIP (Continuous Improvement Process) capabilities.

VITA aimed for delivering assessment on the threats to and assurance and protection of highly networked infrastructures, most of which are operating trans-nationally, and disruption of which is critical to Europe's security. In particular the project provided:

- Methods to raise awareness and a sense of urgency on the requirements for international critical infrastructure protection at both the European and national levels by developing, executing and analysing a scenario with national stakeholder participation
- A vision on methods, tools and technologies required for the protection (pro-action, prevention, preparation, incident response, and recovery) of critical infrastructures as

evaluated input to the preparation of the forthcoming European Security Research Program (ESRP)
- A demonstrator experiment of tools and technologies in a selected set of end-user applications for proving the feasibility and efficiency of the approach.

VITA developed a novel approach to risk assessment for critical infrastructures based upon a detailed, very complete, generic, and extensible threat taxonomy. The taxonomy starts with the distinction between natural and man-induced threats and proceeds systematically into further classification considering e.g. natural threats involving ground/soil (earthquakes, landslides), water, air, etc. The taxonomy can be tailored to the specific needs of specific critical infrastructure products and services stakeholders. It is noteworthy that the taxonomy contains only pure threats and that the actual actor causing the event that a threat becomes an incident has been unlinked from the threat itself. Moreover, the threat taxonomy allows the systematic identification of potentials for deliberately caused incidents, e.g., by activists and terrorist. The results of the project also include the analysis of human intent, including aspects of target and 'weapon' selection by activists and terrorists.

24. **US Department of Homeland Security (DHS),** National Infrastructure Protection Plan (NIPP), 2009, www.dhs.gov/nipp ([DHS09])

The National Infrastructure Protection Plan provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the U.S. critical infrastructure and key resources (CIKR) into a single national program. The is to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

The 2009 NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment.

The cornerstone of the NIPP is its risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to: set security goals; identify assets, systems, networks, and functions; assess risk based on consequences, vulnerabilities and threats; establish priorities based on risk assessments; implement protective programs; and measure effectiveness. The results of these processes drive CI/KR risk-reduction and risk management activities.

Sector-Specific Plans have also been developed and are available for the following sectors:
- Agriculture and Food
- Banking and Finance
- Communications
- Defense Industrial Base
- Energy
- Information Technology
- National Monuments and Icons
- Transportation Systems
- Water

25. **FEMA (U. S. Federal Emergency Management Agency),** National Response Framework (NRF), FEMA Publication P-682, 2008, http://www.fema.gov/pdf/emergency/nrf/ ([FEM08])

This National Response Framework (NRF) is a guide to how the United States of America conducts all-hazards response. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the Nation. It describes specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters.

This document explains the common discipline and structures that have been exercised and matured at the local, tribal, State, and national levels over time. It describes key lessons learned from Hurricanes Katrina and Rita, focusing particularly on how the Federal Government is organized to support communities and States in catastrophic incidents. Most importantly, it builds upon the National Incident Management System (NIMS), which provides a consistent template for managing incidents.

The Framework is written especially for government executives, private-sector and nongovernmental organization (NGO) leaders, and emergency management practitioners. It addresses five issues:

- Roles and Responsibilities: It is explained and focus comes on who is involved with emergency management activities at the local, tribal, State, and Federal levels and with the private sector and NGOs.
- Response Actions: It is described what the Nation collectively is doing to respond to incidents.
- Response Organization: It is explained how the Nation is organized to implement response actions.
- Planning: A Critical Element of Effective Response. Here it is emphasized the importance of planning and summarizes the elements of national planning structures.
- Additional Resources: An online NRF Resource Center, is foreseen, which is a new, actively managed DHS/Federal Emergency Management Agency Web site that will deliver state-of-the- art support for the Framework with additional support tools shaped by and addressed to the response community.

26. **AIRSECURE** (Risk-based detection and filtration system for airports against airborne chemical, biological and radiological hazards), 2007, http://www.3gfilters.com/airsecure ([AIR07])

AIRSECURE is a FP6 European Research project aimed at developing a high security detection and filtration solutions against airborne CBR threats at airports. The project was carried out in the period Sept 2005 – Sept 2007, with the participation of 7 partners from 5 EU Member States and the coordination of Lifa Air Ltd., Finland.

The project recognises the vital role of airports to the social and economic development of European countries. To help maintain the free flow of passengers and goods effective security measures are needed to improve the protection against new terrorist threats. The AIRSECURE system that has been developed, forms a reliable, user friendly and cost-effective solution to protect airport passengers and workers against airborne biological, chemical or radiological hazards. The modular system is realized based on risk analysis and it gathers together the important aspects of protection:

- Risk analysis methods for airborne threats in confined spaces.
- Combination of high efficiency particulate filtration with novel gas phase filtration to an advanced filtration unit that offers continuous and efficient protection against chemical and biological hazards.

- Low-cost particle detectors to monitor the performance of the filters to ensure the high protection level at all times.
- Distribution of the filters at high risk areas where protection is mostly needed.
- Utilization of distributed chemical detectors with central monitoring, to trigger alarms and to ensure timely response to imminent danger.

The main idea of the AIRSECURE solution was to combine promising new filtration technologies for removal of both biological and chemical agents with a protective filtration unit. These distributed units can be flexibly and quickly installed in the supply or exhaust air ducts of the high-risk areas. The very low flow resistance of the filter allows its installation without extensive modifications to the ventilation systems. New particle detectors will be developed to monitor the performance of the filtration system for maximum security. The optimum number and location of both particle and gas detectors and protective filtration systems are based on risk analysis. The secure air-filtration and advanced warning systems can deter the attacks, and reduce the effects of a CBR agent release by removing the toxic agents from supply air of the building.

27. **COPE** (Common Operational Picture Exploitation), 2010 ([COP10])

COPE is an on-going FP7-SECURITY European Research project under the Sub-programme Areas SEC-2007-4.3-02 Intelligent decision support and SEC-2007-4.3-01 Developing a common operational picture between regional and national authorities, first responders etc. The project, which is performed under the coordination of VTT, Finland, with the participation of 9 EU partners, is expected to be completed in January 2011.

The Common Operational Picture Exploitation (COPE) project will integrate COTS solutions and novel technologies to achieve a step change in information flow both from and to the first responder in order to increase situational awareness across agencies and at all levels of the command chain. A user-driven approach will be taken to develop new technologies for supporting user information requirements at the scene of the event.

First responders belong to a heterogeneous group in terms of crisis environments as well as roles, command structure, organisational and national differences. Therefore, the project will apply a wide range of human factors methods to better understand the processes of individual agencies to ensure that new systems both match requirements and can be integrated with legacy processes and technologies. COPE will use the skills and competencies of a strong team of research scientists both from industry and academia, of technology providers and systems integrators supported by end users.

28. **CORPS** – Cross Sector Observations of Threat Perceptions and Research Priorities for Biological Homeland Security in Europe, 2009, http://www.corpsproject.org/ ([COR09])

CORPS is a FP6 European Research project carried out in the period 2007-2009, with the participation of the Danish Centre for Biosecurity and Biopreparedness (CBB), Statens Serum Institut, and the International Peace Research Institute, Oslo (PRIO).

The aim of the project has been:

- To establish a network of professionals involved in security and European biological homeland security
- To analyse their security and threat perceptions in relation to the biological security threat
- To provide recommendations on strengthening R&D in European biological homeland security

The CORPS project has collected information on the perception of biological security threats from experts from the health, police, intelligence, defence, civil protection, government and research sectors across Europe. Information was acquired by means of two questionnaires distributed to these experts and recommendations are based on the findings from these questionnaires. A first observation is that the perception of biological threats in Europe appears much less likely than in the USA. Amongst specific recommendations is the need to develop best practices on biological threat assessment methodologies, the need to establish a permanent EU forum for biosecurity agencies, further identification professional scientific societies across Europe and their involvement in promoting responsible science and awareness in order to reduce the "dual-use" problem. Further sharing not only of practices but also facilities, e.g. BSL-4 laboratories, was proposed and the need for further conceptual unpacking of the societal resilience concept was highlighted.

29. **PATIN** – Protection of air transportation and infrastructure, 2007 ([PAT07])

PATIN is a European Research project carried out in the period July 2006 – October 2007, with the participation of 21 partners from 9 EU Member States, funded under the PASR 2005 Action. The project aimed to ensure the security of EU citizens by protecting the whole air transportation system against terrorist attacks, including airport, aircraft, critical ground infrastructure and the information system. The project will assess aspects of crisis management, interoperability and optimisation of security networks.

PATIN analysed all potentially relevant threats and technologies and a set of viable future operational concepts were derived from these. A conference and joint exercises with the stakeholder community (users and security organisations) have been organised to assess the operational concepts and the improved security provided. The project adapts a layered protection mechanism which forms a system-of-systems interconnected through networks. A top level network provides information for the whole of European air transportation. Local networks detect anomalies at airports followed by reactive and proactive measures against co-ordinated terrorist attacks. Issues of human factors, security implications of measures implemented, regulations as well as social and ethical values were also addressed.

30. **SeNTRE** – Security Network for Technological Research in Europe, Strategic research plan for security technology research, http://www.corpsproject.org/ ([SEN06])

SeNTRE started in December 2004 as a Commission-financed support activity under the Preparatory Action for Security Research. The objective was to prepare a proposal for a strategic research plan for European security by establishing and consulting a network of users and technology experts at national and European levels in support of, and to link with, the European Security Research Advisory Board (ESRAB).

Coordinated by ASD (Aerospace and Defence Industries Association of Europe) with the participation of 22 partners from the Industry, Research Institutions and Think Tanks, SeNTRE has developed:

- A strategic security research plan containing a list of prioritised short, medium and long term actions,
- A database of missions and technologies,
- An organized platform of users and technology experts for future consultation
- A methodology to organise and analyse the security needs at the operational level.

The SeNTRE support activity has delivered a strategic research plan for European security by establishing and consulting a network of users and technology experts at national and European levels, in direct link with the EC Advisory Board on Security (ESRAB) .The study, performed by a number of European organisations with relevant expertise, has provided the EU with a comprehensive input for planning its programme for security research (ESRP). SeNTRE has brought together a network of users from Member States and European organisations and through this approach it has made a major contribution to the security of the citizen in Europe. Politically, it has helped to develop support for the action and to build visibility. Technically, it has helped to achieve wider commonality of the best possible security systems in Europe. Organisationally, it has paved the way for an improved exchange between national and European levels through a network of security and technical experts.

At the heart of the SeNTRE methodology lays a double top/down / bottom-up approach to identify respectively the user/capability needs and the technology requirements through the following steps:

- Definition of security missions
- Identification of what security and security-related activities should comprise of
- Preparation and review of initial mission priorities
- Validation through capabilities workshops & security taxonomy
- Preparation of technology priorities
- Validation through technology workshops
- Preparation of a strategic research plan (Final result)

31. **IPSC – EC/JRC (Institute for the protection and Security of the Citizen)** – Research Strategy Paper - Emerging Technologies in the Context of "Security" -Issued in the Framework of Science and Technology Foresight, 2005 ([IPS05])

This report summarises the participation of the European Commission's Joint Research Centre in the road-mapping activities SeNTRE and ESSRT with the purpose to create a European Security Research Programme (ESRP) and the comprehensive strategic analyses made to define and prioritise these activities.

The analysis starts with the definition of the security model, consisting of possible targets, threats and countermeasures, according to CEN BT/WG 161 on Protection and Security of the Citizen. It then continues with a review of Standards for Security and the study of the missions for security. These include vertical and horizontal missions. The 7 vertical missions are:

- Protection of sites and infrastructures;
- Surveillance and control of borders and coastline;
- Protection of transportation
- Protection of distributed networks;
- Protection of the population;
- Disarmament verification – Weapons of Mass destruction;
- Foreign security operations

The 5 horizontal missions – which follow - are relevant for all 7 vertical missions:

- CBRN (prevention, detection, protection and decontamination)
- Human factors
- Economic and monitory protection
- Standards, testing, evaluation and certification
- Interoperability

For all the above missions, a number of issues have been examined and listed:

(i) Support measures
(ii) Support technologies or tools
(iii) Simulation and preparedness
(iv) Integration / validation

Following, a complete SWOT-analysis has been performed for each security missions, out of which specific research and capacity building needs have been identified.

32. **CEC (Commission of the European Communities),** Communication from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 final, 2004 ([CEC04])

This Communication gives an overview of the actions that the Commission had initiated on protection of critical infrastructure (CI) and proposes additional measures to strengthen existing instruments and to meet the mandates given by the European Council in July 2004.

After listing a number of threats and types of critical infrastructures as example, the Communication stresses the need to establish criteria and lists of European critical infrastructures, and the need to take specific measures to strengthen protection of CI. It therefore proposes a European Programme for Critical Infrastructure Protection (EPCIP) and the setting up of a Critical Infrastructure Warning Information Network (CIWIN).

33. **CEC (Commission of the European Communities),** Communication from the Commission to the Council and the European Parliament on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, 2006 ([CEC06])

This Communication sets out the principles, processes and instruments proposed to implement the European Programme for Critical Infrastructure Protection (EPCIP). The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective is achieved by the creation of an EU framework concerning the protection of critical infrastructures which is set out in this Communication.

The Communication clearly sets out that the protection of critical infrastructure is based on an all-hazards approach. The framework established consists of a procedure for identification and designation of European Critical Infrastructures (ECI), measures designed to facilitate EPCIP, CIWIN and information sharing processes, establishment of expert groups, support to Member States concerning National Critical Infrastructures, contingency planning, an external dimension and accompanying financial measures.

Based on this framework, a detailed work plan has been developed, which foresees 3 work streams:

- Consecutive EPCIP strategies. This work stream serves as the strategic platform for overall EPCIP coordination and cooperation through the EU CIP Contact Group.
- Protection of European critical infrastructure (ECI).
- Support concerning National Critical Infrastructures

34. **CEC (Commission of the European Communities),** Commission of the European Communities, Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, COM (2009) 273 final, 2009 ([CEC09])

This Communication presents and explains the proposed EU CBRN Action Plan, its overall goals and measures, together with its implementation plans.

The overall goal of the new CBRN policy proposed - which was based on the recommendations of a CBRN Task Force - is to reduce the threat and damage from CBRN incidents to the citizens of the European Union, by way of a coherent, prioritised EU CBRN Action Plan, which involves all relevant stakeholders, including industry representatives. Coherence and complementarity will be sought with relevant Community and CFSP instruments, in particular the Instrument for Stability10, the INSC and the IPA, which pursue CBRN risks mitigation and preparedness outside the EU, as well as relevant Euratom treaty provisions and secondary legislation.

This goal will be achieved by concentrating efforts and resources on minimising the likelihood of CBRN incidents occurring and limiting their consequences should they materialise. Some of the core measures to achieve these goals are:

- Deploying a risk-based approach to CBRN security in the European Union. This entails the use of risk-assessments to drive the prioritisation of security measures;
- Ensuring that CBRN materials are well protected and the potential for their diversion is limited;
- Strengthening the exchange of information between Member States on CBRN security issues in order to react more swiftly to emerging threats;
- Improving the development and use of detection systems across the EU; and
- Providing responders with the necessary tools to save lives and limit damage to property in case of CBRN incidents.

These aims will be achieved through the implementation of the 133 measures described in the EU CBRN Action Plan, which is part of the current policy package.

The Action Plan foresees three main areas of CBRN security work:

- Prevention - ensuring that unauthorised access to CBRN materials of concern is as difficult as possible;
- Detection - having the capability to detect CBRN materials in order to prevent or respond to CBRN incidents;
- Preparedness and response - being able to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible.

These three areas of work are supported by a number of horizontal measures, which are broadly applicable to all CBRN work.

35. **BMI** (Federal Ministry of the Interior of Germany), BMI-KRITIS - Protection of Critical Infrastructures – Baseline Protection Concept: Recommendation for Companies, 2009 ([BMI05])

This document, developed by the BMI responsible for internal security, provides guidance to companies considered as Critical Infrastructures, on their protection from all hazards (accidents, natural hazards, terrorist acts). The baseline protection concept provides companies in Germany with recommendations from the point of view of internal security. The document stresses that high security

of infrastructures in Germany is an outstanding quality asset to the country. It is in the fundamental interest of the country's enterprises and citizens to safeguard this standard of security in the long term.

The aim of this baseline protection concept is to reduce the vulnerability of critical infrastructures to natural events and accidents as well as terrorist attacks and criminal acts. In this context it focuses on building-related, organisational, personal and technical protection measures. The initial target group for the development of strategic concepts for danger analysis, risk management systems and risk minimisation measures is top level management at infrastructure operators, who should bear the business risk and, where appropriate, liability risks in case of contraventions. The security officers are generally the points of contact at the companies for implementation of these strategic concepts. Implementation of the baseline protection concept is ultimately a task for the entire business in question, requiring support from all levels.

The starting point is a multi-stage analysis and planning process covering identification of the given risks and a subsequent review, together with the adaptation of protective measures, where necessary. This process can be structured as follows:

- The establishment of danger categories, differentiated according to the areas of natural disasters, accident, terrorism/crime,
- based on the above, definition of the respective protection levels,
- the development of damage and threat scenarios,
- the analysis of weak points,
- the formulation of protection objectives as a basis for the definition of protection measures and counter-measures,
- definition of the required scope of action (coordination between public- and private-sector measures),
- implementation of the defined required scope of action and
- regular reviews of this analysis and planning process for the purposes of quality management.

# Annex B Abbreviation List

| | |
|---|---|
| ADM | Assistant Deputy Minister |
| AIRSECURE | Risk-based detection and filtration system for airports against airborne chemical, biological and radiological hazards |
| ASD | Aerospace and Defence Industries Association of Europe |
| ASSRBCVUL | Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis |
| ATC | Air traffic control |
| BIO3R | Bioterrorism, Resilience, Research, Reaction |
| BMI | Federal Ministry of the Interior of Germany (Bundesministerium des Innern) |
| BMI-KRITIS | BMI-National Strategy for Protecting Critical Infrastructures |
| BSL-4 | Biosafety Level 4 |
| CapTech | Capability Technology Areas |
| CBB | Danish Centre for Biosecurity and Biopreparedness |
| CBR | Chemical, Biological and Radiological |
| CBRN | Chemical, Biological, Radiological, and Nuclear |
| CBRNE | Chemical, Biological, Radiological, Nuclear and Explosive |
| CEA | Atomic and Alternative Energies Commission (Commissariat à l'Energie Atomique) |
| CEC | Commission of the European Communities |
| CEN | European Committee for Standardisation |
| CI | Critical Infrastructure |
| CIKR | Critical infrastructure and key resources |
| CIP | Continuous Improvement Process |
| CIWIN | Critical Infrastructure Warning Information Network |
| COPE | Common Operational Picture Exploitation |
| CORPS | Cross Sector Observations of Threat Perceptions and Research Priorities for Biological Homeland Security in Europe |

| | |
|---|---|
| COTS solutions | Commercial off-the-shelf solutions |
| CREATIF | Network of Testing Facilities for CBRNE detection equipment |
| CRESCENDO | Coordination Action on Risks, Evolution of Threats and Context Assessment by an Enlarged Network for an R&D Roadmap |
| DECOTESSC1 | DEmonstration of COunterTErrorism System-of-Systems against CBRNE terrorist acts |
| DEMASST | Demo for mass transportation security |
| DHS | US Department of Homeland Security |
| DoD | Department of Defence |
| DoDAF | Department of Defence Architecture Framework |
| EA | Enterprise architecture |
| EC | European Commission |
| ECI | European Critical Infrastructures |
| EDA | European Defence Agency |
| EOS | European Organisation for Security |
| EPSIP | European Programme for Critical Infrastructure Protection |
| ESEM | European Security Equipment Market |
| ESRAB | European Security Research Advisory Board |
| ESRIA | European Security Research and Innovation Agenda |
| ESRIF | European Security Research and Innovation Forum |
| ESRP | European Security Research Programme |
| ESSRT | European Security: General Roadmap for Security Research |
| ESSTRT | European Security: High level Study on Threats, Responses and relevant Technologies |
| FEMA | Federal Emergency Management Agency (US) |
| FoSs | Families of Systems |
| FP7 | Seventh Framework Programme |
| HE | High-explosives |
| IABG | Industrieanlagen-Betriebsgesellschaft mbH |

| | |
|---|---|
| ICT | Information and Communication Technology |
| ILO | International Labour Organisation |
| IMO | International Maritime Organisation |
| IMPACT | Innovative Measures for the Protection Against CBRN Terrorism |
| IND | Improvised Nuclear Devises |
| IPSC | Institute for the protection and Security of the Citizen |
| JFC | Joint Force Commander (US) |
| LE | Low-explosives |
| MS | Member states |
| MTS | Multidimensional Taxonomy System |
| NGO | Nongovernmental Organization |
| NIMS | National Incident Management System (US) |
| NIPP | US National Infrastructure Protection Plan |
| NRF | National Response Framework (US) |
| NRP | US National Response Plan |
| OCHA | Office for the Coordination of Humanitarian Affairs |
| OECD | Organisation for Economic Co-operation and Development |
| PASR | Preparatory Action for Security Research |
| PATIN | Protection of Air Transportation and Infrastructure |
| PRIO | International Peace Research Institute, Oslo |
| PSC | Public Safety Canada |
| PSEPC | Public Safety and Emergency Preparedness Canada |
| R&D | Research and Development |
| R&T | Research and Technology |
| RBC agents | Radiological, biological and chemical agents |
| RTO | Registered Training Organisation |
| SeNTRE | Security Network for Technological Research in Europe |
| SME | Small and medium-sized enterprises |

| | |
|---|---|
| SOREM | Committee of Senior Officials Responsible for Emergency Management |
| SoSs | Systems of Systems |
| STACCATO | Stakeholders Platform for Supply Chain Mapping, Market Condition Analysis and Technologies Opportunities |
| START | National Consortium for the Study of Terrorism and Response to Terrorism |
| STIB | European Security and Technological Industrial Base |
| STRAW | Security Technology Active Watch |
| SWOT-Analysis | Strengths, Weaknesses, Opportunities and Threats Analysis |
| TIC | Toxic industrial chemical |
| TIMs | Toxic industrial materials |
| TNO | Netherlands Organization for Applied Scientific Research |
| UNECE | United Nations Economic Commission for Europe |
| UNEP | United Nations Environment Programme |
| UNOCHA | United Nations Office for the Coordination of Humanitarian Affairs |
| VITA | Vital Infrastructure Threats and Assurance |
| VTT | Technical Research Centre of Finland (Valtion Teknillinen Tutkimuskeskus) |
| WHO | World Health Organisation |