Ex-post Evaluation of PASR Activities in the field of Security and Interim Evaluation of FP7 Security Research

CBRN Case Study

January 2011

Centre for Strategy & Evaluation Services

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk

Contents

Introduction

1

1.1 7th RTD Framework Programme 2007-2013

The 7th Framework Programme for Research and Technological Development (FP7) for the period 2007-2013 is the EU's main instrument for funding research and development. FP7 has a budget of €50.5 bn over 7 years. The RTD FPs are a key tool in achieving the aims of the Europe 2020 strategy, which includes *'smart growth: developing an economy based on knowledge and innovation'* as a key priority. The objectives of FP7 have been grouped into four categories: Cooperation**,** Ideas**,** People and Capacities**.**

1.2 EU Security Research and CBRN

Following the successful implementation of the PASR Preparatory Action on Security Research in 2004-2006, an EU Security Research programme was included for the first time in the RTD Framework programme in FP7, with a budget of €1.4bn from the European Commission. FP7 Security Research is part of the Cooperation objective, which fosters collaborative research across Europe and with other Associated States and partner countries.

The programme's objectives are to: make Europe more secure for its citizens, strengthen industrial competitiveness; promote research excellence and state-of-the-art; prevent the fragmentation of research efforts and strengthen critical mass in particular areas of security research. Among the specific objectives include: stimulating the development of a European market for new and emerging security products and systems; ensuring the security of EU citizens from new and emerging threats; delivering mission-oriented research results to reduce security gaps; ensuring the optimal use of available and nascent technologies and stimulating cooperation between providers and users of civil security solutions.

An important area of intervention in both FP7 Security Research and in the PASR Preparatory Action was funding for **Chemical, Biological, Radiological and Nuclear (CBRN).** It has been addressed in a number of work programmes. The extent of continuity between calls under PASR and FP7 SEC is summarised in Appendix A of this case study.

1.3 Case study methodology and structure

The case study outlines the main challenges faced by relevant authorities at European and national level in the area of Chemical, Biological, Radiological and Nuclear (CBRN). The various ways in which PASR and FP7 Security projects contributed to progress in improving the detection, identification and monitoring of CBRN materials, promoting standardisation in the area of testing and certification and improving strategies for prevention, preparedness and response to malevolent use of CBRN are highlighted.

The case study was prepared using a combination of desk research and field work. An interview programme was undertaken with a number of lead project coordinators and partners and with relevant Commission officials responsible for CBRN. In addition, project officers responsible for monitoring the implementation of PASR and CBRN projects were carried out.

Section 2 - provides an overview of the policy contextand the main issues relating to challenges and threats in the CBRN field;

Section 3 – examines projects that were supported through PASR and FP7 Security in the CBRN field

Section 4 – outlines conclusions, and reviews progress towards the achievement of objectives.

Policy Context and Key Security Issues 2

In this section, the nature of the threat posed by CBRN to EU internal security in general, and EU citizens in particular, is examined. The EU policy and regulatory context is then outlined.

2.1 CBRN – review of threats and challenges

There are various aspects to the CBRN threat, however policy makers and relevant security agencies are primarily concerned with terrorist groups whose intention is to acquire and carry out CBRN attacks on crowded public areas.

There is a consensus among academics and experts in the field of counterterrorism that ongoing globalisation processes are changing the nature of warfare together with the increasing threat from global networked, decentralised and outsourced terrorist groups who are prepared to use CBRN materials no longer as a means to achieve political objectives but as an end in itself. There is a growing need to protect society from potential future scenarios in which CBRN materials might be deployed by **unconventional means of delivery.** This will require cooperation between governments, counterterrorism officials and counter-proliferation agencies.

Since the terrorist attacks of September 11th 2001, there has been a proliferation of extremist groups whose explicit intention is to engage in high profile and **sophisticated attacks targeting civilians** that include the use of CBRN together with stolen or rudimentary Weapons of Mass Destruction (WMD).[1]

While only states have hitherto possessed a monopoly on the facilities and investment required for the weaponisation of CBRN materials, there are signs that a **black market** in the distribution and sale of WMD has emerged. Furthermore, there is continuing concern regarding the lack of adequate security for traditional biological and nuclear weapons sites in the former Soviet Union. One of the most important threats comes from the spread of technical knowledge and capabilities that can enable dedicated individuals or groups to build CBRN devices.

The level of threat from terrorist attacks using CBRN varies depending on the chosen agent, technical expertise of the user and the means of delivery available to terrorist groups. Toxic and cyanide compounds are considered to be the most likely choice of chemicals that terrorists might seek to acquire including Hydrogen Cyanide (HCN), Cyanogen Chloride (ClCN), mustard agents, nerve agents (VX) and toxic industrial chemicals. There is a risk that these chemicals could be exploited using new reactor technologies including phase-transfer catalysis, microwave reactors, and electrochemistry which can serve a malignant purpose as duel use technologies. Importantly, some of these process technologies can be scaled down to sizes that could be operated inconspicuously outside a normal chemical production setting.

Biological weapons could be used to attack people or infrastructure (e.g. food and water supplies). There is a risk that biological agents such as Anthrax and Ricin could be used by terrorists to cause fear among the civilian population. There are also risks associated with the malevolent use of radiological and nuclear materials. There are concerns, for example, that an **Improvised Nuclear Device (IND)** could be detonated using nuclear weapon components, modified nuclear weapons, or a self-made device.[2] Although currently beyond the reach of terrorist organisations, there is a risk that in the near future terrorists may seek to produce meaningful quantities of nuclear materials through enrichment techniques.

Another concern is that a **Radiological Dispersal Device (RDD)** could be designed to disperse radioactive materials through an explosion (or 'dirty bomb') to cause destruction, contamination,

[1] Campbell J K. Excerpts from research study 'weapons of mass destruction and terrorism: Proliferation by non-state actors', Terrorism and Political Violence 9, no. 2. 2007. p 25

[2] CIA. 4

and injury from the radiation produced by the material. Radioactive elements such as strontium-90 and cesium-137 can be found in many medical and industrial locations. Since 1998, in the US alone, there have been more than 1,300 reported incidents of lost, stolen, or abandoned devices containing sealed radioactive sources, an average of about 250 per year.[3]

Another challenge is the need for **improved monitoring of nuclear and radioactive materials** and the prevention of their illicit trade. There are large quantities of highly enriched uranium (HEU) in the former Soviet Union. Additionally, the Illicit Trafficking Database of the International Atomic Energy Agency has reported 540 confirmed cases of illegal commerce in both nuclear and radioactive materials between December 1993 and 2003. Project Geiger[4] has also recorded more than 2,200 cases of trafficking, of which 133 took place in 2009[5]. In addition, there have been a number of failed attempts globally to steal fissile material in the past decade. This presents a clear threat to the EU's internal security.

2.2 EU policy and legislative context

The responsibility to protect civilian populations against CBRN incidents is mainly a Member State competence, however, the EU plays an important coordination role, for example, in enhancing the security of high risk CBRN materials and facilities, developing lists of high-risk CBRN materials and risk-based approaches to security and the identification of good practices concerning the security of high-risk chemical facilities.

In recognition of this, the CBRN Task Force was launched in February 2008, with a view to preparing a list of measures that could be undertaken at EU level and in the Member States to lower the risks of terrorist acts using CBRN materials. Based on the recommendations of the Task Force, the EU CBRN Action Plan[6] was published in 2009. The Action Plan highlights the need for coordinated action to prevent, detect, prepare and respond to CBRN incidents and make sure new systems and technologies are put in place to deal with multiple 'all hazard' threats to society and critical national infrastructure. The action plan identifies three main areas of work:

- **Prevention -** the use of risk-assessment to prioritise high-risk CBRN materials, and then focus on the security and control of these materials and the related facilities;
- **Detection -** essential to support prevention and necessary for response. Common CBRN detection standards will be developed, testing and certification schemes will be established, and the exchanges of good practices will be enhanced;
- **Preparedness and response -** attention to emergency planning, information flows, modeling tools, and countermeasure and criminal investigation capacity.

The goal of CBRN policy is to minimise the threat and damage to the public from CBRN incidents through the:

[3] General Accounting Office. Nuclear Security: Federal and State Action Needed to Improve Security of Sealed Radioactive Sources. US: Senate. 2003. P 4

[4] Project Geiger is a joint initiative between INTERPOL and the International Atomic Energy Agency (IAEA), with the aim of gathering comprehensive data on the illicit traffic in nuclear and radiological materials, analysing the threats and assisting with international investigations.

[5] INTERPOL. Annual Report. http://www.interpol.int/Public/Icpo/Publications/default.asp. 2009

[6] Communication from the Commission to the European Parliament and the Council of 24 June 2009 on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan

Policy Context and Key Security Issues 2

- Use of a risk-based approach to security;
- Effective protection of CBRN materials;
- Improved exchanges of security-related information between Member States;
- Further development of detection systems in the EU;
- Provision of the necessary tools to manage CBRN incidents.

The Commission's CBRN Action Plan is being implemented in close consultation with national authorities, the private sector, academic institutions and wider stakeholders to ensure the plan's coherence with existing national and international regulations. A key part of the Action Plan is the Commission's intention to launch an EU CBRN Resilience Programme, which brings together the various civil protection activities included in the EU CBRN Action Plan and ensures a consolidated contribution to the overall implementation of this Action Plan.

In the external sphere, DG RELEX operates through 130 EC Delegations in third countries to prevent the transfer of sensitive information and technical knowledge from to rogue states and non-state actors. An emphasis is placed on retraining nuclear scientists for sustainable careers in the civilian labour market and working with regional CBRN centres of excellence to develop local capabilities to address the proliferation of WMD and to ensure adequate export controls are in place to prevent the trafficking of illicit CBRN materials.

The table below outlines some of the main policy and regulatory developments in the field of CBRN that preceded the drawing up of the CBRN Action Plan.

Table 2.1: Summary of key EU policy actions in area of CBRN

Issue	Relevant CBRN policy document	Summary overview
Initial response to the CBRN threat following terrorist attacks of September 11th 2001	14627/2002 Programme to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats	The programme aimed to improve cooperation between Member States on the evaluation of risks, alerts and intervention, the storage of such means, and in the field of research. The programme addressed the detection and identification of infectious and toxic agents as well as the prevention and treatment of chemical and biological attacks
Sets out the EU's response to the proliferation of CBRN materials	15708/2003 EU strategy against proliferation of Weapons of Mass Destruction	The EU's strategy implementation plan is based on an action plan which will be subject to regular revision. It is based on four priorities: • Resolute action against proliferators • Stabilise international and regional environment • cooperating closely with the US and other international partners • Develop the necessary structures within the Union
Introduced as a response to the outbreak of severe acute respiratory syndrome (SARS)	851/2004 European centre for disease prevention and control	The new European centre was established in order to improve the coherence and effectiveness of Community action for the protection of European citizens against infectious agents including bio-weapons
Outlines the EU's counter terrorism strategy	14469/4/2005 The European Union Counter-Terrorism Strategy (incorporates the 2004 EU Solidarity Programme on terrorist threats and attacks)	The EU proposes four pillars to combat terrorism including: prevent, protect, pursue and respond. A key priority is to prevent terrorist access to weapons and explosives, ranging from components for homemade explosive to CBRN material
Coordination of civil	EC /779/2007 Community Civil	The cooperation mechanism aims to improve the

Policy Context and Key Security Issues 2

protection assistance	Protection Mechanism	coordination of civil protection assistance intervention in major emergencies.
Promoting cooperation in nuclear safety field with third countries.	300/2007 establishing an Instrument for Nuclear Safety Cooperation	The Regulation establishes a framework for funding measures aimed at providing a high level of nuclear safety and radiological protection, as well as the implementation of effective and efficient safety controls in Non-EU Member Countries.

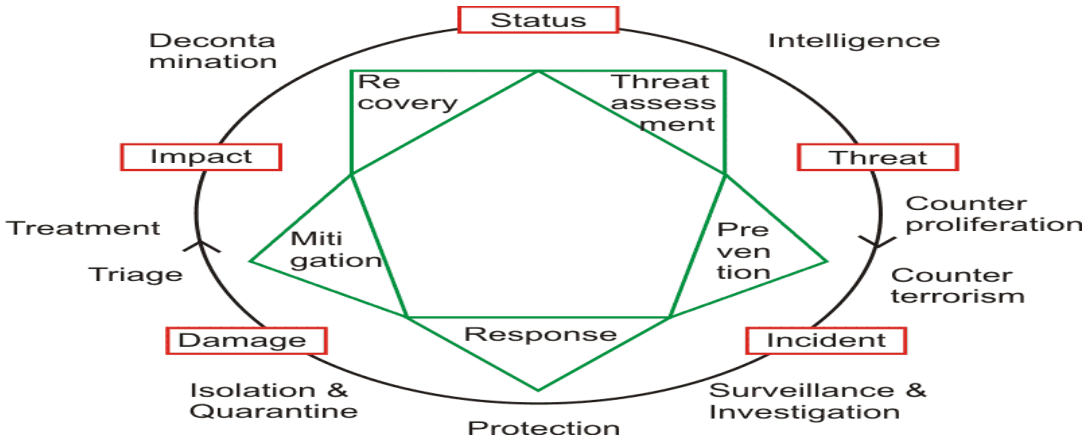
As the table shows, there have been a number of key policy, strategic and legislative developments in the CBRN field that impact on the context in which CBRN projects supported through the European Security Research Programme are implemented.

The EU is a signatory to various international agreements and treaties relating to the non-proliferation of CBRN materials such as the Chemical Weapons Convention (CWC), the Biological and Toxin Weapons Convention (BTWC), the Convention on Physical Protection of Nuclear Material and the Nuclear Non- Proliferation Treaty (NPT). Since the terrorist attacks of September 11th, there has been greater coordination between the Commission and Member States regarding the main policy challenges from CBRN attacks however the above international treaties and legal agreements continue to play an important role in reducing the amount of dangerous CBRN materials on the market as well as restricting the access for rogue states and terrorist groups to Weapons of Mass Destruction technologies and capabilities.

2.3 The CBRN cycle – Prevention, Preparedness, Response

The CBRN security cycle provides a framework which outlines the links between different CBRN management stages including specific actions for the prevention, preparedness, response, mitigation and recovery from CBRN incidents. The CBRN cycle is set out in the diagram below:

Figure 1: CBRN cycle showing stages, intervention strategies, and tools



Source: ESRIF Final Report

Prevention measures include the development of lists at EU level of high-risk CBRN materials; identifying and reporting suspicious transactions and behaviour; enhancing security and control of high risk CBRN materials; facilities and transport infrastructure; Contributing to the development of a high security culture of staff; improving information exchange; strengthening the import/export regime; strengthening cooperation on the security of nuclear materials.

Preparedness requires improved emergency planning; stronger countermeasure capacity; improved domestic and international information flows regarding CBRN emergencies; the development of new

modelling and better decontamination and remediation capacity; ensuring greater capacity to conduct criminal investigations.

Responding to CBRN events demands enhanced international cooperation; improved lines of communication with the public; more robust information tools for CBRN security; advanced training courses for first responders; improved personnel security; and ensuring that legislation is put in place to tackle CBRN terrorism.

2.4 Key stakeholders in the field of CBRN

First responders are most directly concerned in the event of a CBRN attack. Members of the rescue services, security forces and health professionals must be equipped with the specific tools and training to implement immediate response measures together with mass vaccination and decontamination programmes. They also need effective equipment and personal protective clothing in order to respond to CBRN incidents.

There is also a need for more effective coordination between **civil protection authorities** at local, regional and national – as well as on a cross-border basis within the EU in order to integrate response procedures and to facilitate rapid analysis of CBRN materials there is a need for online, secure and networked databases which allow sensitive information to be exchanged between specialised first responders and centralised laboratory testing facilities. **CBRN laboratories** are therefore an important stakeholder in the programme, and have been involved in standardisation work to develop common approaches to testing and certification at EU level.

The **European Commission's** DG Justice is responsible for the implementation of the EU CBRN Action Plan. The research results from the ESRP feed into the achievement of approximately 40 of the 120 specific actions identified in the Action Plan.

Law enforcement agencies and **intelligence agencies** are also important stakeholders in CBRN and play a key role in tracking the illicit trafficking of CBRN materials and in preventing and disrupting their production.

European citizens are also among the ultimate target audience of some projects. CBRN attacks pose a direct threat to the critical infrastructure of open societies, as they have the potential to disrupt the economy by denying use of physical spaces as well as testing societal and psychological resilience.

All of the above stakeholders have been actively involved in CBRN projects, and are among the prospective users of project research outcomes.

Project assessment - CBRN 3

A range of PASR and FP7 SEC projects have been supported that deal with the emerging threat posed by CBRN, and help to address current technology gaps. In this section, a sample of projects funded to date is examined.

3.1 CBRN Research in PASR and FP7 Security – overview

There has been a strong focus in projects funded through PASR and FP7 SEC on the response phase of CBRN incidents. CBRN projects have addressed the need for measures to strengthen coordination and improve communication between public agencies and emergency services. Projects have also addressed the need for investment in improving CBRN detection equipment and technical limitations such as design weaknesses and the lack of standardised Personal Protective Equipment. There has been support for the development of protocols governing sampling and identification methods. These are a necessary pre-condition for common EU decontamination procedures in response to CBRN attacks.

New technologies and capabilities need to be developed to prevent, prepare and respond to potential CBRN incidents. This requires a focused research effort on interoperability to ensure that detection technologies are mobile and versatile enough to operate in a variety of physical environments such as land boarders, airports and maritime port facilities. The EU security industry has a major role to play in the design of innovative and low-cost equipment to improve CBRN detection that can be integrated with larger security setups such as biometrics, databases and communication networks (i.e. GPS and 3G radiation sensors).

PASR and FP7 Security have provided support to a number of CBRN projects, as summarised in the table below:

Table 3.1: PASR and FP7 Security Projects supported in CBRN field

Project	Full name	Programme	Call	EU Contribution	Budget
Bio3R	Bioterrorism Resilience, Research, Reaction	PASR	PASR 2006	€ 481,550	€ 642,067
BODE	Biological optical detection experiment	PASR	PASR 2006	€ 1,815,614	€ 2,494,355
IMPACT	Innovative Measures for Protection Against CBRN Terrorism	PASR	PASR 2004	€ 2,717,640	€ 2,717,640
TIARA	Treatment Initiatives after Radiological Accidents	PASR	PASR 2004	€ 324,752	€ 171,900
WATERSAFE	On-line monitoring of drinking water for public security from deliberate or accidental contamination	PASR	PASR 2006	€1,923,975	€ 5,565,300
HAMLeT	Hazardous Material Localisation & person tracking	PASR	PASR 2006	€ 218,823	€ 318,267
BeSeCu	Human behaviour in crisis situations : A cross cultural investigation in order to tailor security-related communication	FP7 Security	SEC-2007-6.1-02	€ 2,093,808	€ 2,446,144
CAST	Comparative assessment of security-centered training curricula for first responders on disaster management in the EU	FP7 Security	SEC-2007-6.2-01	€ 1,974,670	€ 2,858,318
COCAE	*Cooperation Across Europe for Cd(Zn)Te based security*	FP7 Security	SEC-2007-1.3-01 SEC-2007-4.3-03	€ 2,037,610	€ 2,653,077
COPE	Common Operational Picture Exploitation	FP7 Security	SEC-2007-4.3-02 SEC-2007-4.3-01	€ 2,535,049	€ 3,886,574

CREATIF	CBRNE related testing and certification facilities - a networking strategy	FP7 Security	SEC-2007-7.0-03	€ 831,300	€ 831,300
SECUREAU	Security and decontamination of drinking water distribution systems following a deliberate contamination	FP7 Security	SEC-2007-1.3-05	€ 5,269,168	€ 7,462,072
FRESP	Advanced first response respiratory protection	FP7 Security	SEC-2007-4.3-03	€ 3,029,967	€ 4,032,757
LOTUS	Localization of Threat Substances in Urban Society	FP7 Security	SEC-2007-1.3-03	€ 3,189,146	€ 4,298,593

Funding and extent of prioritisation of CBRN in PASR and FP7 SEC

There has been a gradual increase in funding allocated to the CBRN theme during FP7 Security Research, which demonstrates its considerable importance within the programme. Data for the years 2007-2010 was obtained:

Project overview by area of CBRN

Although the evaluation focused on the first and second calls in FP7 Security, it is worth noting the areas of CBRN-related funding for the most recent calls. As of November 1st 2010, 21 CBRN projects had been supported through FP7 SEC (18 grant agreements have been signed, and 3 are in ongoing negotiations), with a total EU contribution of €83 m. This demonstrates that CBRN is among the most important themes in EU Security Research, accounting for 9.1% of the total financial allocation across the first 3 Security Calls and the Joint ICT and Security Call of €750m (While some projects have addressed the full gamut of CBRN issues, other projects have focused on particular areas within CBRN, e.g. chemicals, explosives, etc. The number of projects in specific spheres includes:

- **Chemical -** 14 projects
- **Biological** – 15 projects
- **Radiological and Nuclear** – 13 projects
- **Cross cutting CBRN** – 10 projects
- **Explosives** – 5 projects have been added as a research topic to the 2011 call

As the ESRP has evolved during PASR and FP7, there has been a steady increase in the number and scope of research topics included under the CBRN theme. This is reflected in the consistent increase in funding allocation, especially during FP7 SEC.

Thematic focus in calls for proposals

A number of research topics were supported through PASR in the area of CBRN. PASR 2005, prioritised the integration of active and passive sensor techniques with data platforms, detection systems and equipment for decontamination activities. These activities continued to be prioritised in PASR 2006, with the addition of the detection of explosives. Other CBRN topics supported under PASR include the mapping of pre-standards, and surveillance security.

During FP7 SEC, there has been a strong focus over in successive calls for proposals on the development of improved detection equipment. For example, in the first call for security research in 2007, there was a focus on the development of stand-off scanning and detection devices that could be deployed in fixed positions or mobile vehicles. In the 2009 and 2010 FP7 SEC Calls, an emphasis was placed on improving the efficiency and sensitivity of detection devices together with state-of-the-art technologies to improve personal protective equipment.

Funding was also made available for enhancing border surveillance and responding to CBRN crisis incidents as part of strengthened resilience e.g. in the 1st call in FP7 SEC. There has also been a strong focus on increasing the resilience of critical public infrastructure by increasing the level of interoperability and secure communication systems for first responders. In the 3rd call in 2010, support was extended to include Intelligent Surveillance and enhancing border security in respect of CBRN detection, with an emphasis on EU external borders.

Among the findings from the review of the prioritisation of CBRN in the PASR and FP7 SEC annual security work programmes was that there is strong continuity between calls on CBRN topics. This is consistent with the Security Research Unit's focus on strengthening security in particular fields through an incremental, building-block approach. Under FP7 SEC, many of the topics addressed through PASR have been followed up, such as funding for the development of innovative CBRN detection devices. A number of new topics related to CBRN have emerged that were not covered through PASR, such as track and trace technologies for crowded areas and border checkpoints.

A detailed review of CBRN-relevant research topics in the PASR and FP7 SEC calls for proposals is provided in Appendix B.

3.2 PASR and FP7 project assessment – CBRN

Selected project examples are now analysed supported in the field of CBRN through both PASR and FP7. An explanation of the categorisation of measures to support CBRN was provided in section 2. The projects examples have been categorised according to whether they related mainly to: prevention, preparedness and response.

Prevention projects:

The ESRP supported a number of foresight activities to improve knowledge about potential threats over the medium to long term. Foresight scanning provides an effective tool for gauging future risks in terms of their likelihood, vulnerability and potential impact. This can in turn be used to improve strategic planning and to inform scenario models which help security organisations to take preventative actions against CBRN threats. Foresight and horizon scanning, is therefore, playing an increasingly important role in shaping strategies at national and EU level to prevent CBRN incidents.

An example of how foresight capabilities have been strengthened through the ESRP is the **FESTOS** (FP7 SEC, Call 2) project, which addressed CBRN as one of a number of areas of focus on the potential threats resulting from new and emerging technologies.

Table 3.3: Addressing gaps in strategic planning for CBRN attacks	
Project(s):	FESTOS - Foresight of Evolving Security Threats Posed by Emerging Technologies
Project timeframe:	March 2009 - February 2011
Lead Partner:	Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF), Tel-Aviv University
Total cost and EU Contribution:	€1,232,976 and €824,552
Call and Call Topic:	SEC-2007-6.3-01 - Security and society - Research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects)
Project type:	Capability project
The project identifies and assesses the evolving future threats posed by the abuse of emerging technologies and new scientific knowledge (in order to anticipate evolving threats and reduce the likelihood of catastrophic events). FESTOS is not specifically focused on threats from CBRN however many of the project activities draw heavily on overlapping CBRN threats addressed by other projects, such as FRESP and SecurEau**.** A number of NGO's and SME's were involved in the delivery of project outcomes including the implementation of a security mapping survey that was used to identify	

threat level indicators in relation to CBRN attacks and review the relevant linkages between security decision makers, civil society, institutions and research centres.

The research findings will be used by the FESTOS team to draw up detailed reports that highlight new threats linked to emerging technologies, recommendations for policy guidelines, narrative scenarios and future foresight exercises in order to pre-empt the innovations terrorists are likely make in the delivery of CBRN weapons. FESTOS analysed a variety of threats along a 20-30 year timeline which included Low probability, but high impact threats such as CBRN terrorism. The project looked at the ways in which converging technologies such as CBRN, ICT, Nanotechnology and robotics are generating new threats to Europe's interconnected, market states and societies. Some user organisations have already expressed strong interest in using the outcomes from the research, for example, in a database of new and emerging threats and in the results of work on future threat scenario modelling.

While foresight can contribute to improving the quality of strategic planning for CBRN incidents, there is also a need to invest in strengthening technological capabilities to detect CBRN.

Another key priority for the ESRP in the CBRN domain was to invest in research and development on detection equipment. The aim was to strengthen capabilities through the development of improved detection equipment capable of being used on a stand-off and remote basis, such as hand-held and portable detection devices. The aim is to equip the border security personnel of the future with new generation technologies that provide more accurate results, and also pose less health and safety risk to the personnel concerned. One of the key challenges identified in the FP7 2007-2008 work programme was the need to support activities to *Detect, track, trace, identify and neutralise CBRNE.*

In addition to developing new breakthroughs in detection technologies, ESRP projects have made existing devices more user-friendly by improving their performance in terms of sensitivity, specificity, false alarm rates, detection limits, distance from source, time to detection, size and weight. The **IMSK** (FP7, Call 2, Integrated Mobile Security Kit), **DETECTER** (FP7, Detection technologies, terrorism, ethics and human rights), **EFFISEC** (FP7, Call 1, Efficient Integrated Security Checkpoints) projects are indicative of the holistic approach taken by ESRP projects in building progressing Europe's detection and screening capability.

There are capability gaps concerning the protection of water supply from contamination by chemical and biological agents. Water supply systems could be used to spread communicable diseases to a large city population long before detection health agencies are able to effectively respond. Improving the monitoring of water supply for contamination has been supported both in PASR and in FP7 SEC, for example, through the **Watersafe** (PASR, 2006) and **SECUREAU** (FP7, Call 2) projects. There is a need for both technological innovation and security vigilance in this area.

Table 3.4: Preventing contamination of the water supply by CBRN substances	
Project(s):	Watersafe - On-Line Monitoring of Drinking Water for Public Security from Deliberate or Accidental Contamination
Project timeframe:	January 2007 – January 2009
Lead Partner:	C-Tech Innovation Ltd, UK
Total cost and EU Contribution:	€2,565,300 and €1,923,975
Call and Call Topic:	PASR 2006
Project type:	Capability project
Networked water systems are considered to be particularly vulnerable to terrorist and criminal group's attempts to contaminate the water supply. In the case of an accidental or deliberate contamination of the using CBRN substances, effective early warning capabilities play a key role in preventing further distribution and potential loss of life. For example, the project Watersafe was funded under PASR and brought together 4 SME's with research groups to develop new approaches to detecting and mitigating against various water contamination scenarios.	

Project assessment - CBRN 3

The project made use of breakthrough nanotechnologies to develop online early warning systems and advance new sensing and detoxification methods by ensuring they were intelligent, sensitive, flexible, compact and cost effective. A key priority was to guarantee the system was interoperable and complied with compatible technology standards allowing it to be deployed at vulnerable points in the water system such as piped distribution systems, water tanks, towers, treatment facilities. New data collection techniques were combined with an integrated system of water analyses and monitoring (i.e. PH conductivity).

The increased threat level of CBRN terrorism demands improved networking and coordination between relevant national and EU stakeholders. It also requires common testing and certification equipment. The **CREATIF project** (FP7 SEC, Call 1) had a strong networking dimension and was designed to strengthen cooperation and knowledge exchange between relevant CBRN actors across Europe. While the project is at a relatively early stage in implementation, there are some promising aspects, such as the development of pre-standards in the area of CBRN detection equipment. Also worth highlighting was the use of an advisory board of end-users and industrial experts. Good practice shows that the more successful ESRP projects, in terms of the take-up of research results, closely involved end-users in the planning, implementation and evaluation process.

Table 3.5: Projects to prepare for Radiological and Nuclear incidents

Project(s):	CREATIF - Networking strategy to strengthen cooperation and knowledge exchange within Europe
Project timeframe:	January 2007 – June 2011
Lead Partner:	Austrian Research Centers GmbH - ARC
Total cost and EU Contribution:	€831,300 (100% co-financed)
Call and Call Topic:	SEC-2007-7.0-03 - Security Research coordination and structuring - Network of facilities for testing, evaluating and certifying security related products
Project type:	Coordination and support action

The CREATIF network aims to establish a communication platform for technology users, decision makers, providers and testers to discuss the future development of testing and to support user decisions and industry product / service development. The project will gather information on test facilities and their areas of expertise through the development of a database. It will also a provide roadmap for the development of common standards and certification procedures. This is designed as a prelude to the creation of a uniform EU-wide technical and certification process that guarantees quality assurance.

Moreover, CREATIF has developed an extensive network of civil and military partners, whose expertise, the project leaders intend to leverage in order to set up a database on testing facilities for CBRNE detection equipment, together with a framework for joint testing exercises. Presently only a few Member States have the site security and authorisation to conduct CBRN product trials. Furthermore the sensitive nature of CBRNE testing is a barrier to cooperation at the EU level, particularly with regard to political negotiations about EU security labelling. SME's are disadvantaged by the current testing process which allows more access for large security firms national testing programmes.

The activities carried out by CREATIF are designed to breakdown and lay the foundations for a European certification system for CBRNE sensor systems, devices, detection methods and relevant labelling systems. Such a structure will do much to overcome the imperfections in the presently highly fragmented European security market.

Preparedness projects:

The current generation of CBRN detection systems does not focus sufficiently on the production phase of explosives. The following example demonstrates how new systems could allow law enforcement agencies to be more proactive. This would mean acting during a phase where there is low threat to citizens, for example, while terrorists groups are at the stage of mixing explosive chemicals. Dealing with threats at this stage gives police more time and resourcing options to deal with threats as well as a wider scope for response. The same system could also be used to target organised criminal networks by detecting if drugs are being produced in a known area.

Project assessment - CBRN 3

Table 3.6: Projects to provide detection and early warning of harmful substances	
Project(s):	LOTUS - Localization of Threat Substances in Urban Society
Project timeframe:	January 2009 – October 2012
Lead Partner:	Swedish Defence Research Agency (FOI)
Total and EU Contribution Cost:	€4,298,593 and €3,189,146
Call and Call Topic:	SEC-2007-1.3-03 - Increasing the Security of citizens - Localisation and tracking of components of substance production
Project type:	Capability project
The LOTUS project is developing a new anti-terrorism tool for law enforcement agencies in the form of an integrated surveillance system for continuous chemical background monitoring with fixed site and/or mobile detectors in order to identify chemical hotspots, such as bomb or drug factories. The aim is to detect the production of explosives and drugs during the production stage by tracing chemical signatures over a wide urban area. The detectors could be placed at fixed positions or mobile. These distributed detectors will continuously sample the air while the carrier performs its normal duties. For example, the detection device could be placed on public transportation such as buses and underground railway stations. When a suspicious substance is detected in elevated amounts, information about the type, location, amount and time is registered and sent to a data collection and evaluation centre for analysis. Several indications in the same area will trigger an alert, enabling law enforcement agencies to further investigate and respond. The project will utilise existing technology and integrate them into public infrastructure for positioning (GPS) and mobile communication (GSM, GPRS or 3G networks). This will allow the deployment of the LOTUS system anywhere in the world at relatively low installation costs.	

There is an increased risk from biological warfare agents, given that only limited financing and training is needed. Biological weapons pose a particular risk because they can be dispatched and smuggled more easily than conventional weapons. Small quantities of lethal biological agents could cause mass casualties. Distinguishing biological agents from the myriad of similar naturally occurring micro organisms in the environment makes this task especially daunting.

Although biological weapons have been a threat for many years, recent advances in biotechnology make the problem potentially more serious. Furthermore, traditional detection and early warning systems are less reliable when it comes to accurately distinguishing biological agents compared with chemical precursors. The **BODE** project (PASR, 2006) therefore addressed important gaps in the reliability and accuracy of stand-off biological detection devices.

Table 3.7: Stand-off optical detection technologies	
Project(s):	BODE - Biological Optical Detection Experiment
Project timeframe:	January 2007 –March 2009
Lead Partner:	CILAS Compagnie Industrielle des Lasers, France
Total and EU Contribution Cost:	€2,494,355 and €1,815,614
Call and Call Topic:	PASR
Project type:	Capability project
BODE began by analysing existing state of the art detection capabilities to help identify the function and operational requirements of detection apparatus. The partners decided to base the BODE detection system on Dry Detection and optical stand-off technologies, which made use of an intelligent warning algorithm. Additional features of the project include improving methodologies to support analysis of physical aerosol signatures. This could help prevent attacks like the one carried out in 1995 when thirteen people were killed by the release of Sarin nerve gas on the Tokyo subway. The BODE detection system will follow a miniature design and be made to withstand certain physical shocks in different operating environments. The project has utilised the resources of companies, industrial and governmental researchers, as well as users and first responders to integrate the technology with networked systems. Partners are confident that once the reliability of the detection system has been established there are many opportunities to fully exploit the projects commercial potential.	

Project assessment - CBRN 3

The next project example, **BIO3R**, (PASR 2006), a supporting activity, demonstrates how projects have contributed to strengthening knowledge about operational requirements and functional capabilities needed to respond to CBRN threats and promoting co-operation between relevant stakeholders in the area of bioterrorism resilience, research and improving response. The project also focused on risk assessment, which was relevant to the achievement of the EU CBRN Action Plan, which highlights the need for a risk-based approach in the area of CBRN.

Table 3.8: Improving resilience to bioterrorism attacks	
Project(s):	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
Project timeframe:	January 2007 – August 2008
Lead Partner:	Fondation pour la Recherche Stratégique, France
Total and EU Contribution Cost:	€642,067 and €481,550
Call and Call Topic:	PASR
Project type:	Capability project
BIO3R's comprehensive policy on bioterrorism, recommended action in three areas which included Research, Reaction and Resilience. The research sphere carried out an evaluation of state of the art technology and risk assessment to identify priority tasks. The next step, reaction, was designed to reinforce crisis management policies by improving the integration of legal aspects of security strategies at local, national and European levels. Finally, activities were carried out to improve the resilience of EU societies and to promote awareness of the bio threat, through reliable information, education and training. The resilience theme Contribution to the improvement of the prevention, resilience and mitigation of threat A study of crisis management issues and a cross evaluation of public health policies will be carried out, and the issue of communication and coordination between the actors will be looked into. BIO3R will also contribute to the education and training of hospital professionals and first responders through the development of a training kit, as well as to the improvement of the comprehension and awareness of the European citizens thanks to a web portal and a model of public handbook.	

The **HAMLeT** project was established to classify, track and localize potential threats from hazardous materials. The core functions of the project provide an in-door security assistance system for real-time decision support by using advanced sensors and multiple sensor fusion techniques.

Table 3.9: Projects to provide detection and early warning of harmful substances	
Project(s):	HAMLeT - Hazardous Material Localisation & Person Tracking
Project timeframe:	January 2006 – March 2007
Lead Partner:	Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) e.V.
Total and EU Contribution Cost:	€318,267 and €218,823
Call and Call Topic:	PASR 2006
Project type:	Capability project
The HAMLeT system is a network of atmosphere monitoring sensors that are attuned to particular chemical molecules. They are designed to detect a whether a moving object is carry a hazardous material such as an explosive device or bomb particular chemical residues on skin and clothing surfaces. The system works by connecting oscillating crystals to the electronic smell sensor through advanced computer chips. These sensors capture chemical molecules, by homing in on changes to their oscillation frequency. The precise nature of the change is different for different substances. Among the main project achievements were the ability to collate all the data and convert it into a clear and accurate overall picture. The sensor data fusion process employs complex algorithms which allow HAMLET to build up a precise image of pedestrian flows and connect a particular smell with a specific individual. Among the results were recommendations to help characterise and standardise detection performance for sensors that detect chemical traces. The introduction of common standards in this area is an important step towards market take-up of integrated multiple sensor technologies.	

A further challenge is that current detection devices do not provide sufficient mobility and flexibility to identify multiple CBRN, each of which may require a different set of technologies in order to

detect. For example, current techniques to detect chemical and biological agents require close interaction with the materials, which poses a significant contamination risk to first responders. A number of projects, such as **CoCAE** (FP7, Call 1) addressed this problem through the development of standoff detection technologies and by increasing the number of chemical and biological agents that can be identified.

Table 3.10: Project to prevent the illegal transit of nuclear and radiological materials	
Project(s):	COCAE - Cooperation Across Europe for Cd(zn)te based Security
Project timeframe:	January 2008 – January 2012
Lead Partner:	Technological Educational Institute of Halkida (TEI) Thesi Skliro
Total and EU Contribution Cost:	€2,653,077 and €2,037,610
Call and Call Topic:	SEC-2007-4.3-03 - Restoring security and safety in case of crisis - Personal equipment
Project type:	Capability project
The project produced a new portable radiological detection device with a spectroscopic measurement equivalent to NaI detectors (using scintillation crystals) and an energy resolution similar to that of HPGe (High-Purity Germanium) devices. This was achieved using a new form of high purity, detector grade Cd(Zn)Te crystals which provides the unique ability to give information about the spatial distribution of radioactive contamination and to detect the existence of a shielding material around the source. The new technology allows the Compton Effect[7] to be exploited leading to improved variable detection efficiency. There is a growing international market for Cd(Zn)Te detection crystals, although, only the EU, US, Canada and Israel have the scientific capabilities to produce them. The crystals perform well under a range of conditions and can be adapted for use in medical detection equipment. The project partners are confident that COCAE research will have a major impact on the competitiveness of the European market in detection equipment, provided that technology and scientific knowledge is retained in this area. However, only one commercial firm was involved in the project directly, and as yet there has not been the opportunity to exploit the commercialisation potential of the technology. Nevertheless, the project is producing research results that demonstrate state of the art.	

Response and Recovery projects:

Ensuring the durability of personal protective equipment is vital for the CBRN operational response phase. Therefore a premium should be placed on developing items such as transportable CBRN tool kits, improved collective protection systems such as mobile isolation chambers, rapid containment solutions, and advanced filtration systems together with reliable R/N biodosimetry and antidote activities for exposure victims. Current detection technologies are limited by the number of biological agents, toxicity and contagion levels they can accurately detect.

Table 3.11: Design and production of lighter respiratory protection	
Project(s):	FRESP - Advanced First Response Respiratory Protection
Project timeframe:	January 2008 – May 2011
Lead Partner:	Royal Military Academy
Total and EU Contribution Cost:	€4,032,757 and €3,029,967
Call and Call Topic:	SEC-2007-4.3-03 - Restoring security and safety in case of crisis - Personal equipment
Project type:	Capability project
FRESP aims to establish a network of scientists and research institutions, who will develop a new type of protective breathing apparatus for first responders. The design will incorporate broad-spectrum, low burden, Nano-porous adsorbent features. The product can protect against both chemical warfare agents and toxic industrial chemicals without losing capacity in either area. It will also integrate state-of-the-art adsorbents which allow enhanced protection against radioactive gases against biological threats.	

[7] The Compton effect (also called *Compton scattering*) is the result of a high-energy photon colliding with a target, which releases loosely bound electrons from the outer shell of the atom or molecule.

Project assessment - CBRN 3

The project is seeking to overcome technical issues relating to the effects of different impregnation methods and developing innovations to ensure the respirator maintains high absorption capacity when coming into contact with water vapour. This will be possible after the new absorbents are fully examined for health and safety issues. The project partners have developed an IPR strategy and aim for commercial scale produce of the nano-porous adsorbent, the filter canister and the hood. The possibility of commercialisation procedure of the new adsorbents is being investigated.

Containing the effects of a CBRN attack heavily depends on the extent to which **early warning procedures and technologies** are put in place at vulnerable locations. The specificity of CBRN materials, and the need for tailored sensors, places a significant burden on first responders who require detailed information on the type of threat in order to effectively implement their response and allocate resources. **LOTUS** (FP7, Call 1) fulfils this capability gap through an all hazards approach to chemical detection.

In light of the growing threat from international terrorism, resources have been allocated to prepare the emergency services for the possibility of CBRN attacks and incidents in crowded areas. There is a need to strengthen capacity, given that only a small proportion of doctors have experience in treatment procedures for victims of CBRN attacks. Better guidance on dose assessment and the effectiveness of different treatments for patients that have had exposure to CBRN is needed.

The effects of mass casualty scenarios on the operational needs of first responders should be mapped out to ensure procedures and protocols are relevant to the scale of public disruption. Many of these issues are addressed by ESRP projects which work closely with a broad range of stakeholders including DG SANCO, national health authorities and first responders. The European Atomic Energy Community (EURATOM) has also contributed to the development of improved remediation and response measures through the introduction of the TMT handbook. One of the projects with direct links to this activity was TIARA.

Table 3.12 Decontamination and remediation

Project(s):	TIARA - Treatment Initiatives After Radiological Accidents
Project timeframe:	January 2005 – January 2007
Lead Partner:	Commissariat à l'énergie atomique (CEA), DSV/CARMIN, France
Total and EU Contribution Cost:	€324,752 and €171,900
Call and Call Topic:	PASR
Project type:	Capability project

TIARA created a European network to facilitate the crisis management in the event a malevolent dispersal of radionuclides[8]. The project focused on the remedial implications of radiological contamination in crowded areas resulting from the use of improvised nuclear and/or radiological dispersal devices ('dirty bombs'). The first step towards meeting this objective was to prepare the physicians, inexperienced in the management of radiological exposures and treatment by generating scientific and radiological information in the form of guidance notes. This included physicians involved in decorporation[9].

Once the TIARA network was established, experts were employed to evaluate the appropriate level of pharmaceutical stocks and to exchange good practices relating to the administration the administration of antidotes. Cooperation among the project partners had a positive impact on the harmonisation bet between a range of organisations. This was fed into scenario workshops which discussed dose assessment, treatment decision making, antidote stockpiling, crisis distribution, and the effectiveness of medical treatments. These discussions complemented the TIARA training course which aimed to prepare and inform relevant stakeholders about the management options for radioactively contaminated persons.

[8] An unstable and therefore radioactive form of a nuclide.
[9] The removal of radioactive isotopes from the body using specific drugs called decorporation agents.

Project assessment - CBRN

3.3 Achievements at project level and research quality

A summary of progress achieved in relation to achievements at the project level across the CBRN security cycle (Prevention, Preparedness and Response) is now provided. It should be noted that ESRP has only addressed mitigation and recovery aspects in the more recent calls within FP7 SEC.

3.3.1 Prevention

Personal Protective Equipment for first responders to protect against CBRN incidents has been improved. The FRESP project is developing an advanced technology for the respiratory protection of first responders. This will fill an important gap in the response capability of emergency services to CBRN events.

Progress has been made in addressing vulnerabilities linked to CBRN attacks associated with critical infrastructure. FESTOS carried out scenario mapping exercises, which allowed civil contingency planners to insulate critical infrastructure from a range of near term and future threats, many of which are likely include the innovative use of CBRN.

EU Security Research helped to strengthen knowledge and preparedness about how to respond to CBRN incidents among first responders. The BIO3R project developed cross-border technical expertise through common training activities for bio scientists. In the event of a biological attack, these cooperation structures could provide vital in accelerating the production of antidotes and vaccines.

Some progress has been made towards improving stand-off detection for radiological materials – and the technology being used is highly innovative. Progress has been made towards this aim through various projects, particularly the COCAE project, which made breakthroughs in crystal scintillation and nanotechnologies for handheld CBRN detection devices for use in border protection.

Progress has also been made towards standardisation and the development of common approaches to certification and testing. CREATIF created a roadmap for the development of common standards and certification procedures in the field of radiological detection. Provided that political agreement can be reached at EU level on common standards, CREATIF could make a strong contribution to the improved competitiveness the European security market.

Vulnerabilities to CBRN incidents in critical infrastructure have been addressed through security research. Examples include procedures to safeguard water supply in the event of malicious contamination. Watersafe addressed a vulnerability in the defence of critical infrastructure against the malicious use of CBRN materials by harnessing state of the art nanotechnologies in order to provide early warning systems that can be used by a variety of agencies to detect and rapidly respond to accidental and deliberate releases of chemicals and deadly toxins into the water supply.

3.3.2 Preparedness

New methods have been developed for detecting covert production facilities at a range of locations. Mobile sensors developed through the LOTUS project should help to provide an improved early detection and warning system on CBRN materials. The project offers police and law enforcement agencies automated detection to aid in the investigation of CBRN production sites.

Progress has also been made towards the establishment of common databases that list chemical molecular and sub-molecular properties, biological pathogens, viral strains and radiological isotopes. The BIO3R project has fostered greater cooperation structures and promoted knowledge exchange between Europe's leading CBRN facilities, to give first responders a head start in the race to identify specific CBRN properties in crisis situations.

FP7 security contributed to state-of-the-art detection technology in a number of areas. Research by the COCAE project has moved detection technology beyond the existing state-of-the-art by utilising muon radiography[10], spectroscopic monitors, new scintillation devices, active interrogation, photo-fission[11] and thermal infrared spectroscopy. While the project is only at the prototype stage, it is clear that the use of the crystals is highly advanced and has potential to enable Europe to compete with the US and Israel in this area.

3.3.3 Response and Recovery

Strong support was provided in both PASR and FP7 SEC to projects that focused on meeting the operational and mobility needs of first responders. For, example FRESP multi-purpose chemical resistant body protections that allow first responders to remain encapsulated yet operational over long periods with increased mobility, communication and tactile capability.

The ESRP has also addressed the need for effective triage, decontamination and post-incident diagnosis. A good example in this regard was the TIARA project, which offers a combined system of procedures focusing on the particulars of R/N threats, as well as taking maintaining a forensic approach that preserves vital evidence from the location in which CBRN events took place.

Increasing societal resilience to CBRN threats and incidents is a paramount task in re-building open societies after a CBRN incident, and prominently among FP7 security work packages. The assessment, carried out by the BeSeCu project, of individual and group behaviour in emergency situations, could lead to significant improvements in training procedures and allow cultural factors to be integrated with disaster modelling techniques.

3.3.4 Conclusions – research quality

The projects examined through the case study research appear to demonstrate research excellence. For example, progress towards state of the art was identified in projects such as **CoCAE**, which involves the production of scintillation crystals for high-resolution radiological detection for use in portable, stand-off detection devices at land borders. The crystals used in the technology are very rare, and the technology being developed is unique in Europe and will enable the EU to compete with competitors in the US and China.

A barometer of research excellence was the extent to which the organisations taking part in projects represent world-class research in their respective area of specialisation. A number of CBRN project examples were found to have brought together leading security industry players together with universities and established research institutions. For example, **LOTUS** established a positive working relationship between Swedish and Spanish national security research institutes and a leading security company in the Netherlands.

Examples were identified of high calibre, specialist researchers working on CBRN projects funded through the ESRP that have transferred skills and knowledge from CBRN projects supported through national security research programmes into the Work Packages of FP7 SEC projects. An example in this regard was the **FESTOS** project, which gained valuable inputs from intelligence agencies about a series of foresight scenarios and potential threats arising from the emergence of new technologies and cyber-threats to critical CBRN infrastructure, such as energy networks.

CBRN projects made some contribution to enhancing the knowledge base across different areas of CBRN Security Research. However there is scope for improving knowledge transfer between projects. For example, both Watersafe and SECUREAU aimed to address the need for greater early

[10] Muons passing through high-atomic-number materials (like uranium and plutonium) are scattered more than those passing through other materials (like steel or water).

[11] nuclear fission as the result of the absorption of a gamma ray or other high-energy photon

warning of contamination of the water supply, however there was relatively little cooperation between these projects at the planning and operational level. There has also been a lack of information sharing to date between the **FESTOS** and **FORESEC** projects, despite the potential cross-over between the two projects in terms of surveying low probability, high impact events.

Some projects helped to produce recommendations that are likely to influence the formulation of new policies and legislation/ regulations in the CBRN sphere. For example, projects such as Watersafe developed an early detection and warning system to prevent the contamination of public water supplies. This could be implemented through the adoption of regulatory standards at national level.

3.4 End-user involvement in CBRN

A range of experts in the CBRN field were interviewed during the case study research process including those who worked in the police, military, health agencies, Centres for the Protection of Critical Infrastructure and the scientific research community. Among the findings were that:

- The involvement of end-users in the mapping and implementation of CBRN projects was crucial in maintaining the relevance of CBRN research priorities.
- The views and concerns of end-users appear to have been taken on board and integrated into project planning by some consortia in the CBRN domain.
- There is a need to develop secure ICT networks to facilitate information exchange between actors in the CBRN domain.
- Progress has been made towards the development of common testing and certification processes in the CBRN domain which has potential to address the lack of adequate testing facilities for civil security purposes in many countries.

The **FESTOS project** (FP7 SEC, Call 2) was especially interesting in terms of the end-user dimension. As a project that dealt with foresight and horizon scanning of 'low probability, high impact' events, there was considerable cross-over between the activities of FESTOS and those of national intelligence organisations in Germany and Israel. The inputs of national intelligence agencies taking part in the project were valued by the lead coordinator, with the sharing of analytical resources which has enabled the project to map threats more effectively. However some end-users mentioned that cooperation was not always possible due to insecure ICT exchange networks.

The need for further progress in the area of standardisation is a significant issue in the CBRN field. The absence of common EU testing and certification processes limits the range of security products available to end-users. To address this shortcoming, the CREATIF project developed a forum which involved political decision makers, CBRN end-users and other stakeholders including private testing facilities and the European Committee for Standardisation (CEN).

Interviews carried out with prospective end-users, such as national civil contingency agencies, confirmed the important role played by common technical standards in fostering cooperation and interoperability between different types of end-users. For example, some end-users operate at the strategic level (e.g. governmental departments and intelligence agencies) while others are responsible for using specialised products and managing crisis situations. The challenge for future projects in the CBRN field is to ensure that both types of end-users are able to collaborate more effectively through secure channels of communication. Overall, project partners had a positive view about the contribution made by users to project outcomes. However, the fragmented nature of the EU security market, interaction between cross-border security projects and national authorities did not always result in lasting relationships.

Conclusions

4

In this section, the contribution of EU Security Research in PASR and FP7 Security to date towards promoting key aims in the CBRN domain is assessed, drawing on the analysis of the main achievements of research results at the project level.

4.1 Conclusions

The ESRP has made a strong contribution to strengthening coordination at EU level on CBRN, promoting a more integrated approach to addressing CBRN threats, and improving prevention, preparedness and response capabilities. Projects have promoted better information sharing between relevant CBRN actors at EU and national levels. Projects also focused resources on tackling vulnerabilities identified in the EU CBRN Action Plan, with a focus on achieving practical results through cooperation, increased networking and knowledge transfer.

Technologies to detect, monitor and assess CBRN materials have been promoted through the programme's emphasis on interoperability and on building networking capacity.

While CBRN events are local, developing an effective response requires cross-border cooperation, information sharing and the exchange of good practices. It also requires greater interoperability of equipment and the need for intricate systems of systems that allow for the horizontal exchange of secure information.

EU Security Research has made significant improvements in Personal Protective Equipment for first responders. Nanotechnology is being leveraged to design durable fabrics, which are both versatile and tailored to defend against a range of CBRN threats.

Projects have led to initial progress towards standardisation and the development of common certification and testing processes for CBRN detection products at EU level. There remain however barriers which inhibit the distribution and take up of planning and response capabilities and interoperable products to prevent, prepare and respond to CBRN incidents. There is a need for further regulatory actions to stimulate standardisation in procurement and security evaluation procedures to promote greater take up of project results.

CBRN projects have played a vital part in the definition of capabilities in this domain. They have promoted a better understanding among relevant stakeholders with regard to what activities it is appropriate to address at EU and national levels respectively.

FP7 Security has played a role in strengthening the priority given to areas of CBRN security research that had not hitherto been sufficiently prioritised at national level. Among the areas where there is particular value added in a European approach include the developments of lists of CBRN threats, cross-border training programmes among first responders, and information sharing in the response phase on CBRN incidents.

Through the selection process for FP7 Security, the Commission has successfully ensured that projects supported complemented similar activities at the national level. The Security Scrutiny procedure has played a useful role in this regard.

Projects in the CBRN field were successful in creating economies of scale with arguably greater efficiency and effectiveness compared to equivalent activities supported through national programmes.

Sustainable networks have been created through the ESRP in the CBRN domain. These have provided a useful mechanism through which the sustainable exchange of information and data can take place on CBRN foresight, detection and incident recovery protocols.

Conclusions 4

4.2 Recommendations

1. **The ESRP has not yet fully addressed the prevention dimension of the CBRN cycle.** In particular, there is a need to promote intelligence-sharing among Member States through secure ICT networks.

Intelligence plays a major role in preventing CBRN threats before they arise. There should be more emphasis placed on projects that overcome barriers in cross-border information sharing.

2. **Further resources should be targeted at cross-cutting preparedness issues since these have not yet been fully addressed in FP7 SEC Calls.** Examples of relevant research topics include global remote sensing technologies (e.g. the integration of satellite surveillance) and support for practical transnational training exercises.
3. **A continued effort should be made to promote standardisation.** While progress has been made in the development of common testing and certification for CBRN testing laboratories, standards are at an early stage in development.
4. **Realistic modelling scenarios could be expanded to include a combination of both real-time 3D virtual and physical (i.e. first aid and remediation procedures) simulations.** These were found to be an effective means for first responders in preparing for CBRN events.
5. **First responders need to acquire greater knowledge and awareness concerning the specifications of personal protective equipment.** This needs to be incorporated into future training programmes and modelling scenarios more systematically.
6. **Research results from previous CBRN projects on the decontamination of water supply should be disseminated on a restricted basis to defined stakeholders.** While recognising the need for transparency in research results, there are ongoing concerns about such information being used malevolently.
7. **Expertise in preparing and responding to CBRN attacks in the military could also be leveraged to improve the quality and contribute to the knowledge base of civilian training programmes.** This could be achieved through the European Framework Cooperation (EFC) with the EDA.
8. **The European Commission should play a greater role in promoting the dissemination of knowledge and good practices in incorporating resilience into the planning and design of future Critical infrastructure facilities.** Various projects have touched on resilience issues, although this aspect could be strengthened in the research topics supported in future Calls.
9. **As part of the long-term response to the remediation phase, there needs to be a greater emphasis on preparing societies and promoting awareness about the societal impact of CBRN incidents (including psychological aspects).** ESRP projects should include the public among the users given that there is a need to improve interaction between individuals and first responders in CBRN events.

Interview list

A

No.	*Name/ position*	*Organisation*	*Organisation type*	*Project (where applicable)*
1	Bastian Giegerich - Research Fellow for European Security	International Institute for Strategic Studies	User	FORESEC
2	Andy Sigsworth Senior manager	Police National CBRN Centre	User	NA
3	David Omand – Former Director	UK GCHQ	User	NA
4	Paolo Guglielmetti - Commission Official	DG SANCO	User	NA
5	Jörg Beckmann – Director	Federal Institute for Materials Research and Testing, Division VIII.3: Non-Destructive Testing / Radiological Methods	Partner/user	CREATIF
6	Yair Sharan – Director	Tel-Aviv University - Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF)	Partner	FESTOS
7	Jaime Pereira - Rail infrastructure manager	Facilities and Railways Systems – rolling Stock and Technology management	Partner	DEMASST
8	David A Ritchie - Chancellor, Masters and Scholars	University on Cambridge	Partner	TERASEC
9	Roman Peperhove – Director	Institute for Cooperation Management and Interdisciplinary Research, Berlin	Partner	FESTOS
10	Edward Galea – Professor	University of Greenwich	Partner	BeSeCu
11	Tristan Simonart	European Commission	Security Research Unit, CBRN project officer, H3	NA
12	Clément Williamson	European Commission	Security Research Unit, CBRN project officer, H3	NA

NA – Not applicable

CBRN in PASR and FP7 SEC Calls

B

The table below provides a summary of the treatment of CBRN in the annual work programmes of PASR and FP7 SEC respectively.

Work Programme	Types of CBRN Activity Supported
PASR 2005	Issues for project implementation: • Demonstration of effective integration of active and passive sensor techniques, suitable for a wide range of platforms and data correlation techniques for detection and identification systems. • Demonstration of the viability of technologies and protocols for personnel, facilities and equipment decontamination against biological or chemical or other substances. • Assessment and identification of the overall needs of an enlarged EU for bio safety level 4 laboratories in order to guarantee optimal complementarity and development of effective methodology for networking.
PASR 2006	• Effective integration of various sensor techniques and data correlation techniques for fast, sensitive and affordable detection and identification of (i) explosive devices or (ii) biological substances. • Technologies for protection and countermeasures against (i) the impact of explosions, or (ii) the effects of CBRN with an emphasis on biological EN 6 EN releases. • Tools for the detection of illicit trade of WMD and their means of delivery.
FP7 2007-2008	**Function: Detection, identification & authentication** **Topic SEC-2007-1.3-01 Stand-off scanning and detection of hidden dangerous materials, objects or stowaways, fast and reliable alerting and specification.** Aim: to develop stand-off large throughput scanning capabilities required to pick out from a stream suspect items, such as drugs, CBRN(E), hidden objects or persons, including both fast narrow scanning in specific streams, and wide area scanning with sufficient granularity to enable law enforcement to intervene. The steps to take will be (a) very fast alerting with low false alarm rates on a broad class of objects and substances, (b) after the alarm and within reasonable time identification of a type of substance and (c) very thorough analysis and profiling on the biological or chemical components of specific substances. Call: Security Research Call 1 Funding scheme(s): Collaborative project. **Function: Intelligent surveillance and enhancing border security** **Topic SEC-2007-3.2-02 Unregulated land borders and wide land surveillance system:** Aim: To develop an integrated, adaptable land border and large area (including rough or devastated environments) surveillance system. It will be able to detect and locate (the movements of) individuals, vehicles, and hazardous substances (e.g. CBRNE) crossing unregulated land borders and, when required, track and trace their movements thereafter. It will combine novel dedicated remote or autonomous platforms equipped with multi-sensor data acquisition systems (of different types such as chemical and biological) with active imaging (such as radar, infrared, visible). Call: Security Research Call 1 Funding scheme(s): Collaborative project **Function: Restoring security and safety in case of crisis** **Topic SEC-2007-4.2-02 Integrated specialist search and rescue system:** Aim: To develop an integrated system to improve the ability to locate, assess, and rescue injured and/or contaminated victims in a CBRNE or natural disaster environment. This will include the detection of buried people; the use of sensors (acoustics, radars, video streaming, etc.) to enhance situation awareness; on-site monitoring of damaged structures and the environment; basic service systems (e.g. power generation); the ability to transmit, receive, and display data from specialist centres (command and control); mobile and autonomous specialist rescue and extraction equipment; biotechnological and medical counter measures; rapid decontamination; temporary protection during rescue and shelter for victims; etc. Call: Security Research Call 1 Funding scheme(s): Collaborative project.

CBRN in PASR and FP7 SEC Calls

B

	Topic SEC-2007-4.3-04 Neutralisation of devices/effects: Technical content / scope: In order to contain and limit the effects of terrorist devices - including CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) and firearms - on the environment, the task is to develop novel, fast, wide range, mobile and easy to use approaches to the neutralisation of devices and effects, including techniques and systems for isolation, shielding, decontamination, etc. Call: Security Research Call 1 Funding scheme(s): Collaborative project.
FP7 2009	**Increasing the Security of Citizens:** Activities to: • *Detect, track, trace, identify and neutralise CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) – both 'traditional' and 'home grown'.* Technical applications for demonstration projects were supported with a consistent portfolio of counter measures for CBRNE along the chain from prevention to response and recovery. CBRNE will require an integrated approach to threat assessment and consequence modelling, detection and identification of agents and devices, incident management tools, infrastructure protection mechanisms for individuals and environments, decontamination processes/techniques and medical care. Improvement and demonstration areas include**:** • *Affordable networked sensor systems for CBRNE alerting and detection;* • *Rapid identification sensor equipment and systems for CBRNE and precursor chemicals* • *Integrated monitoring system of CBRNE sensors combined with a monitoring system that traces and tracks people, goods and platforms.* • *Development of portfolio of real time spread prediction models capable of integration into existing command and control environments* • *Integration of CBRNE monitoring networks in existing sensor, transaction and distribution networks.* • *Protection measures, systems and processes for infrastructure and civilian populations.* • *Decontamination systems and methods applicable to civilian environments.* • *The development of large scale pre- and post-incident medical care.* **Intelligence Surveillance and Enhancing Boarder Security:** Activities to: • *Address border security through integrated border management. Create a coordinated and integrated security system to ensure the security of goods supply chains and logistics networks, while addressing traceability, standardisation and more affordable robust solutions as well as reduction of unit cost and screening times* **Restoring Security and Safety in Times of Crises:** Address two challenges: • *First by ensuring that governments, first responders and societies are better prepared prior to unpredictable catastrophic incidents using new, innovative and affordable solutions.* • *Second, improve the tools, infrastructures, procedures and organisational frameworks to respond and recover more efficiently and effectively both during, and after, an incident.*
FP7 2010	**Function: Intelligent surveillance and enhancing border security** **Topic SEC-2010.4.2-2 Preparedness and Resilience to a CBRN crisis:** Aim: to contain and limit the effects of such an event due to terrorists or linked to industrial accidents, the task is 1) to integrate capabilities and to develop a system of tools and methods to improve and coordinate operational reaction following the occurrence of the event 2) to develop information and training kits to the public and to specific audiences envisaged before (preparedness) and after the event (response). The system includes early warning systems, isolation, shielding, decontamination, medical counter-measures etc. Societal reaction, communication and human factors for first responders Call: Security Research Call 3, Funding scheme: Collaborative Project