European Commission
Enterprise and Industry

EU Workshop on Chemical, Biological, Radiological and Nuclear Research (CBRN),

9-10 November 2010, Brussels

Final report

Ruud BUSKER, FP7 Security Advisory Group, TNO, NL
Tristan SIMONART, Security Research Unit, EC DG ENTR

January 2011

Workshop on Chemical, Biological, Radiological and Nuclear (CBRN), 9-10 Nov 2010, Brussels

Executive Summary

This first 1.5 day EU workshop on CBRN Research organized by the EC (DG ENTR) was well attended with 124 participants from 21 countries including many representatives from end user organizations.

Major outcomes: first of all, in **session 1 on EU institutional stakeholders**, the high added value of continuous information sharing and cooperation between EC services sharing CBRN responsibilities (HOME, JRC, SANCO, MOVE, RTD, ECHO, RELEX and AIDCO) and the EDA on civil-military dual research has been well confirmed by all speakers and participants. Session 1 also demonstrated the internal and external dimension of CBRN (e.g. Regional CBRN centers of excellence).

Secondly, **session 2 on end users** has enlightened the essential role and responsibility of end users, early on in the CBRN research activities (design, specification, testing, validation, training, field exercises). Experience from incidents needs to be shared, although classification makes that difficult. Integration of field and real exercises are crucial to make applications accepted. Equipments and systems must be simple, robust, easy to use and affordable (cost and procurement feasibility). Solutions should be acceptable at the citizen level, respecting their privacy and rights. **Civil protection forces and first responders** are key stakeholders in this process. Sharing of information from intelligence databases and expertise has also been recognized.

Finally, **session 3 on demonstration activities** revealed the way to a demonstration program on CBRN(E), with a key conclusion being that coordination between all CBRN stakeholders (prevention to recovery) is crucial. The examples of existing and recent CBRN(E) regional/national clusters or platforms are quite interesting and could pave the way or contribute to such a challenging program.

Report annexes include recommendations for R&D priorities and possible 2011-2012 follow up workshops.

Table of contents

Introduction

Chair: Ruud BUSKER, FP7 Sec Adv. Group, TNO, NL

Chemical, biological, and radiological incidents, be they intentional or accidental, remain major threats to Member States for the coming decades. Earlier strategic initiatives such as ESRAB and ESRIF underlined the relevance of CBRN threats and the role of R&D therein. It was decided to organize a workshop on CBRN in order **to develop a sharper insight into the link between end users needs and R&D**. This first FP7 CBRN workshop organized by the European Commission (DG ENTR) focused on 3 objectives, addressed in dedicated sessions. The workshop drew a lot of attention; registration requests exceeded the available places. Overall there were 124 participants from 21 countries, including 19 participants from EU institutions. The audience and speakers, roughly evenly distributed, represented policy makers, CBRN end-users, R&D, industry and press.

The CBRN security field is characteristic for having a very low occurrence rate but high impact. As in many fields in security, the citizen plays an important role. The unpredictable outcome of incidents with toxic chemicals, radioactive substances and pathogenic micro-organisms affects the society. There will be immediate consequences such as casualties, but (disproportional) reactions due to uncertainty and panic will add up to disruption. The citizen is also on the receiving end when it comes to building counter-capabilities, not only in the sense of costs, but also to some extent in losing privacy and being faced with burdensome security measures.
The low incidence further implies that hands-on experience for response organizations is relatively low. Yet, the CBRN threat is becoming more and more unpredictable in the sense of actors, targets, scale, agents and means of delivery. This development calls for an adaptive approach, but not necessarily for development of dedicated CBRN systems, but rather for seeking to develop and subsequently implement CBRN solutions into existing and developing

security systems: an all hazard approach. Early involvement of users should be ensured. It is the task of policy-makers to design a proportional level of preparedness, taking into account financial as well as societal aspects. More particularly there should be clear guidelines and incentives for industry as CBRN security might be an area with a high market failure risk. Specific information on threat development is usually classified. Therefore the R&D community must have good interfaces with the intelligence community and must be able to work in a restricted secure environment. This adds up to the CBRN paradox: classification versus the need to share information, R&D efforts and facilities.

CBRN Workshop session-1

The main purpose of the first session of the CBRN workshop was to provide an overview of the CBRN research related activities taking place in the EU institutions. The session therefore brought together representatives from a large number of Directorates General such as; DG ENTR, DG HOME, DG SANCO, DG MOVE, DG JRC, DG ECHO and DG RELEX.[1] Additionally representatives from the European Defence Agency and the European Council presented their initiatives in the CBRN area.

Moderator: Gwyn WINFIELD, CBRNE World UK
Rapporteur: Christophe CASTEX, DG ENTR

A considerable number of actors underlines the complexity of the CBRN landscape in the EU institutions. For some actors the main interest in CBRN lies in the EU humanitarian aid across the world, for others the focus lies in the security of the mass transport systems from CBRN attacks while the main interest of the policy oriented Institutions is the implementation of the EU CBRN action plan.
The initial assessments of this session were that:

- The embedding of CBRN related issues in the EU institutions is a complex matter
- CBRN is a very broad/horizontal area, which concerns a wide array of actors
- The lines between the different sectors are increasingly blurred. (civilian, military, health, crisis management, transport, sanitation)

Nearly all those actors can however be categorised to some extent based on their main orientation:

- The FP7 SECURITY Research DG ENTR
- Policy oriented DG's like HOME, SANCO and MOVE,
- DG JRC with its own research facilities and international research activities in the RN field),
- End users oriented DG's like ECHO, EDA and RELEX/AIDCO,
- Intergovernmental institutions like the European Council.

This relative fragmentation of CBRN research related responsibilities across different DG's harbours a certain danger of duplication as well of efforts as of finance. It is therefore crucial to establish a mutually coherent approach between the various actors. Only through a cross-

---

[1] ENTR stands for Enterprise and Industry, HOME stands for Home Affairs, JRC stands for Joint research Centre, RELEX stands for External Relations, DH ECHO stands for Humanitarian Aid and Civil Protection, SANCO stands for Health and Consumers, Move stands for Mobility and Transport.

cutting and comprehensive coordination can we guarantee that all relevant actors are taken into account.

The subsequent question that arises is: how can the different actors benefit from each other? Each actor has a limited set of capabilities and/or financial resources which need to be streamlined and brought together. The Policy DG's can provide the legal framework, share their respective networks and establish the links to end users.

The Research DG's can provide funding and develop the needed technologies. Furthermore they can support the European industry through an enhanced "research to market" dimension. In this context DG ENTR has already achieved considerable results in the integration of topics from the EU CBRN Action Plan. Another fruitful example of cooperation is the ongoing European Framework Cooperation (EFC) between DG ENTR and the European Defence Agency to ensure complementarity and avoid the funding of similar projects.

This session clearly underlined that the EU needs a common approach to the issue of CBRN research. The EU has an impressive number of actors and capabilities in the field of CBRN that must to be brought together and coordinated in order to work in an efficient way.

CBRN Workshop session-2.

Central question of this session was: how can it be ensured that end users engage fully with those carrying out the research, enhancing the challenging link between CBRN operators, being the demand side, and beneficiaries, the supply side?

The objective was to focus the discussion on defining orientations and recommendations that contribute to improve the dissemination, transfer and take up by final users of research results.
Part 1: 'CBRN Detection, identification and forensics:
Moderator: Chaim RAFALOWSKI, FP7 Sec Adv. Group, Magen David Adom, IL
Rapporteur: Rob DUIVEN, National Coordinator Counter-Terrorism, NL

All presenters touched on the issue of ensuring that end users engage fully with research. Many different approaches and solutions were given.

• Threat or intelligence or scenario driven
• Innovation or technology driven
• Operational requirements driven
• Policy driven (EU CBRN policy/policies, FP7)

There was agreement that a proportional mix of short / mid / long term requirements is necessary in alignment with research efforts. No single solution will serve all goals, however generic good practices need to be shared and integrated into a next generation approach. End-users should be involved in R&D in accordance with the following aims:

• As soon as possible:
    o Helping to defining scenarios and sets of requirements (BBK, CEA)
    o Join in Programme Partnerships etc. (BBK, CEA)
• As close as possible
    o Linking operational experience with R&D and training & exercises (CENTREX, Thales, discussion)
    o Testing, determine practicability / applicability, accessible handbooks, realistic modelling, training (CEA, BBK, discussion)
• As flexible as possible

- o Incorporate changes in threat and risk(perception) (Anderson, CENTREX, discussion)
  - o Take into account changes in modes operandi (CENTREX, Anderson)
  - o Take note of lessons learned & shared (CENTREX, Thales, discussion)
- As focussed as possible (end user and R&D)
  - o Focus on real life use (first responders and military)
  - o Efficient matching operational needs & intelligence with innovative research (CENTREX)
  - o Limited resources, available knowledge & experience (CENTREX, Thales, discussion)
- As mutually beneficial as possible
  - o E.g. using NATO-models and other dual-use potential (discussion)
  - o Focus in funding needed, EU policies/activities and FP7 (discussion)
  - o Use of /setting up databases & sharing the information therein (CENTREX, Thales)

The main focus of the second part of session 2 was to identify and to describe the needs and requirements of end-users regarding protective equipment, medical countermeasures and decontamination procedures.

Moderator: Chaim RAFALOWSKI, FP7 Sec Adv. Group, Magen David Adom, IL
Rapporteur: Roman WOELFEL, Bundeswehr Institute of Microbiology, DE

BULL provided an overview of the Hazardous Area Response Team (HART) project. HARTs are paramedic teams who have received additional training and equipment to perform patient care in difficult circumstances, including after CBRN incidents. Hazardous area response teams are available at 12 sites in England and have been successfully employed in several real-life incidents as well as in large CBRN exercises. Interaction between SMEs and paramedics was supported to ensure research is prioritized against user requirements. Suppliers were focused on HARTs needs and improvement of the user experience was at the centre of the research process. For example, an innovative web based tool, designed to collect incident data and recordings including an E learning platform with the ability to support wider ambulance emergency preparedness was explained. The presenter suggested a common evidence based standard for end user requirements, as well as a common evidence based approach for human decontamination as a main focus for future research.

GESRET described the national civil CBRNe defence in France. Structures and organization of CBRNe response are closely linked to the general French administrative structures. Based on the experiences gained from on-going projects it was concluded, that end-users should not be considered as the first test subjects for a final product. Real end-user needs should be identified at the start of the research program and the equipment resulting from research programs must meet their requirements, especially concerning simplicity, efficiency in real field conditions and robustness.

BIEDERBICK described a case of viral haemorrhagic fever imported to Germany in 2006. The severely ill patient travelled from Liberia via Belgium to Germany and came in contact with several hundred people until he was eventually diagnosed with a Lassa virus infection. Although the patient survived the disease, his recovery took 12 weeks of treatment in the isolation ward. BIEDERBICK proposed to intensify research on diseases like these. Quality and comfort of protective equipment should be further improved, as well as point-of-care diagnostic tools. Attention for guidelines and legalisation concerning the transport of highly contagious patients was suggested.

CABRIA started his presentation with a description of the forensic aspects in the CBRN detection process, followed by an overview of existing CBRN capabilities and needed improvements in Spain. Integrated detection systems and modelling systems for CBRN incidents were pointed out as most relevant. In addition, national and European research efforts should focus on deployable CBRN lab capacities and programs for standardized CBRN reagents and joint CBRN databases.

In the last presentation RAFALOWSKI described the CBRN defence preparations of Magen David Adom (MDA), Israel's national emergency medical service (EMS). In contrast to similar services in other nations, all employees get specifically trained for CBRN incidents. PPE and chemical antidotes are available in nearly all MDA ambulance vehicles. Taking into account the expected panic reactions of patients in a mass CBRN event, MDA EMS personnel will immediately act in the contaminated area, instead of waiting for more specialized personnel and equipment. Disrobing is considered as the most appropriate way of initial decontamination. A more intensive wet decontamination will be conducted at the hospital's gate. Several suggestions for further projects in CBRN preparedness were given: future research should be focused on a better understanding of CBRN threats. This should lead to a more precise description of the feasibility and the consequences of CBRN defence concepts for decision makers, to make preparedness and response plans more focused.

In the subsequent DISCUSSION, several participants of the workshop emphasized the importance of a transnational, European wide standardization in the CBRN field. Additionally it was suggested to harmonize technical requirements for detection of CBRN agents, including definitions of safety thresholds for detection and decontamination procedures.

CBRN Workshop session-3

FP7 CBRN Demonstration program: The way ahead, defining a roadmap for a large research demonstration program on CBRN, in conjunction with the 2 ongoing feasibility projects DECOTESSC1 and CBRNEMAP
Objective: contribute to define the way ahead for the foreseen CBRNE research demonstration program.

Moderator: Tristan Simonart, DG ENTR
Rapporteur: Maria Spulber, REA

SELLSTROM presented CBRNE-MAP, a roadmapping study of CBRNE demonstrator – phase 1. Three communities are involved in the project: end users, researchers and industry representatives. The work packages include:
- end-users decide what technologies and capabilities are needed
- scenarios are formulated by an end-users group
- technologies and risk and threat
- final deliverables-the roadmap and the concentration on technologies that although not mature are needed for the future-let the EC know about them

Generally, the practice is to deal with an event after it has happened. The project aims to find ways to improve the system. One ought to suggest what could have the greatest impact-would it make a larger difference if we could create a market for CBRN? Should we concentrate our money on training? How would that affect the totality of the CBRNE area? We should look at where the EC money is used and where it might be more useful. There is a need for modeling and simulation to better handle and process information.

NIEUWENHUIZEN is coordinator of DECOTESSC 1 – Demonstration of counter –terrorism system of systems against CBRNE phase 1. Aim of the project to analyze a European Integrated CBRNE counterterrorism system-of–systems: definition of the whole system, ideal system-of-systems against CBRNE threat, current situation, gap analysis, strategic roadmap for phase 2 and beyond, proposal of suitable demonstrations during phase 2).

A system-of systems approach is needed to deal with the complete system instead of parts. Three dimensions need to be dealt with: the security cycle, an all hazard approach and multi effect levels (direct as well as long-term societal effects). The final product is the strategic roadmap:

- Outlines all the necessary missions, tasks, capabilities, systems, technologies, etc. to be considered.
- Focuses on integrated operational competences rather than on R&D only.
- Demonstration program is the first step in realizing and ideal system.

Some preliminary results identified the dilemma of sharing of scare and confidential information and stressed the importance of multidisciplinary and international approaches. Integration of the chain elements means including many elements, other communities outside CBRN and the entire of counter-terrorism system. Finally in the recovery phase, after care and psychological plus ethical aspects are very important.

Both projects do have an active interfacing, even considering a joint symposium but it is important to keep the 2 projects separate to have cross-validation.

KELLY put specific emphasis on human behavior; ethics is becoming increasingly important in FP7

From the perspective of an SME to get involve din FP7 is quite difficult. In his view there are 2 strategies:

- Wait for the publication of the working program
- To get involved in the European R&D community; like this waiting for the working program will be a formality

He presented some examples, the IMOSEC project, aiming at providing as much security as is needed and suitable for all stakeholders. The project will provide a scoring matrix identifying the level of security for routes etc. and human behavior is the third vector. The upcoming project PRACTICE will deliver an improved system of tools to deal with CBRN attacks/crisis (terrorist or not). Training kits for the public and first responders are included. The first exercise of the project will be in a crowded indoor facility will be the set up of the field work in the UK. The recovery phase will also be looked at during which the public is weary although not in immediate danger anymore.

PEKKALA introduced the Finnish CBRN Cluster initiative. In response to the recent changes in the CBRN marketplace, networking and more intense inter-company co-operation, thus establishment of an alliance called CBRNE-Finland together with authorities and research institutes was considered the way to go. CBRNE-Finland will create conditions / possibilities to connect needs and demands, standards, R & D, experimentation, tests, results, funding in order to create ready-made, tailored products (solutions, models, systems) for international markets. The goal is to get the ideas from the end-users and then the others try to get good products for these. The idea is not to create a piece of equipment but to find more tailored solutions.

DODEMAN suggested the road to a European CBRN demonstration project. Aim is to provide a system of system solution for CBRN resilience of the society, critical infrastructures

and public places, including integrated CBRN surveillance and protection system; the situation awareness; a prevention, detection, response and recovery capacity. Central is to achieve a real capability and integrated approach which bridges the gaps between the needs - mainly of the end-users and stakeholders (first responders, fire brigades, law enforcement officers, emergency units, public authorities). Major issues to be considered:

- Detection paradigm and timeline: detect to protect, detect to warn or detect to treat;
- Subway, airport, city and nation concept
- Characterization or airflow and transports of contaminants in urban areas (indoor and out door);
- System approach and decision tools for rapid response and recovery

A number of operational and technical challenges has been identified, such as permanent and advanced surveillance of crowded places and critical infrastructures.

WILLIAMSON (Canada) gave a presentation on the approach of the Canadian government. They launched multiple program elements spanning a range of Technology Readiness Levels to investigate and develop emerging technologies, to demonstrate concepts and technologies to responders and to accelerate technologies towards commercialization. The full-spectrum event continuum is a particularly useful way of mapping operational and policy drivers (strategies, action plans, regulations etc) across identified capability areas. It is tailored to terrorist events but it can apply to any event: e.g. disease outbreak, earthquakes.

The DISCUSSION of this session focused on needs and priority topics drawn from the presentations:

- There should be clearer and more uniform understanding to what extent to address CBRN versus CBRN-E
- Need to clarify the definition and the involvement of the whole CBRN system: from prevention to recovery
- The community should learn from other system elements in a "system of systems": sharing information and yet deal with classification etc.
- Identify the existing gaps and find improvements
- Involvement of users, industry and R&D in development of solutions using concepts such as field labs
- Simulation programs
- Involvement of social scientists and end-users from social sciences
- Added value of CBRN action plan: protection of the supply chain, medical countermeasures, forensics, biological and chemical strategic reagents (probes, primers, strain), standardization and harmonization for testing (interoperability of the sensors)

CBRN Workshop Overall conclusions

Out of the logical sequence of sessions, some overarching conclusions can be extracted.

There is a need for better <u>coordination</u> on many levels including that of R&D. Whereas DG ENTR has the lead in the FP7 Security theme, each of the other EU institutions has expressed R&D needs and some do have activities. Specifically:
- **Timelines of the demand and supply side need to be better coordinated into short term versus long term needs**
- **Although it is realized that some R&D efforts have long time constants, there should be attention for development pace, which could include launching of quick projects**
- **Time for projects to start is very long due to administrative limitations which need to be carefully assessed**
- **There are many exemplary national approaches which should better flow into EU efforts. Some of those have been presented and the benefit and best practices should be investigated.**
- **An important multi-national benefit can be found in developing a CBRN preparedness & response blueprint for high attention events such as summits or sport events.**

There is a commonly agreed need for intensified <u>sharing</u> of information and experience. Special attention in this sense is needed for:
- **Information gathering, needs intelligence capabilities but also needs up-front support from technical experts to allow a more efficient way of looking and searching.**
- **Sensitive information, which needs to be shared at some level. R&D may be helpful in designing ways to deal with this.**
- **Filtering: as early and efficient as possible divide sense from nonsense and distribute information to the proper channels.**
- **Lessons identified**
- **Standards, both for operations, data sharing as well as testing and evaluation**
- **Training (simulated or not), use of serious gaming tools**
- **Databases (projects, activities, incidents)**
- **Networks (intelligence, operations, laboratories)**

In the workshop a serious plea was recorded for better <u>interfacing</u> between policy-makers, users, the R&D community and the security related industry. Several national initiatives were presented; analysis of best practices would give guidance for a holistic approach containing
- **Scenario based (GE) and/or Capability based (CAN)**
- **Feed-in loops (NL)**
- **Exercises (many)**
- **Field labs (ambition)**

Special attention was drawn to the acceptance of solutions in many senses. A system of proportional solutions would need to consider:
- **Affordability, including innovative ideas to develop multi-purpose equipment**
- **The interest of the citizen, respecting aspects such as civil rights and privacy**

End users should be 'obligatorily' involved in R&D and procurement from the early onset on. It must be realized that user defined requirements involve:

- **Simplicity in use, realizing that many end-users have a complex variety of operational tasks and limited time for dedicated CBRN training and exercise.**
- **Definition of needs, having a clear sense of reality, standardization, robustness and operational limitations**
- **An up-front defined follow-up of research: application and implementation must be clear before R&D starts**
- **Exercises, training and demonstration of systems in the prototype phase**

ANNEX-1A : Recommendations for R&D priorities

1. **Establishment of CBRNE R&D cross border expert clusters/platforms or field labs.** These would include representatives of first responders, researchers, industry & SMEs, authorities. They should play the role of providing :

   a. advice on CBRNE research needs (prevention, protection, detection, resilience, recovery). Field labs for ex. mimic realistic environments, under controlled experimental conditions, where research, industry jointly evaluate systems already in the prototype phase, and where input and needs from users are easily adapted.

   b. recommendations for the implementation and demonstration of CBRNE activities including testing/ validation/ exercises and training.

   (*examples described at the workshop: CBRNE-Finland/ CENTREX CBRNE, NL / FR joint ministerial CBRNE research program …*)

2. **CBRNE INTELLIGENCE sharing**. Feasibility study on the exchange of CBRNE intelligence information between existing databases in the different regimes (e.g. NSG, MTCR, AG and WA). Development of a database of CBRN databases. A custody-holder for such an overarching database should be appointed, possibly JRC.

3. **CBRNE AND TRANSPORT**: Developing an Incident Response Guide for CBRNE incidents in crowded urban transport conditions. This should consider planning, cooperation, conducting exercises, training.

4. **CBRNE MEDICAL RESPONSE**. Developing a common evidence based approach for people decontamination, either clinical or 'mass' public.

5. **SAMPLING FOR FORENSICS**. Development of standard or interoperable forensic protocols for sample collection, preparation and transport (including containers easily handling with protective suits). The role of forensics in CBRN is twofold, it contributes to the preparedness phase in delivering information to security services, it also yields evidence for prosecution. In close communication with EDA, forensic CBRN capabilities need to be improved.

6. **CARGO SCREENING.** There is urgent need for rapid high flow screening means for closed packages and cargo.

7. **ACCEPTABLE CBRNE RISKS LEVELS.** Review of existing legal standards, incl. definition of acceptable CBRNE risk levels.

8. **Development of DECISION SUPPORT TOOLS** for CBRNE counterterrorism. Involves modelling and simulation of the CBRN chain from an incident scenario database, including application of detection and protection, predicting the outcome in the sense of casualties and damage as well as of the effectiveness of countermeasures to be taken.

9. **CBRNE GAMING**. Requirements for serious gaming to be used as tools for creating awareness and high level training purposes.

10. **"C" FIELD EXPOSURE DIAGNOSTICS**. Methods for on-site application of diagnostics for exposure to chemical agents. The goal is to rapidly identify the causative agent in a remote environment prior to onset of symptoms.

11. **STANDARD "B" POINT DETECTIONS**. Develop standard protocols for testing and evaluation of point detection systems for biological agents. Should include description of testing equipment, how to measure detection characteristics, reference materials.

12. **MASS and CROWDS unpredictable reactions.** . CBRN threats, hoaxes and incidents typically involve reactions of society which are difficulty to predict let alone control. Mass hysteria may heavily complicate any incident which involves unconventional and invisible stuff such as chemicals, radioactive substances and pathogens. There is too little knowledge in this area.

ANNEX-1B: Recommendations for subsequent CBRN workshops

Workshop on CBRNE research achievements: A second workshop dedicated to achievements of individual completed or currently running FP7 EU projects, possibly including others like EDA CBRN projects. To stimulate dissemination and offer the opportunity to share knowledge, insight and experience, a number of projects will be invited to present their findings and best practices. An additional aim would be to make a synthesis out of the projects. This will also involve projects on 'explosive', so CBRNE.

CBRNE Industry and innovation workshop: Whereas in the first workshop (EU) stakeholders, end users and R&D were invited to share their vision, a next workshop may invite industry to give their view on future developments and on industrial policy with regards to CBRN.

The advise is also to organize a small number of thematic workshops on themes that thus far received little attention:
- **Workshop on CBRNE Hazard management**, including decontamination of larger crowds
- **Workshop on Medical countermeasures** and feasibility of Security R&D
- **Workshop on CBRNE intelligence sharing**

ANNEX 2: Programme and presentations of speakers

See: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4574

ANNEX 3: List of Participants

See: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4574