[PRACTICE]

D3.1 SURVEY METHODOLOGY

PRACTICE WP3 deliverable

Dissemination level: ***public***

Nature: ***Report***

SEVENTH FRAMEWORK PROGRAMME

PREPAREDNESS AND RESILIENCE AGAINST CBRN TERRORISM USING INTEGRATED CONCEPTS AND EQUIPMENT

practice.fp7security.eu

Title:	D3.1 Survey methodology	
Date:	January 16, 2012	
Author(s):	Ingrid Bastings	TNO
	Clara Peters	TNO
	Jeroen Wevers	TNO
	Nathalie Vink	TNO
	With review contributions from all WP3 partners	

This project has received funding from the European Community's Seventh Framework Programme. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Community.

Summary Work Package 3

The objective of WP3 is to identify existing operational functions and (best) practices, training concepts, and standards used in Europe to prepare for, respond to, and recover from the effects of CBRN events. Other objectives are to identify ways in which EU member states and associated countries try to prevent CBRN events from happening, how they detect that an event is occurring, and how they discern between real events and hoaxes.

WP3 is divided in four different tasks:

- *3.1 Development of the survey methodology*

  A plan will be written to determine what operational functions for combating CBRN events are in use in Europe today. WP3 will propose a methodology for the work to be done and design deliverable formats.

- *3.2 Survey of operational functions*

  The goal of the survey on operational functions is to get insight in the current, existing operational functions on CBRN-events throughout Europe; its member states, institutes and organisations.

- *3.3 Development of an ideal set of operational functions and best practices*

  A list of ideal operational functions and best practices needed to prevent and overcome CBRN incidents, will be generated.

- *3.4 Evaluation of survey results and the ideal set*

  Evaluation and comparison of the survey results (3.2) and the ideal set of operational functions (3.3) will lead to identification of commonalities and needed improvements.

Work Package team:

Anders Sjöstedt	Umea University European CBRNE Center, UMU
Svenja Stöven	Umea University European CBRNE Center, UMU
Monica Endregard	Forsvarets Forskninginstitut, FFI
Hanne Breivik	Forsvarets Forskninginstitut, FFI
Ingrid Bastings	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek, TNO
Nathalie Vink	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek, TNO
Clara Peters	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek, TNO

Jeroen Wevers	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek, TNO
Kristian Krieger	King's College London, KCL
Ed van Zalen	Netherlands Forensic Institute, NFI
Marcin Smolarkiewicz	Szkola Glowna Sluzby Pozarniczej, SGSP
Tomasz Zweglinski	Szkola Glowna Sluzby Pozarniczej, SGSP

Contents

1. Executive Summary

The Survey methodology is the first task of WP3 of the PRACTICE project. This document is the result of task 3.1 and describes the methodology for the survey on operational functions. The following definition is used for operational functions: activities (tasks) that need to be performed (1) to identify and to actively counter CBRN threats and (2) to be prepared for, respond to and recover from CBRN incidents.

The goal of the survey on operational functions is to gain insight into the current *existing* operational functions on CBRN-events throughout Europe; its member states, institutes and organisations. To retrieve this insight, several components of this insight should be addressed:

- What do we need to know about the operational functions?
- How can we retrieve answers to these questions?
- Which parties in Europe carry out operational functions and should therefore be questioned?

In the survey methodology these questions are further explored and a division of work between the WP3 partners has been made regarding conducting the survey.

In this document, first a list of definitions and descriptions is provided, to 'set the scene' for this work package. A detailed description of the survey methodology will then be provided. The methodology will, at the end, propose the information to be gathered from whom and how.

2. Introduction

The objective of WP3 is to identify existing operational functions and (best) practices regarding the performance, training, concepts, and standards used in Europe to assess the risk of CBRN events and to prevent, prepare for, respond to, and recover from the effects of CBRN events or hoaxes.

WP3 is divided in four different tasks:

- *3.1 Development of the survey methodology*

  A plan will be written to determine what operational functions for combating CBRN events are in use in Europe today. WP3 will propose a methodology for the work to be done and design deliverable formats.

- *3.2 Survey of operational functions*

  The goal of the survey on operational functions is to get insight in the current, existing operational functions on CBRN-events throughout Europe; its member states, institutes and organisations.

- *3.3 Development of an ideal set of operational functions and best practices*

  A list of ideal operational functions and best practices needed to prevent and overcome CBRN incidents, will be generated.

- *3.4 Evaluation of survey results and the ideal set*

  Evaluation and comparison of the survey results (3.2) and the ideal set of operational functions (3.3) will lead to identification of commonalities and needed improvements.

The Survey methodology is the first task of WP3 of the PRACTICE project. This document describes the survey methodology, which will be used for identifying "current operational functions regarding prevention of, preparation for, response to and recovery from CBRN events and assessment of CBRN risks".

In this document, first a list of definitions and descriptions is provided, to 'set the scene' for this work package. A detailed description of the survey methodology will then be provided. The methodology will, at the end, propose the information to be gathered from whom and how.

3. Focus of WP3 - Definitions and descriptions

3.1 Security cycle

PRACTICE comprises the security cycle which involves five phases: threat assessment, prevention, preparedness, response and recovery (as is shown in Figure 1). The following definitions[1] are used for the phases of the Security Cycle:

Figure 1 Security Cycle

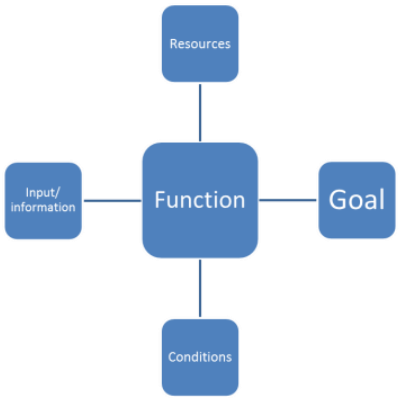
- Threat assessment: comprises an analysis of the actor(s), their capabilities and possible target(s).
- Prevention: prevent an actor from becoming a threat. This includes preventing an actor from obtaining/producing CBRN reagents and dispersion equipment.
- Preparedness: stop an actor from executing an attack, prepare and train responders, promote awareness and resilience within the general public in case of an incident.
- Response: first response directly after an incident and early diminishment of the effects of an attack.
- Recovery: recover people and repair damage; restore to normal situation.

The PRACTICE-project is a security (and therefore terrorism / intentional acts) focussed project. However it has been decided within the PRACTICE-project to not only focus the toolkit (that will be developed by PRACTICE) on intentional acts (terrorism), but also include accidents; a lot of the activities that are involved in preventing and/or countering CBRN incidents are the same. The security cycle which is described above can also be used when handling accidents, although certain phases need to be read slightly different (e.g. threat assessment would be replaced by risk assessment).

3.2 Operational functions

The goal of the survey on operational functions is to get insight into the current existing operational functions on CBRN-events. The following definition is used for operational functions:

Operational functions: Activities (tasks) that need to be performed (1) to identify and to actively counter CBRN threats and (2) to be prepared for, respond to and recover from CBRN incidents.



An operational function can be visualised as a process with four 'angles':

- First of all, by performing an operational function a particular **goal/effect** should be achieved.
- Particular **resources** will be needed to successfully perform a specific operational function.

[1] DECOTESSC1: EU FP7 security project 242294

- There are probably several types of **conditions** that need to be fulfilled in order to perform the operational function (e.g. victims need to be decontaminated before medical treatment can be performed).
- Advance **input/information** is needed to start a function and in order to successfully perform an operational function.

A very important aspect that combines all these four 'angles' is *communication* (and the information that is exchanged through communication) between all stakeholders and involved network parties.

4. Survey of operational functions

The goal of the survey on operational functions is to get insight into the current existing operational functions on CBRN-events throughout Europe; its member states, institutes and organisations. To retrieve this insight, several components of this insight should be addressed:

- What do we need to know about the operational functions?
- How can we retrieve answers to these questions?
- Which parties in Europe carry out operational functions and should therefore be questioned?

In the following text all four of these components will be further addressed.

4.1 What to ask?

The Description of Work on WP3 states that the survey should come up with a list of operational functions. It is the idea that 'only' a list with functions is not enough; to be able to address gaps and design concepts for the toolbox (WP4) a qualitative assessment of the current functions should be available. Below are some questions that might be asked to perform this qualitative assessment. Further tuning with WP4 and WP5 needs to be done.

- What is the goal of the operational function? And when is that goal achieved?
- Which organisations are involved?
- What is the trigger for starting the function, who is giving this trigger and what information is needed to get it started?
- What 'start-up' time is needed, what is the average 'time in production'? What scaling options are available for prolonging the 'time in production?
- What resources are used/ needed (human, technical, information)?
- What conditions need to be fulfilled to be able to perform the function?
- What if the goal of the function is not achieved? Who will be involved? What resources and conditions are needed then? What is the 'start-up' time?
- Which elements in the current functions need to be improved (what are things that are not optimized in the current way of performing this function)?

For comparability purposes a template has been developed for the answers to these questions. Since these forms are the output of the interviews – and therefore will be integrated in D3.2 – the template is made in such a way that based on the output the interviews cannot be traced and therefore the output stays anonymous.

4.2 How to question?

The survey will NOT start with a clean sheet; Annex A includes a (draft) set of operational functions. This set is composed, based on existing lists from the IMPACT-project, NL-national lists of functions, the ACRIMAS-project and DHS[2]. When performing the survey, this set of functions can be used as a 'baseline'. Note that the operational functions are not specifically CBRN functions; it comprises the activities to be performed under CBRN circumstances.

[2] IMPACT: EU PASR security project SEC4-PR-008000, Dutch project on MultiRespons CBRNe, ACRIMAS: EU FP7 security project 261669, DHS Target Capability List – September 2007

Obviously, there are numerous ways to retrieve information on the operational functions, from electronic surveys to 1-on-1 interviews. However, not every partner will be able to or comfortable with certain methods. Holding *interviews* with hand-picked people out of the personal network of WP3-partners have by far the preference. Suggestions for alternatives are:

- *Workshops* (national and/or aligned with CBRN-events to gather a more heterogeneous group)
- *Case studies* (CBRN-events, but also safety incidents)
- Desk study on *past and current EU-projects*, addressing similar topics
- *Written surveys*, preferably in combination with (telephone) interviews

The use of WP2 scenarios

The scenarios from WP2 can be used during the interviews and/or workshops to provide examples of possible incidents and to assess the differences between these incidents. For instance; does the response to an intentional incident differ from the response to an accidental incident? Is there a difference in performance of functions when addressing a C, B- or R/N-incident?

WP2 uses two national workshops to validate the scenarios and assess the consequences of the scenarios that are developed. It is to be expected that during these WP2-workshops a lot of information will be given about operational functions. To minimize the interference in the WP2-workshops with WP3-questions, it is suggested to have a minutes secretary present, who can record any interesting remarks that are made[3]. These can afterwards be integrated in the WP3 findings.

4.3 Who to question?

Within Europe several, different parties are involved with the operational functions for combating CBRN-events. It is the objective to question as many of these parties as possible, within the time and resources of WP3. Different parties are:

- Nations, including the first responder organisations (including local governmental/ municipal), crisis management organisations (including research institutes that perform specialized tasks) and policy makers
- Political bodies like UN (OPCW…), EU (MIC, RAS-BICHAT)
- Others, like vital Infrastructures, 'Industry' (possible targets), non-political bodies (NGOs), organizations that support victims
- Intelligence organisations (although this might be classified, it would be interesting for the prevention and threat assessment phase)
- Media
- If needed, organisations that deliver information to first responders (e.g. weather information)

The interviews will probably have a national focus, but in case a partner has contacts and knowledge of EU bodies it is highly recommended to extend the survey to the European level!

[3] All four partners of WP2 that are organizing a WP2-workshop are also participating in WP3. The WP2-workshops will probably held in the native language, which makes it hard for non-native speaker to attend the workshop and make notes.

Besides identifying which organisations that need to be questioned, it is also important to determine the organizational level that should be questioned. Our suggestion is to focus on the operational level, not being the actual person who is performing the operational function but the person who is responsible for the performance of the function on an operational level.

5. Who is questioning whom on what?

This work package includes seven partners. Given time, resources and expertise available at each of the partners, the workload described above is divided according to Table 1. Below more detailed information is given for each of the partners.

Table 1 Workload of interviews within WP3

	Threat assessment	Prevention	Preparedness	Response	Recovery
FFI		CRN*	CRN	CRN	RN
FOI			CBRN	CBRN	CBRN
KCL			CBRN*	CBRN*	CBRN*
NFI				CBRN*	
SGSP	CBRN		CBRN	CBRN	
TNO	CBRN	CBRN	CBRN	CBRN	CBRN
UmU		B	B	B	B

* means that only some of the operational functions in the specific phase will be explored upon.

FFI

Focus of the survey will be on four of the security cycle phases (all except threat assessment) and C, R/N-substances. For the prevention phase, FFI will focus on the function 'non-proliferation measures'. Based on FFI's contacts and knowledge, most interviews will focus on the preparation and response phase. Important sources for the recovery phase will be the Norwegian workshop (held for WP2) and historic events (e.g. Chernobyl).

FOI

FOI will explore all the letters of CBRN for three of the security cycle phases: preparation, response and recovery. To retrieve information on these functions, interviews will be held with first responders. An important source for knowledge on the existing operational function will be interviews.

KCL

KCL will focus on those functions which address crisis communication (communication with population, care for, create awareness) during the last three phases of the security cycle. KCL's output will mainly focus on UK experiences and some other countries (e.g. Poland).

NFI

NFI will focus on the operational function 'forensics' in the response phase, national as well as European wide. This will be done by the means of a written/electronic survey.

SGSP

Focus will be on the operational functions for three of the security cycle phases: threat assessment, preparation and response. SGSP will record information for all C, B, R/N and will retrieve information from other nations than Poland, given their international network. An important source of

knowledge on the existing operational function will be the Polish workshop which will be held for WP2.

TNO

TNO will retrieve information for all of the security cycle phases. This information will be based on national NLD experience, but also a desk research into historical cases and past/present EU-projects will be performed.

UmU

Given the expertise, UmU will focus on biological substances, for four of the phases (all except threat assessment). For those phases they will retrieve information from a selected set of EU-nations (based on differences between those nations that might affect how biological incidents are handled). Examples of these nations are Sweden, Greece and Germany.

I Annex I: Operational functions

Threat assessment

- Identify/trace suspected terrorists (suspected intentions and capabilities included)
- Conduct (national) risk and vulnerability assessment of areas and vital infrastructures/possible targets
- Determine alert state
- Trend watch on emerging threats

Prevention

- Apprehend suspected terrorists
- Track and trace (dangerous) goods (including securing storage and transport, continuous screening of water and food for CBRN contaminants, export control etc.)
- Enforce non-proliferation measures
- Execute anti-radicalisation programs
- Screen people (working at security related companies)

Preparedness

- Create redundancy in company processes (for possible targets)
- Create public awareness (for early warning and mitigation of effects)
- Monitor and protect vital infrastructures/possible targets
- Monitor (general) public health
- Execute capability assessment in relation to threat/risk assessment
- Develop and procure equipment and methodologies for first responders
- Develop and train emergency plans and CBRN protocols for first responders and crisis management organisations
- Develop plans to support incident command
- Develop communications network (for crisis management)
- Ensure interoperability between first responders and crisis managers (standard operating procedures)
- Establish (inter)national subject matter expert teams
- Cooperate and coordinate with international institutes/agencies to exchange information and experience
- Implement lessons learned

Response

General and situational awareness

- First alert
- Determine scale of incident, propagation in time, appropriate security zones and level of response
- Detect, sample, identify and monitor hazardous materials
- Determine cause and origin of incident, preserve evidence

- Check for and deactivate secondary threat (in case of intentional incident)
- Assess consequences for (public) health, infrastructure and environment
- Report to higher command
- Communicate with the media
- Involve (inter)national subject matter expert teams (for communication and assessment of information)

Environment

- Remove debris, (instable) constructions and vegetation (with the aim to reduce or prevent the risks resulting from the incident)
- Handle/dispose of contaminated waste
- Secure affected area
- Manage traffic (emergency transport, managing other traffic flows)

Organisation

- Coordinate crisis management organisations
- Scale up/down emergency response
- Control and monitor hazardous material on-site
- Command and control

Public care

- Search and rescue
- Manage casualties on-site (triage – treatment – stabilization)
- Decontaminate people, animals and vehicles
- Register and evacuate injured people
- Isolate infected people
- Treat patients in hospitals
- Distribute mass prophylaxis
- Organize (additional) medical capacity
- Register and take care of the deceased
- Warn population in surrounding areas
- Evacuate surrounding areas
- Register and trace exposed people
- Provide shelter, nutrition, water, sanitation and hygiene to evacuated people
- Register and handle belongings that were left behind
- Inform the general population
- Manage the public order
- Provide psychological care

Recovery

- Decontaminate infrastructure and environment (static)
- Clear debris
- Determine residual contamination level
- Reconstruct basic services (e.g. energy supply, telecom), infrastructure and environment (including private property)
- Provide long term health care (keep track of / conduct research on long term effects)
- Provide long term psychological care
- Restore first response capabilities
- Restore (trust in) society, government and economy
- Prosecute perpetrators
- Evaluate incident response and retrieve lessons learned

II Annex II: Results report template

See also Excel file '*D3-1 Template.xlsx*', which contains the electronic version of the template and is used for reporting results of the survey.