Expected results

COUNTERFOG will result in the development and characterization of the system with a guide for use, efficiency assessment and other parameters.

It will lead to the development, test and demonstration of a practical, fast, harmless and efficient system for neutralization of CBRN attacks and decontamination of large areas, including a way to track the progress of decontamination.

It will produce a set of demonstrated decontamination agents suitable for use in COUNTERFOG and an assessment of their expected efficiency. Particular attention will be focused on test the effectiveness of the system to counteract against combined risks that can arise as a consequence of terrorist attacks or accidents.

As a result of the tests, practical guides and know-how about the best way to install and use the COUNTERFOG will be provided.

PARTNERS	COUNTRY
Universidad de Alcalá (UAH)	Spain
University of Strathclyde (STR)	United Kingdom
Institute of Solid State Physics. Bulgarian Academy of Sciences (BAS)	Bulgaria
Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT)	Spain
Institute of Inorganic Chemistry. Academy of Sciences of Czech Republic (IIC)	Czech Republic
Consilium Marine & Safety AB (CONSILIUM)	Sweden
BPE e.K. (BPE)	Germany
Sección Española de la Asociación Europea de Ferroviarios (AEC-ES)	Spain
Universidad Carlos III de Madrid (UC3M)	Spain
Vojensky Vyzumny Ustav SP (VVU)	Czech Republic

FRESP / Advanced first response respiratory protection

© Loren Rodgers - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218138
Total Cost
€4,074,891.01
EU Contribution
€3,029,967
Starting Date
01/06/2008
End Date
31/05/2012

Coordinator

ECOLE ROYALE MILITAIRE – KONINKLIJKE MILITAIRE SCHOOL
Avenue de la Renaissance 30
BE-1000 Brussels
Belgium
Contact
Dr. Peter Lodewyckx
Royal Military Academy – DEAO
E-mail: Peter.Lodewyckx@rma.ac.be
Website: www.rma.ac.be/fp7-fresp

Project objectives

Protection against terrorism is one of the major issues of this programme. If an incident occurs, despite precautions taken to prevent incidents at all, it is important to reduce the consequences, i.e. to minimise the effects of chemical, biological, radiological and nuclear (CBRN) attacks.

The objective of the project is to create the network of scientists and research institutions, who will develop a broad-spectrum, low-burden, tailor-made nanoporous adsorbent, with the aim to integrate the two main areas of protection (versus chemical warfare agents and versus toxic industrial chemicals) without a significant loss of capacity in either of them. It will also integrate features that are not at all (certainly not explicitly) available in the current state-of-the-art adsorbents: protection against radioactive gases and against biological threats.

This integration requires an in-depth study of mutual effects of impregnates and impregnation methods, as well as ways to diminish the deleterious effect of water vapour on the adsorption capacity. Moreover, the possibility of a commercialisation procedure for the new adsorbents will be investigated.

Description of the work

The primary goal of this project is the development of broad-spectrum low-burden respiratory protection systems for first responders. The first step in this process is developing novel nanoporous sorbents, combined with new or existing types of additives for chemisorption, possibly in combination with catalytic conversion, to neutralise weakly adsorbed components. The new nanoporous adsorbents and additives can be integrated or can be combined in mixtures or separate layers.

Specific tasks have been selected in order to meet project objectives:

» Nanoporous adsorbent development

- Development of nanoporous adsorbent materials with increased protection against toxic industrial chemicals (TIC) such as ammonia and highly volatile organics, chemical warfare agents, radiological and biological threats;
- Development of materials with low burden in weight and breathing resistance;
- Health and safety examination of the sorbents (flammability, ecotoxicity, mechanical resistance, etc.).

» Evaluation and optimisation of adsorbent performance

Establishment of the relation between the structural characteristics and interfacial properties of the adsorbent's performance. Application of Model Predictive Control (MPC) to optimise the preparation conditions in order to achieve the required optimum structure and performance.

» System development

Development of a new gas mask canister and protective hood, both based on the new nanoporous adsorbent.

» *System evaluation and optimisation of the performance*

- Determination of the optimum characteristics for the advanced respiratory protection systems;
- Optimisation of the filter and hood systems.

» *Economic feasibility and manufacturability, exploitation and dissemination, IPR policy*

Examination of viability of a full scale production of the nanoporous adsorbent, the filter canister and the hood.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Ecole Royale Militaire - Koninklijke Militaire School (RMA)	Belgium
Budapest University of Technology and Economics (BME)	Hungary
University of Brighton (UoB)	United Kingdom
University of Alicante (UALI)	Spain
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
High Technology Filters s.a. (HTF)	Greece
MAST Carbon (MAST)	United Kingdom
NORIT Nederland B.V (NORIT)	The Netherlands
Laser Optical Engineering Ltd. (LOE)	United Kingdom
ProQares BV (ProQares)	The Netherlands

IFREACT / Improved First Responder Ensembles Against CBRN Terrorism

© IFREACT

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285034
Total Cost
€5,475,980.60
EU Contribution
€3,394,615.40
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

UNIVERSITE PARIS XII- VAL DE MARNE
SAMU 94
51 Avenue de Lattre de Tassigny
94000, Creteil, France
Contact
Dr. Catherine Bertrand
Tel: +33 1 45 17 95 29
Mobile: + 33 6 82 82 24 11
Fax: + 33 1 45 17 95 30
E-mail: catherine.bertrand@hmn.aphp.fr
Website: www.ifreact.eu

Project objectives

IFREACT aimed to provide the next generation of protective clothing for first responders. Bringing together leading protective technology and blending it with some of the latest software, it enhanced the chemical, biological and radiological protection of European first responders. European major cities continue to face the threat of terrorism and, in the near future, may be subject to a serious chemical, biological or radiological terrorist attack. When the time comes it will be the brave men and women of the various emergency services who will answer the call – and they need to be adequately protected and prepared.

Description of the work

The consortium delivered qualitative and quantitative evaluation of existing Personal Protective Equipment (PPE) by both a laboratory and end-users and focused its research on the most emergent threats in order to best fulfil the needs of those end-users who are in the greatest need of protection from both terrorist and non-terrorist related crises. Once this preparatory work had been completed, it was tempered by direct feedback from the user community, and the team began to work on prototype ensembles that:

» address the real protection needs of conventional users, with regards to both the level of protection and its total capacity;

» provide adequate protection, while keeping the burden of the system as low as possible;

» include solutions for hand and foot protection, whilst taking safety, ergonomic and logistic aspects of the conventional user group into consideration;

The protective system provided added functionality regarding the C4I needs of the first responder. Typical tactical needs such as communication, (indoor) localisation & situational awareness, were enabled by affordable, robust and easy to use technology. Wearability, graceful degradation and logistics dictated innovative approaches to the material as well as to the system level;

The suit was configured as a platform that carries the energy and the connections to the components of the sensor subsystem. The sensors itself was housed in the suit as well as in the respirator, depending on their function. The configuration of the system enabled other / new energy cells and sensors to be connected whenever required;

This platform has been interfaced with the external infrastructure to get extra capabilities/situation awareness without constraints and cost as regards the suit itself.

Moreover, the project developed a platform that allows end-users and procurement staff to best select the PPE system needed for the mission of the first responder and the expected threat.

Results

Major EU cities continue to face the threat of terrorism and in the near future, may be subject to serious chemical, biological, or radiological terrorist attacks.

IFREACT succeeded in providing the next generation of protective clothing for civilian first responders integrating the latest knowledge and needs of end users. IFREACT created highly protective and user-friendly ensembles (a combination of three types of airway protection including an innovative one-size overpressure hood and three types of skin protection).

Bringing together leading protective technology, (Saratoga air-permeable material) providing low physiological burden, and combining it with some of latest software, integrating communication devices (audio/voice, images, text, etc.) will give EU first responders high situational awareness and agility. It also comprises a miniature integrated bio-collector and a PPE selection tool. Laboratory and field tests proved the level of protection and usability of the ensembles.

http://www.dailymotion.com/video/x2hedey_projet-europeen-ifreact-vostfr_school

PARTNERS	COUNTRY
Universite Paris XII- Val de Marne (SAMU)	France
IB Consultancy BV (IBC)	The Netherlands
NBC-SYS SAS (NBC Sys)	France
Blücher GmbH (Blücher)	Germany
Astrium SAS (Astrium)	France
Falcon Communications Limited (CBRNe World)	United Kingdom
Bertin Technologies SAS (Bertin)	France
Statni Ustav Jaderne, Chemicke a Biologicke Ochrany vvi (SUJCHBO)	Czech Republic
Drzavna Uprava za Zastitu i Spasavanje (DUZS)	Croatia
Prometech BV (Prometech)	The Netherlands
Hotzone Solutions Benelux (Hotzone Solutions)	The Netherlands

MIRACLE / MobIle Laboratory for the Rapid Assessment of CBRN Threats Located within and outside the EU

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312885
Total Cost
€1,420,617.05
EU Contribution
€1,130,605.00
Starting Date
01/12/2013
End Date
31/05/2015

Coordinator

UNIVERSITÉ CATHOLIQUE DE LOUVAIN (UCL)
Centre de Technologies Moléculaires Appliquées (CTMA)
Clos Chapelle-Aux-Champs
UCL- B1.30.24
1200 – Brussels - Belgium
Contact
GALA JEAN-LUC
Tel: +32 2 764 33 32
+32 2 764 33 65
Mobile: +32 495 59 78 13
Fax: +32 2 764 31 66
E-mail:
Jean-luc.gala@uclouvain.be
Website:
http://www.uclouvain.be/ctma.htlm

Project objectives

In case of major intentional, accidental or natural CBRN incidents, the speedy detection and identification of agents on scene are crucial to ensure adequate risk assessment, optimal risk management, and proper counter measures. Consequently, a determining factor is to bring a rapidly deployable CRBN diagnostic and forensic capacity as close as possible to the crisis area.

However, there are many different ways to develop mobile capacities as a countermeasure in case of a CBRN-event. In that respect, the C, B, or RN specificity of the threat is of paramount importance, as is the possibility to have scalable capacities and joint multinational intervention.

The objective of MIRACLE was to harmonise the definition of a mobile CBRN laboratory, define the needs, and subsequently provide solutions for the deployment of this capacity within and outside the EU.

Description of the work

A set of scenarios were developed in which a mobile laboratory capacity would be of added value. The scenarios were divided by agent (C, B or RN) and location (within or outside the EU). For each scenario, the criteria used to elaborate on the development of a mobile capacity was the potential cross-border impact of the CBRN incident and the potential added value of a rapidly deployable capacity (no matter in what form). Accordingly, we defined and analysed the type of missions of a deployable capacity according to a set of eight scenarios of Chemical, Biological, Radiological and Nuclear cross-border incidents within and outside Europe.

A state of the art of existing capacities within the EU, and a gap analysis were carried out to identify actions for improvement and to assess the best possible organisational and operational architectures that enable sustainability at optimal costs for society. The role of national or international regulatory authorities and agencies was reviewed to assess who should be the stakeholders of CBRN mobile capacities, and how to coordinate activities and EU mechanisms of CBRN crisis management. The interface with existing EU capabilities and expertise was taken into consideration. A strong emphasis was put on other synergistic EU and non-EU projects.

Practicalities (i.e., structures, equipment and functions including operational procedures, communication, logistics, forensics and related legal issues) were assessed with technological suppliers and end-users. Building partnerships and cooperation with interested stakeholders (e.g., EU key actors, nations within and outside the EU in strong demand for this type of capacity) was a specific task dedicated to the dissemination of the MIRACLE project.

Results

The project's outcome was a set of deliverables describing the needs and solutions for a mobile CBRN laboratory capacity and the proposal of a flexible evidence-based mobile CBRN laboratory architecture that was scalable, modular, and interoperable if requited by the type, location, magnitude and length of the crisis.

Recommendations were provided and formulated in a position paper (short and long versions available) written according to policy-maker requirements. Both versions (see reference hereafter) are open access and can be downloaded from http://www.uclouvain.be/ctma

References:

- Long version: D6_3 Recommendations
- Short version: Short-Position Paper_MIRACLE-2015-10-28

PARTNERS	COUNTRY
Université catholique de Louvain (UCL)	Belgium
Astrium SAS (AST)	France
Bundeswehr Institute of Microbiology (IMB)	Germany
Forsvarets forskningsinstitutt (FFI)	Norway
Totalforsvarets forskningsinstitut (FOI)	Sweden
Nederlands Forensisch Instituut (NFI)	The Netherlands
Health Canada (PHAC)	Canada
Police Service of Northern Ireland (PSNI)	United Kingdom
National Institute of Public Health & the Environment / RijksInstituut voor Volksgenzondheid en Milieu (RIVM)	The Netherlands

MULTIBIODOSE / Multi-disciplinary biodosimetric tools to manage high scale radiological casualties

© rolffimages - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241536
Total Cost
€4,580,243.01
EU Contribution
€3,493,199
Starting Date
01/05/2010
End Date
30/04/2013

Coordinator

STOCKHOLM UNIVERSITY CENTRE FOR RADIATION PROTECTION RESEARCH
Department of Genetics, Microbiology and Toxicology
Stockholm University
Svante Arrhenius väg 20C
106 91 Stockholm
Sweden
Contact
Andrzej Wojcik
Tel: +46 8 16 1217
Mobile: +46 762 122 744
Fax: +46 8 16 4315
E-mail:
andrzej.wojcik@gmt.su.se
Website:
www.multibiodose.eu

Project objectives

In the event of a large scale radiological emergency, biological dosimetry is an essential tool that can provide timely assessment of radiation exposure to the general population and enable the identification of those exposed people who should receive immediate medical treatment. A number of biodosimetric tools are potentially available, but they must be adapted and tested for a large-scale emergency scenario. These methods differ in their specificity and sensitivity to radiation, the stability of signal and the speed of performance. A large scale radiological emergency can take different forms. Based on the emergency scenario different biodosimetric tools should be applied so that the dosimetric information can be made available with optimal speed and precision.

Description of the work

One work package (WP) will be devoted to each tool. Starting with the state of the art, each tool will be validated and adapted to the conditions of a mass casualty situation. A training programme will be carried out where appropriate and automation as well as commercial exploitation of the tools will be investigated and pursued. Towards the end of the project, a comparative analysis of the tools will be carried out with respect to their sensitivity, specificity and speed of performance. Future training programmes will be developed. Two additional WPs will deal with: (1) the development of an integrated statistical software tool that will allow fast interpretation of results, and (2) the development of a guidance document, based on the TMT handbook, regarding the logistics of biodosimetric triage in a large scale accident and decision making regarding the methods best suitable for a given accident scenario. Moreover, a programme of disseminating the results among European emergency preparedness and radiation protection authorities will be carried out, so that the functional laboratories and networks can be easily contacted in the case of an emergency.

The project beneficiaries will be supported by an advisory committee that will include experts in bio-dosimetric tools and management of radiation accidents.

Results

The MULTIBIODOSE project analysed and adapted a variety of biodosimetric tools for assessing radiation exposure to the general population and enabling the identification of those exposed who should receive medical treatment.

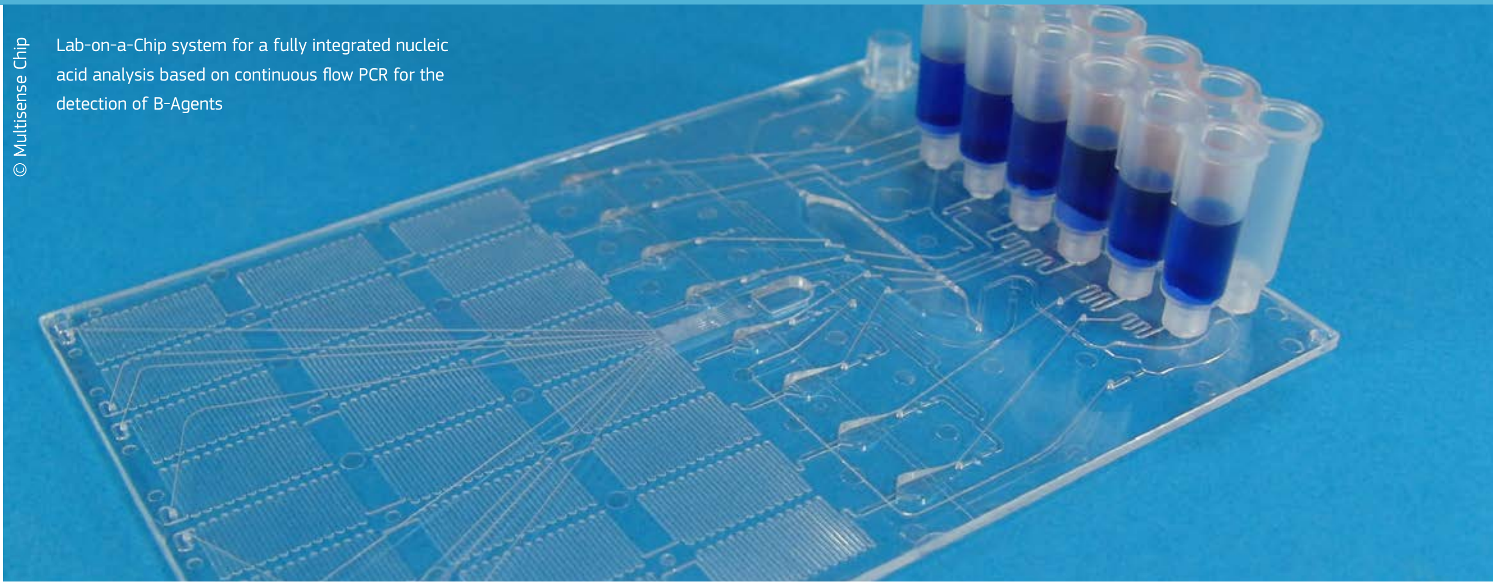
The following biodosimetric tools were tested: dicentric assay, micronucleus assay, gamma-H2AX assay, blood serum protein expression assay and electron paramagnetic resonance (EPR)/optically stimulated luminescence (OSL) dosimetry in components of pocket electronic devices.

The project also established a biodosimetric network called “Realizing the European Network of Biodosimetry” (RENEB), which kicked off January 2012. The goal of RENEB is to establish a sustainable European network in biological dosimetry involving laboratories and organisations from 16 countries that can support a coordinated response in case of major nuclear or radiological emergency in Europe. All MULTIBIODOSE partners are members of RENEB, and all biodosimetric tools developed and validated in MULTIBIODOSE are also included in the network. Within RENEB an exercise and training program was developed that will be pursued in the future.

The project also produced a software package for integrated statistical analysis of data from each of the assays described. Full details of the software functions are given in the manual which is available for download, using the software from the web page of MULTIBIODOSE. The software and manual were finalised and tested with the assistance of all project participants.

PARTNERS	COUNTRY
Stockholm University Centre For Radiation Protection Research (SU)	Sweden
Bundesamt für Strahlenschutz (BfS)	Germany
Universiteit Gent (UGent)	Belgium
Health Protection Agency (HPA)	United Kingdom
Institut de Radioprotection et de Sûreté Nucléaire (IRSN)	France
Istituto Superiore di Sanità (ISS)	Italy
Norwegian Radiation Protection Authority (NRPA)	Norway
Radiation and Nuclear Safety Authority (STUK)	Finland
Westlakes Scientific Consulting (WSC)	United Kingdom
Universitat Autonoma de Barcelona (UAB)	Spain
Institute of Nuclear Chemistry and Technology (INCT)	Poland
Helmholtz Zentrum München (HMGU)	Germany
Bundeswehr Institut für Radiobiologie in Verbindung mit der Universität Ulm (UULM)	Germany
University of Oxford (UOXF)	United Kingdom
EURADOS (EURADOS)	Germany

MULTISENSE CHIP / The lab-free CBRN detection device for the identification of biological pathogens on nucleic acid and immunological level as lab-on-a-chip system applying multisensor technologies



© Multisense Chip

Lab-on-a-Chip system for a fully integrated nucleic acid analysis based on continuous flow PCR for the detection of B-Agents

Information

Grant Agreement N°
261810
Total Cost
€8,986,775
EU Contribution
€6,619,399.50
Starting Date
01/06/2011
Duration
48 months

Coordinator

MICROFLUIDIC CHIPSHOP GMBH
Stockholmer Str.20
07747 Jena, Germany
Contact
Andrzej Wojcik
Dr. Claudia Gärtner
Tel: +49 3641 3470511
Mobile: +49 172 52 58 506
Fax: +49 3641 3470590
E-mail: Claudia.Gaertner@microfluidic-ChipShop.com
Website:
www.multisense-chip.com

Project objectives

The goal of Multisense Chip is the development of a detection and identification system for biological pathogens, which shall include both the sample preparation stage, during which target molecules are extracted directly, and the nucleic-acid-based and/or immunological detection and identification steps.

The chosen technologies offer several advantages: on the one hand, a small, portable, and easy-to-use device can be realized due to miniaturization; on the other, the so-called lab-on-chip technology enables operation outside of lab settings, meaning that the complete analysis including sample preparation, extraction of target molecules, etc. will be carried out in a small device the size of a microtiter plate with all necessary reagents on board. This includes dry reagent storage of lysis reagents, master mixes for the PCR, antibodies, and liquid storage of buffers. The overall target is a "sample in, result out"-type handling procedure.

Description of the work

The overall goal is the realization of a complete analysing system for biological pathogens consisting of a micro-nano-based consumable chip with integrated sensor technology, an innovative instrument to run the chip, as well as the respective biological assays themselves.. Finally this will be embedded in advanced information and communication technologies. To cope with this multidisciplinary work from the technical and application side and to ensure full compliance with ethical aspects connected to the intended use of the system, the work will be arranged in thirteen work packages. A detailed requirement specification combined with regular design reviews will guide the way to a proper project run. The technical work packages are grouped around the biological assay, the sensor technology and micro- and nanofabrication technologies. The system and integration tasks will be covered within the microfluidics, software, communication and instrumentation work packages. An important aspect within the project is the validation and demonstration task for ensuring a proper performance and usability of the system. The training aspect in particular of future users to get them in touch with lab-on-a-chip technology as early as possible is an important aspect as well. To guarantee the awareness and proper handling of ethical issues an independent work package was installed.

To realize the integrated system, the following latest enabling technologies will be applied:

» **Sample enrichment: Novel air sampling technologies** and sampling procedures easily combinable with a chip;

» The target material for the biological assays and tests will be extracted on-chip via **novel micro-nanotechnological devices** combined with advanced biochemistry;

» **Microfluidics** allows for fast and efficient hybridization of the PCR products on the capture microarray, implementing **3D-nanotechnology**;

» **Electrochemiluminescence-based** detection or **electrochemical sensors** ensure ultrasensitive detection.

Expected results

The aim is to produce a portable analytical instrument for the detection and identification of biological pathogens on the molecular and immunological levels. This system will be based on a portable instrument and a lab-on-a-chip as a consumable. It will combine sample enrichment, extraction of the target molecules from the sample, the biological reaction and finally the carrying out of the detection reaction via innovative sensor technologies.

PARTNERS	COUNTRY
Microfluidic ChipShop GmbH (MFCS)	Germany
Bertin Technology (BT)	France
Friedrich Loeffler Institut (FLI)	Germany
Integrated Microsystems for quality of Life SL (iMicroQ)	Spain
Institut für Mikrotechnik Mainz (IMM)	Germany
Universitat Rovira i Virgili (URV)	Spain
Institute of Physical Biology (IFB)	Slovenia
Cedralis (CED)	France

PRACTICE / Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment PRACTICE

© PRACTICE

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261728
Total Cost
€11,695,072
EU Contribution
€8,424,029
Starting Date
01/05/2011
End Date
31/10/2014

Coordinator

UMEA UNIVERSITY
European CBRNE Centre
Linneaus väg 6
90187 Umea, Sweden
Contact
Dzenan Sahovic
Tel: +46 (0) 90 786 5774
Mobile: +46 (0) 73 073 5303
Fax: +46 (0) 90 786 6681
E-mail: dzenan.sahovic@cbrne.umu.se
Website: www.umu.se/cbrne

Project objectives

The objective of the PRACTICE project was to improve the preparedness and resilience of the Member States and Associated Countries countries to an attack from a terrorist group using non-conventional weapons such as CBRN (Chemical, Biological, Radiological and/or Nuclear agents) materials. This was done with the help of a newly developed integrated CBRN incident management toolbox.

Description of the work

The development of a new toolbox was based on:

» identification, organization and establishment of knowledge of critical elements in the event structure through studies of a wide selection of scenarios, real incidents and exercises;

» analysis and identification of gaps in the current response situation and organization and integration of the allocated response capabilities or functions in a toolbox of equipment, procedures and methods; and

» an allocated system or kit for public information, decision-support, first-responder training and exercises.

These response capabilities functions were to a great extent universal in character and independent of national organizational structures. Particular attention was given to integration and understanding of human factors and societal aspects in all the parts of the project. The final concept and integrated response system (toolbox) and subsystems were tested and validated. A whole system demonstrator was shown and tested in the final phases of the project.

Results

The project's main achievement is the PRACTICE Toolbox, an integrated system for CBRN incident management. The toolbox was validated in a series of live large-scale validation exercises and it proved to be useful for both planning, training, response, and recovery activities. The toolbox was validated in three different national contexts (Sweden, Poland and UK) to demonstrate its adaptability to pre-existing CBRN management systems and different national legal and political contexts. Specific achievements in R&D activities are:

» Analysis of gaps in existing CBRN incident management systems and CBRN management tools.

» Development of a novel CBRN incident management concept, specifying observable incident parameters, and response functions that are universal in character and not dependant on organisational structure and national context.

» Development of the PRACTICE Toolbox architecture, which is open, flexible, and adaptable to different national contexts.

» Development and integration of a number of specific tools in following categories:

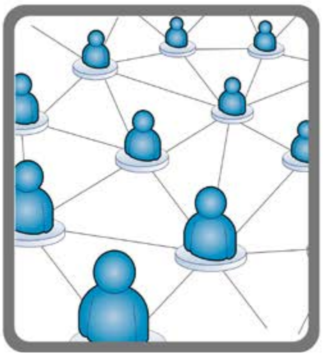
- observational tools supporting situational awareness,
- integration of live information (such as maps, location of available resources),
- integration of static information (guidelines, recommendations/protocols),
- action tools (such as sensors, modeling software, etc.).

» Amongst the developed tools, PRACTICE project also developed dedicated information kits for communication with the public, and a dedicated training kit enabling use of the PRACTICE Toolbox for purposes of first responder training.

PARTNERS	COUNTRY
Umea University (UmU)	Sweden
Forsvarets forskningsinstitutt (FFI)	Norway
ASTRIUM S.A.S. (AST)	France
Cassidian S.A.S. (EADS)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
KING'S COLLEGE LONDON (KCL)	United Kingdom
IB Consultancy BV (IBC)	The Netherlands
CBRNE Ltd (CBRNEltd)	United Kingdom
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRD)	Greece
Totalförsvarets Forskningsinstitut (FOI)	Sweden
UNIVERSITE CATHOLIQUE DE LOUVAIN (UCL)	Belgium
Netherlands Forensic Institute (NFI)	The Netherlands
STATNI USTAV JADERNE, CHEMICKE A BIOLOGICKE OCHRANY vvi (SUJCHBO)	Czech Republic
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
SELEX GALILEO LTD (SELEX)	United Kingdom
ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (AstriPL)	Poland
COMITE EUROPEEN DE NORMALISATION (CEN)	Belgium
Szkola Glowna Sluzby Pozarniczej (SGSP)	Poland
MITTUNIVERSITETET (MIUN)	Sweden
Prometech BV i.o. (PRO)	The Netherlands
BRUHN NEWTECH A/S (BNT)	Denmark
HEALTH PROTECTION AGENCY (HPA)	United Kingdom
SODERSJUKHUSET AB (SPC)	Sweden

A4A / Alert for All

© DLR



Information

Grant Agreement N°
261732
Total Cost
€4,881,506
EU Contribution
€3,497,469
Starting Date
16/03/2011
Duration
30 months

Coordinator

DEUTSCHES ZENTRUM FÜR LUFT- UND RAUMFAHRT E.V.
Institute of Communications and Navigation
Linder Hoehe
51147 Cologne
Germany
Contact
Cristina Párraga Niebla
Tel: +49 (0) 8153 282824
Mobile:
+49 (0) 1727134781
Fax: +49 (0) 8153 282844
E-mail:
Cristina.Parraga@dlr.de
Website: www.alert4all.eu

Project objectives

The overall objective of A4A is to improve the effectiveness of alerts and communication to the population in crisis management.

To achieve this goal, A4A will provide an extensive and interdisciplinary alerting framework that integrates the key enablers to achieve significant improvements in terms of the level of alert penetration, cost-benefit ratio and intended vs. actual impact of alert strategies. With the project results, A4A aims at contributing to lay the foundations of an effective alert and communication paradigm that is scalable from the regional to pan-European range.

A4A will provide solutions to align alert procedures and processes in contemporary crises (natural or man-made) with available and emerging information management and communication technologies, emerging information sources and trends in social and human behaviour.

Description of the work

A4A builds its alerting concept on five research areas that are key enablers to achieve the aimed effectiveness improvements: authorities' and responders' operations, human behaviour, the role of new media, information management and communications technologies.

As a multi-disciplinary alerting framework, A4A will develop and exploit synergies among its research areas. In particular, the A4A work plan foresees the following research activities:

» To develop a suitable communications protocol and a scalable alert message dispatcher that connects several mass market communications technologies to disseminate alerts in a multi-channel approach, including satellite components, to consumer devices, providing ubiquitous penetration of the alert system and resilience in the face of major disasters;

» To develop a portal for efficient information management that enables the coordination and common situational awareness of involved authorities and responders, enhancing the (common) operational picture for optimizing the alert strategies;

» Situational awareness and trends in social behaviour will be addressed from two different perspectives: (i) understanding the impact of alerts in the population and (ii) understanding the role of new media, such as social networks, during the crisis. The first aspect will be tackled by research and modelling of social behaviour in crisis. From this research, an alert impact simulation tool will be developed to support decision making processes in crisis management. The second aspect will be tackled by investigating the information flows and their timing during crisis to understand the role of new media and by developing tools to efficiently monitor the information exchanges within new media to improve the situational awareness of authorities, especially on the perception of the society of the crisis situation;

- The integration of these research activities will allow for defining recommendations for the improvement of operational concepts that make use of and benefit from the A4A tools. Furthermore, the development of training material for authorities and responders will contribute to the end user acceptance.

Investigations on organisational, institutional and funding aspects for the deployment of A4A and a final showcase will complete the A4A activities.

Expected results

Through its research activities A4A will provide an extensive and scalable alerting and communications concept that is capable of optimising the penetration and impact of alerts and can be incrementally deployed, both in terms of technologies/features and in terms of operating range, from a regional to a pan-European scope.

PARTNERS	COUNTRY
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
German Red Cross (DRK)	Germany
Avanti Communications Ltd. (AVA)	United Kingdom
BAPCO LBG (BAPCO)	United Kingdom
TECNOSYLVA S.L. (TSYL)	Spain
Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)	Portugal
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Universität Stuttgart (USTUTT)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	Germany
Eutelsat S.A. (EUT)	France
Institut fuer Rundfunktechnik GmbH (IRT)	Germany

AF3 / Advanced Forest fire Fighting

Information

Grant Agreement N°
607276
Total Cost
€19,270,384.14
EU Contribution
€12,985,486.14
Starting Date
01/05/2014
Duration
35 months

Coordinator

Finmeccanica-Selex ES S.p.A (SES)
EC & Regional Projects
Technical Coordination
Piazza Monte Grappa, 4
00195 Roma - Italy
Contact
Cecilia Coveri
Tel: +39 0558950057
Mobile: +39 3357499660
Fax: +39 0558950600
E-mail:
cecilia.coveri@selex-es.com
Website: www.selex-es.com

Project objectives

The AF3 project objective is to substantially improve the efficiency of current fire-fighting operations and the protection of human lives by developing innovative technologies which allow a high level of integration between existing and new systems.

The AF3 project evaluates the readiness and capabilities of existing fire countermeasures. It aims to overcome current operational gaps via a framework to enhance monitoring and firefighting methods with solutions that tackle inefficiency.

The AF3 technological objectives are to develop:

» innovative active and passive fire countermeasures

» advanced integrated crisis management

» Early detection and monitoring technologies (including public channels)

Description of the work

AAF3 project focuses its activities on the following areas:

» Innovative active countermeasures: implementation of the novel AAFF (Advanced Aerial Fire Fighting) system to accurately and safely disperse extinguishing materials from high altitudes by aircrafts and helicopters in any condition

» Innovative passive countermeasures: fast build-up of preventive defensive lines of capsules to prevent the spread of fire from forest to populated areas

» Advanced Integrated Crisis Management: An innovative AF3 Core Expert Engine that coordinates all firefighting missions, composed of a command-and-control centre, a real-time risk analysis tool and a fire fighting laboratory multipurpose simulation tool to predict the progression of a fire and the effectiveness of countermeasures.

» Early detection and monitoring: deployment of diverse systems, including satellites, airplanes, UAVs, and both mobile and stationary ground systems for early detection and for monitoring smoke and toxic clouds.

» Advanced public information channels: smart phones, internet and dedicated broadcasting will be integrated in the global system

The AF3 work plan has been sub-divided into 10 work packages, three of which run the whole length of the project. The seven operational work packages follow a chronological sequence and are broken down into sub-work packages addressing different aspects of fire emergencies. Ethical and legal issues of each activity are taken into account.

The involvement of end-users, particularly in the definition phase, the organisation of trials and the evaluation phase ensure that AF3 should attain its goals.

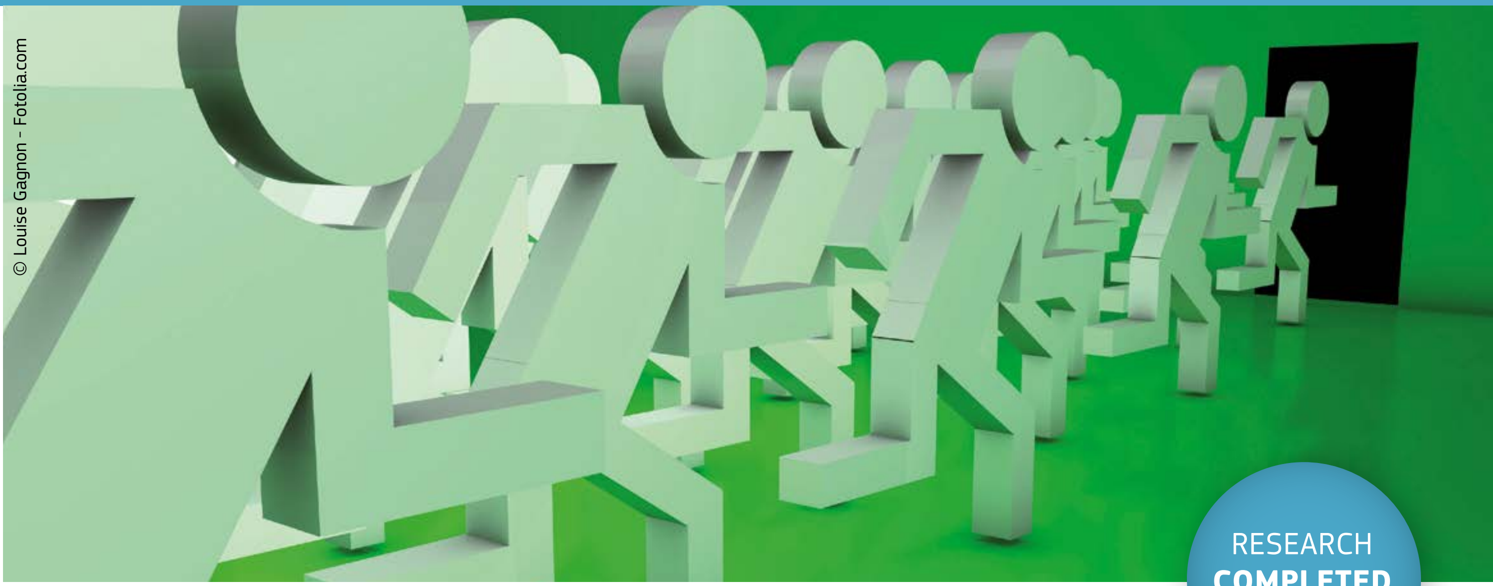
Expected results

The project work plan includes three sections of field tests:

- pre-final real fire carried out in Greece, with the cooperation of the Hellenic Ministry of Defence, finalised to assess AF3 advanced firefighting capabilities compared to conventional aerial firefighting
- real firefighting flight test carried out in Spain, with the cooperation of the Spanish National Authority, finalised to test the accuracy and the efficiency of the Advanced Aerial Firefighting system
- final comprehensive integrated demo carried out in Israel, with the cooperation of the Israeli Ministry of Public Security, finalised to demonstrate the international interoperability.

PARTNERS	COUNTRY
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
German Red Cross (DRK)	Germany
Avanti Communications Ltd. (AVA)	United Kingdom
BAPCO LBG (BAPCO)	United Kingdom
TECNOSYLVA S.L. (TSYL)	Spain
Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)	Portugal
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Universität Stuttgart (USTUTT)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	Germany
Eutelsat S.A. (EUT)	France
Institut fuer Rundfunktechnik GmbH (IRT)	Germany

BESECU / Human behaviour in crisis situations: a cross-cultural investigation in order to tailor security-related communication



© Louise Gagnon - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218324
Total Cost
€2,705,344.54
EU Contribution
€2,093,808
Starting Date
01/05/2008
End Date
31/12/2011

Coordinator

ERNST-MORITZ-ARNDT-UNIVERSITAT GREIFSWALD
Lehrstuhl Gesundheit
und Pravention
Institut fur Psychologie
Robert-Blum-Str. 13
17487 Greifswald
Germany
Contact
Prof. Silke Schmidt
Tel: +49 (0) 3834 863810
Fax: +49 (0) 3834 863801
E-mail: silke.schmidt@uni-greifswald.de
Website: www.besecu.de

Project objectives

Floods, fires, earthquakes or terrorist events in Europe raise important questions about human behaviour in crisis situations. Does culture play a role in how people respond to these events? More important: could a better understanding of cultural responses help define better emergency communication and evacuation procedures?

That was the goal of BeSeCu: to investigate cross-cultural and ethnic differences in human behaviour during crisis situations to produce tailor-made security-related communications, instructions and procedures. Its field work involved 1130 survivors and 3011 first responders.

Focused on eight European countries, BeSeCu carried out:

- video-tape analysis and the simulation of real-time evacuation scenarios;
- assessment of first responder roles and how communities were affected;
- standardized evaluation of survivors' cognitive, behavioural and emotional response to fires, terrorist attacks, floods or earthquakes.

Results

One of BeSeCu's discoveries was that it is possible to cross-culturally assess different types of incidents using a set of standard psychological tools. The project also discovered that different crisis situations incite different psychological impacts, with fires and building collapses producing the highest post-traumatic stress symptoms and floods the lowest.

Survivors with high post-traumatic stress levels reported significantly higher risk perception, levels of dissociation, panic and physiological reactions. They also had less time to inform themselves about the situation or to prepare for evacuation. As a result, they acted "automatically" or instinctively during the crisis. However, all survivors reported a common impulse toward supportive social behaviour such as helping other victims, sharing food and water, etc.

Among other findings, BeSeCu's research:

- produced a set of scientifically sound and cross-culturally validated instruments ("BeSeCu-S") to assess human behaviour in security-relevant crisis situations across cultures of survivors of disasters;
- extracted original data from 300 firefighters per country regarding their professional experience in crisis situations and culturally-relevant concepts of emergency operations, leading to new evidence about non-verbal communication by first responders;
- confirmed that information about the crisis itself is critical for occupants to response appropriately;

- developed two comprehensive evacuation model validation data sets from Turkish and Polish evacuation trials;
- confirmed that while behaviour and cognitions differ across cultures, common indices were identified regarding prevention, knowledge and safety culture habits.

BeSeCu's work will inform future R&D efforts focused on improving communication and emergency procedures regarding the links between culture and evacuation behaviour.

© Besecu

PARTNERS	COUNTRY
Ernst-Moritz-Arndt-Universitat Greifswald	Germany
University Medical Centre Hamburg	Germany
University of Greenwich, School of Computing and Mathematical Sciences	United Kingdom
Institute of Public Security of Catalunya	Spain
Hamburg Fire and Emergency Service Academy	Germany
Man-Technology-Organisation (MTO)-Psychology	Sweden
Faculty of Fire Safety Engineering (SGSP)	Poland
Prague Psychiatric Centre University of Prague	Czech Republic
Association of Emergency Ambulance Physicians	Turkey
Alma Mater Studiorum - Università di Bologna (UNIBO)	Italy

BRIDGE / Bridging resources and agencies in large-scale emergency management

© BRIDGE

RESEARCH COMPLETED

Information

Grant Agreement N°
261817
Total Cost
€18,075,144.20
EU Contribution
€12,983,143.75
Starting Date
01/04/2011
Duration
30/06/2015

Coordinator

STIFTELSEN SINTEF
Forskningsveien 1
P.O. Box 124 Blindern
0314 Oslo
Norway
Contact
Geir Horn
Tel: +47 22067561
Mobile: +47 93059335
Fax: +47 22067350
E-mail: geir.horn@sintef.no
Website: www.sintef.no

Project objectives

BRIDGE's goal is to increase the safety of citizens by developing technical and organisational solutions that significantly improve crisis and emergency management.

A BRIDGE platform will provide technical support for multi-agency collaboration in large-scale emergency relief efforts. The key to this is to ensure interoperability, harmonization and cooperation among stakeholders on the technical and organisational level. The vision of the BRIDGE project is to:

» facilitate cross-border and cross-agency collaboration;
» allow the creation of a common, comprehensive, and
» reliable operational picture of the incident site;
» enable integration of resources and technologies into workflow management;
» enable active ad-hoc participation of third parties.

Social practices, ethical concerns and legal and bureaucratic demands must be taken into consideration during the realization of this vision. Therefore, BRIDGE will facilitate constructive deep integration of multi-dimensional social, legal and ethical analysis into ambitious interdisciplinary user-led socio-technical innovation.

Description of the work

BRIDGE elaborated solutions for the generation and distribution of 3D simulations of emergency situations for use in training and in case of an emergency. The visual presentation of threat scenarios and their consequences were designed to help link the differences in technical and operational backgrounds between the parties involved.

In addition, BRIDGE developed technical solutions in three different areas.

» Interoperability of data, systems & technology to:
- manage heterogeneous ad-hoc networks
- handle information in different formats & from different sources
- collect & manage context information

» Exploration of a common operational picture to:
- develop intelligent, adaptive & multimodal user-interface
- obtain, filter, share, & annotate information
- provide a decision support tool for crisis management

» Runtime inter-agency & inter-agent collaboration to:
- allow the dynamic creation & composition of interagency workflows
- carry out actor-agent networks & agent-based simulations
- facilitate a shared situational awareness

Results

BRIDGE's realistic scenarios in real-world environments led to yearly demonstrations of the BRIDGE platform under different foci. Its exploitation activities targeted three groups: emergency management end-user communities in different European countries, industrial partners, and non-BRIDGE technology and solution providers in Europe.

Its results included:

- Resilient ad-hoc network infrastructures, focusing on the requirements evolving from emergency scenarios
- Generic, extensible middleware to support integration of data sources, networks, and systems
- Context management system to foster interoperability of data, providing meaningful, reliable information

To exploit the ever-increasing amount of data in emergency management, intelligent human-computer interaction techniques are needed to make these data usable. BRIDGE developed:

- adaptive, multi-modal user interfaces
- novel stationary and mobile interaction techniques
- approaches on how to raise awareness through visualization of ad-hoc networks

The BRIDGE system supports the flexible assembly of emergency response systems into a 'system of systems' for agile emergency response. The project also developed systems called Concept Cases representing end-user applications whose implementation is based on individual parts and services of the BRIDGE system.

PARTNERS	COUNTRY
Stiftelsen SINTEF (SINTEF)	Norway
Almende B.V. (Almende)	The Netherlands
CNet Svenska AB (CNET)	Sweden
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FIT)	Germany
Lancaster University (ULANC)	United Kingdom
Crisis Training AS (CTAS)	Norway
SAAB Training Systems (SAAB)	Sweden
THALES Nederland BV (THALES NL)	The Netherlands
Universität Klagenfurt (UNIKLU)	Austria
Paris-Lodron-Universität Salzburg (PLUS)	Austria
VSH Hagerbach Test Gallery LTD (VSH)	Switzerland
Technische Universiteit Delft (TUDelft)	The Netherlands
Stockholms Universitet (US)	Sweden
Helse Stavanger (RAKOS)	Norway

CascEff / Modelling of dependencies and cascading effects for emergency management in crisis situations

Information

Grant Agreement N°
607665
Total Cost
€4,626,904.00
EU Contribution
€3,594,937.80
Starting Date
01/04/2014
Duration
36 months

Coordinator

SP SVERIGES TEKNISKA FORSKNINGSINSTITUT (SP)
Fire Research
Brinellgatan 4
Box 857
SE-50115 Borås, Sweden
Contact
Prof. Anders Lönnermark
Tel: +46 10 516 5691
Mobile: +46 722 255691
Fax: +46 33 416012
E-mail:
anders.lonnermark@sp.se
Website: www.sp.se

Project objectives

Modern socio-technical systems are increasingly characterised by high degrees of interdependencies. Whereas these interdependencies generally make systems more efficient under normal operations, they contribute to cascading effects in times of crises.

CascEff will improve our understanding of cascading effects in crisis situations through the identification of initiators, dependencies and key decision points. The main objectives of the CascEff project are to:

1. gain a better understanding of the cascading effect in crisis situations.

2. develop an "incident evolution tool" for predicting present and future crisis evolution leading to cascading effects.

3. identify human activities in the crisis.

4. improve incident management for present and future threats.

Description of the work

The experiences from past incidents and findings on initiators, dependencies and key decision points will be further developed in the methodological framework of the incident evolution tool. This will enable improved decision support, contributing to the reduction of collateral damages and other unfortunate consequences associated with large crises. Use of the tool will be validated through its integration into different incident management and training platforms representing different end users in the project (e.g. NoKeos, iCrisis, RIB, WIS and XVR).

The work with CascEff is divided into five research work packages:

WP1: Incident management. A methodology will be developed for incident management which integrates predictions of an incident's evolution as based on an improved understanding of cascading effects. The methodology will be developed on the basis of identified and elaborated scenarios, taking into account cascading effects and their effect on the evolution of scenarios.

WP2: Originators and dependencies. The WP aims to identify essential characteristics that are required for development of an incident evolution tool with the aim to manage cascading effects. This includes the development of a methodology for analysing previous incidents regarding their originators, dependencies, and consequences.

WP3: First responders tactics, human activities, interaction and behaviour. The aim is to identify which human activities need to be taken into account during key points in an incident's evolution where decisions need to be made. This work package will also develop a methodology for communication and coordination during crisis situations that reflects the respective roles of members of the public, media organisations, first responders and intervention commanders at different levels.

WP4: Incident Evolution Tool development and implementation in existing systems. The incident evolution methodology that will incorporate cascading effects will be implemented into incident management frameworks used by end users in Europe today. The tools will be developed in close cooperation with end users (first responders, emergency managers, decision makers, etc.).

WP5: Scenario development and simulated exercises.

Scenarios will be devolped for testing the incident command methodology and tools. In addition there is one work package for dissemination of the results (WP6) and one for project management (WP7).

Expected results

The project will produce models of dependencies and effects in crisis situations (of both physical and human components) causing a cascading effect. It will also provide a methodology to create this model for future threats, and tools to foresee the evolution of an incident. These tools will be available on a real time basis as well as for planning and training purposes, in particular in cross border crisis situations.

This will lead to reduced direct and indirect consequences by:

- Reducing the extent of crisis scenarios subject to cascading effects and the risk for cross border scenarios Highlight the need for cross border collaboration in response to specific originators
- Promote new response strategies and structures and methodologies
- Include development of a cloud monitoring system for multi-hazard events
- Improve both the evacuation of large areas in crisis situations and the use and role of the media in crisis situations

PARTNERS	COUNTRY
SP Sveriges Tekniska Forskningsinstitut (SP)	Sweden
Lunds Universitet (ULUND)	Sweden
Myndigheten för Samhällsskydd och Beredskap (MSB)	Sweden
Universiteit Gent (UGent)	Belgium
Institut National de L'environnement et des risques (INERIS)	France
Service Public Federal Interieur (KCCE)	Belgium
Safety Centre Europe BVBA (SCA)	Belgium
Université de Lorraine (UL)	France
University of Leicester (ULEIC)	United Kingdom
Northamptonshire County Council (NFRS)	United Kingdom
E-Semble BV (ESM)	The Netherlands

CAST / Comparative Assessment of Security-Centered Training Curricula for First Responders on Disaster Management in the EU

© Gail Johnson- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218070
Total Cost
€2,719,068.55
EU Contribution
€1,974,620
Starting Date
01/07/2009
End Date
30/06/2011

Coordinator

UNIVERSITAT SALZBURG
Office of the Rectorate
Research Support Unit
Kapitelgasse 4-6
A-5020 Salzburg
Austria
Contact
Prof. Friedrich Steinhäusler
Tel: +43 662 8044 5700
Mobile: +43 680 123 7158
Fax: +43 662 8040 150
E-mail: Friedrich.steinhaeusler@sbg.ac.at
Website:
www.research.sbg.ac.at/cast

Project objectives

The CAST project aimed to address the future needs of EU first responders (FR) from across the 27 Member States for handling a disaster scenario that exceeds in severity any existing training assumption – i.e., a catastrophic terrorist incident or an extremely large-scale “once in a life-time” natural or man-made disaster.

The project sought to identify and categorise a range of unusually extreme disaster scenarios of natural, man-made or terrorist origins. It then aimed to map and evaluate existing training and equipment preparation, and to produce a standardised modular training curriculum to prepare FR staff for these threats. Finally, it tried to streamline and standardise current cross-border preparation in these areas, to avoid pan-European duplications of effort.

Results

This project’s deliverables included a range of new research in the field of disaster preparedness and training.

For identifying potential threat scenarios, the consortia created DERMI – the Database on Emergency Response Major Incidents. Containing 110 real-life incidents from across Europe, Russia and the US, DERMI provided a comprehensive catalogue of disaster scenarios to support the project’s analysis.

A comprehensive survey of existing training programmes for disaster management was also conducted. Featuring 80 responses from across 25 EU Member States, covering themes such as the division of responsibility during a terrorist attack and procedures for the use of protective equipment.

Utilizing the surveys and reports, CAST then formulated a series of “best practice” procedural guides to form the basis of common training curricula for FR staff.

Low probability-high consequence threat scenarios that were explored included the wide area synchronised use of improvised explosive devices, large-scale chemical, biological or radiological releases in urban environments and chemical fires. These were then compared to existing equipment and training procedures to evaluate overall preparedness.

The recommendations and new procedural priorities suggested include:

- making the DERMI database available to all stakeholders;
- preplanning risk assessment in industrial facilities;
- focusing on control room design, structure, future development and management;
- enhancing communication technologies;
- developing new support technologies for CBRNE detection, mobile labs, drone surveillance and protective equipment;
- basing preparation for future large scale accidents based on lessons-learnt from disasters in the 21st century.

PARTNERS	**COUNTRY**
Universität Salzburg (PLUS)	Austria
DSTS-Advisers to Executives (DSTS)	Austria
Fire Service Academy Hamburg (FSAH)	Germany
Research Institute of Red Cross (FRK)	Austria
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT)	Germany
BMLVS / Heereslogistikschule (HLogS)	Austria
International Security Competence Center (ISCC)	Austria
University of Defense Brno (UDB)	Czech Republic
Corvinus University Budapest (VGT)	Hungary
SAAB Training Systems AB (SAAB)	Sweden
Swedish Counter Terrorist Police (SCTU)	Sweden
Diamond Aircraft Industries (DAI)	Austria
Tecnatom (TEC)	Spain
Sigmund Freud Privatuniversität Wien (SFU)	Austria
Police Service of Northern Ireland (PSNI)	United Kingdom

COncORDE / Development of Coordination Mechanisms During Different Kinds of Emergencies

Information

Grant Agreement N°
607814
Total Cost
€4,077,483.20
EU Contribution
€3,378,211.25
Starting Date
01/05/2014
Duration
36 months

Coordinator

Cambridge University Hospitals NHS Foundation Trust (CUH)
EU Unit
Department of Strategy and Planning
Addenbrooke's Hospital, Hills Road
Management Offices, Box 146
CB20QQ, Cambridge, United Kingdom
Contact
Dr. Toni Staykova
Tel: +44 1223274718
Mobile: +44 7765037485
Fax: +44 1223274719
E-mail: as2305@medschl.cam.ac.uk
Website: www.cuh.org.uk

Project objectives

1. Improve preparedness and interoperability of medical services during emergencies and mass disaster events, which affect the health and well-being of large parts of the population at local, regional or cross-border level.

2. Optimise the coordination and quality of response of an open ecosystem of users, to allow for different constellations of crisis response participants according to the demands of the situation.

3. Facilitate ongoing monitoring, evaluation and improvement of response and integration of all results into an intelligent training system, that allows enrichment by users.

Description of the work

Phase 1 – establish the requirements and specifications of the COncORDE platform, and how it will fit together with the current systems used by the domain experts across Europe and beyond.

Phase 2 – Technology research and system design

Phase 3 – Evaluation and trials to test and validate the COncORDE platform against a series of evaluation criteria through the use of case studies and large scale pilots.

Phase 4 – Impact, Dissemination and Exploitation

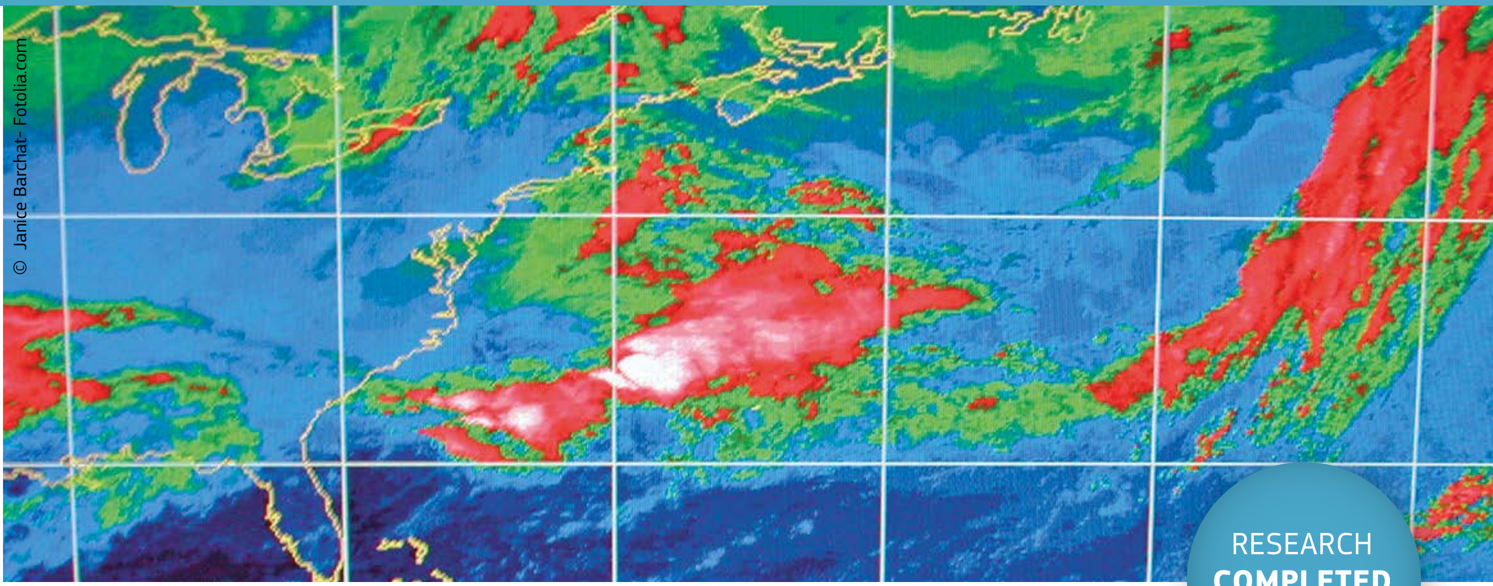
Phase 5 – Co-ordination and Project management

Expected results

The output of COncORDE will be a set of tools with existing technology solutions, to be used by emergency medical responders for in-action (operational) needs and for after-action evaluation. The set of tools will allow participants positioned in different spaces during a response to collate and share information gathered from responders, data sources and the public. This will facilitate a common operational picture, the logging of all activities and record patient data, and evaluation of the response for learning and improved preparedness. It will be based on commonalities of response between member states in order to gain EU wide validity and will be aligned with business-as-usual operational systems in order to enable easy uptake. COncORDE will offer decision support for resource management through enabling collection and integration of reliable data.

PARTNERS	COUNTRY
Cambridge University Hospitals NHS Foundation Trust (CUH)	United Kingdom
European Dynamics Advanced Systems Of Telecommunications Informatics And Telematics (ED)	Greece
Inovamais - Servicos De Consultadoria Em Inovacao Tecnologica S.A. (Inova+)	Portugal
Koç University (KU)	Turkey
University Of Cyprus (UCY)	Cyprus
Elliniki Omada Diasosis Somateio – Hellenic Rescue Team (HRT)	Greece
Stichting Crisislab (CrisisLab)	The Netherlands
Siveco Romania SA (Siveco)	Romania
Crisis Training AS (CTAS)	Norway
Teknologian Tutkimuskeskus VTT (VTT)	Finland
National Center For Scientific Research “Demokritos” (NCSR)	Greece
Konnekt-able Technologies Limited (KT)	Ireland
Public Safety Communication Europe Forum AISBL (PSCE)	Belgium
ESRI Portugal - Sistemas E Informacao Geografica SA (ESRI)	Portugal

COPE / Common Operational Picture Exploitation


© Janice Barchat- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217854
Total Cost
€3,886,574
EU Contribution
€2,535,049
Starting Date
01/02/2008
End Date
31/01/2011

Coordinator

TECHNICAL RESEARCH CENTRE OF FINLAND
P.O. Box 1000
FI-02044 VTT
Finland
Contact
Jari Hämäläinen
Tel: +358 20 722 6467
Fax: + 358 20 722 6027
E-mail: jari.hamalainen@vtt.fi
Website: http://cope.vtt.fi/

Project objectives

First responders are a heterogeneous group regarding their emergency environments, their roles, command structures, and organisational and national frameworks.

COPE's goal was to improve the performance reliability and cost of emergency response management "C2" (command and control) systems by combining user-oriented human factors with technology development. A central aim was to strengthen information flow from and to first responders to boost situational awareness across agencies and at all levels of the C2 chain in emergency management situations.

A user-driven approach therefore drove COPE's development of new technologies that support information requirements at the scene of an event. The project applied a wide range of human-factor methods – from functional task modelling to end-user simulations – to better understand individual agencies, and to ensure that new systems match requirements and can be integrated with legacy processes and technologies.

Results

COPE's obtained its results from its key work packages, which focused on:

» a generic concept for a common operational picture (COP);

» analysis of first responder activity (fire fighters, sector commanders and incident commanders) in three countries;

» technology mapping to align user requirements with hardware solutions;

» definition of user-driven scenarios and key performance indicators.

These led to two exercises: a live one involving first responders and actual fire and hazards events, and a tabletop one with end-users involved in additional C2 and decision-making tasks.

The culmination of COPE's work packages resulted in end-user assessment of technology-in-design using trials and questionnaires. Based on a set of criteria for modern and future COP systems derived from leading international projects, a detailed evaluation of the state of the art achieved was produced, which takes into account technological, operational, and end-user evaluations.

For example, COPE studied the use and benefits of wearable displays, sensors and locational technologies to support first-responders. The advantages and disadvantages of such technologies were identified. According to feedback from first responders and external stakeholders, the system and its components produced “good” to “very good” levels of satisfaction. Though there were certain temporary failures and reductions in functionality, these did not undermine the validity of the project’s overall research results, according to the COPE consortium.

PARTNERS	COUNTRY
TECHNICAL RESEARCH CENTRE OF FINLAND (VTT)	Finland
UTI SYSTEMS S.A. (UTI)	Romania
CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)	Germany
Pelastusopisto, Emergency Services College (ESC)	Finland
Ministry of Interior and Administration Reform (IGSU)	Romania
BAE Systems C-ITS (BAE Systems C-ITS)	Sweden
THE PROVOST, FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY COLLEGE DUBLIN (TCD)	Ireland
BAE SYSTEMS (OPERATIONS) LIMITED (BAE Systems UK)	United Kingdom
SKYSOFT PORTUGAL - SOFTWARE E TECNOLOGIAS DE INFORMAÇÃO SA (Skysoft)	Portugal

CRISCOMSCORE / Developing a crisis communication scorecard

© volant - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217889
Total Cost
€1,013,207
EU Contribution
€799,174
Starting Date
01/02/2008
End Date
30/04/2011

Coordinator

UNIVERSITY OF JYVÄSKYLÄN YLIOPISTO
Department of Communication (Matarankatu 6)
P.O. Box 35 (TOB)
FI - 40014 University of Jyväskylä
Finland
Contact
Marita Vos, prof.
Tel: +358 14 260 1554
Mobile: +358 50 4410 358
Fax: +358 14 260 1511
E-mail: marita.vos@jyu.fi
Website: http://www.crisis-communication.fi

Project objectives

The purpose of this project was to improve public and media crisis communications during natural or man-made security incidents, disasters and emergencies.

To meet this goal the project had four key objectives:

- identify critical factors for an effective media strategy before, during and after crisis situations;
- identify critical factors for communication with citizen groups before, during and after crisis situations;
- construct a scorecard for public authorities to measure and improve their readiness to communicate in crisis situations;
- stimulate implementation by hosting and encouraging the use of the Crisis Communication Scorecard and the Strategy Guides.

Results

CRISCOMSCORE's conclusions were based on extensive best practice studies, assessments of scientific literature, empirical research to clarify existing communications co-operation in end-user response networks and an overview of the current level of reception to such information in stressful situations. These were reported in published strategy guides and academic journals.

These findings then formed the basis for measurable performance indicators in the Crisis Communications Scorecard – an online auditing tool that can be accessed free of charge by all crisis management professionals at: http://www.crisiscommunication.fi/criscomscore/

The scorecard presents critical factors in the communication of public authorities with stakeholders such as citizens, news media, and other response organisations before, during and after emergencies. It separates its analytics into three separate categories, focused on steps which can be taken before, during and after a crisis. In each category, a range of table-top exercises, planning meetings and outcome studies are required to feed into the auditing process.

The final analysis gauges the effectiveness of an organization's communications strategy using a system inspired by business efficiency auditing techniques. It concentrates on key success factors and reveals strong and weak points in performance, thereby enabling the prioritization of resource allocation by participants.

As well as the published strategy guides and scorecard, the website platform hosts a range of advice and recommendations for improving crisis communications.

PARTNERS	COUNTRY
University of Jyväskylä Yliopisto	Finland
Ben Gurion University of the Negev	Israel
University of Tartu	Estonia
Norwegian University of Science and Technology	Norway
Emergency Services College Finland	Finland

CRISIS / Critical incident management training system using an interactive simulation environment

© Francois Doisnel - Fotolia.com

Information

Grant Agreement N°
242474
Total Cost
€4,593,444.66
EU Contribution
€3,495,611.99
Starting Date
01/05/2010
Duration
36 months

Coordinator

MIDDLESEX UNIVERSITY HIGHER EDUCATION CORPORATION
School of Engineering & Information Sciences,
London NW4 4BT
United Kingdom
Contact
Prof. William Wong, BCom (Hons.) PhD FN-ZCS – Head, Interaction Design Centre.
Tel: +44 20 8411 2684
E-mail: w.wong@mdx.ac.uk
Website: http://idc.mdx.ac.uk/projects/crisis/
http://www.eis.mdx.ac.uk/research/idc/

Project objectives

The goal of the CRISIS Collaborative Project is to research and develop in Europe:

» A training and simulation environment focusing on real-time decision making and responses to simulated but realistic critical incidents, focusing on problem diagnosis, planning, re-planning, and acting, rather than just procedural training;

» A distributed, secure, scalable, based on state of the art computer games technology, enabling collaborative and interactive simulation and on-demand training environment for crisis management training in airports, for individuals and team-based activities at command post levels;

» A readily configurable software architecture that can be used at other critical sites such as nuclear power plants;

» A flexible platform that functions as a test bed and evaluation tool for new and current operational procedures.

Description of the work

The project will be executed over a 36-month period in three stages:

» *First stage* – spiral concept development cycle where mock-ups and existing prototypes will be used to illustrate the full CRISIS approach;

» *Second stage* – the design and development of the CRISIS components will take place. The prototype will draw on insights derived from the research team covering crisis management decision support and advanced interaction technology. Early evaluation will be combined with training to give early feedback to the users. The components will then be adjusted during development and before final integration starts;

» *Third stage* – The components will be integrated into a secure architecture together with supporting tools.

Expected results

The expected impacts are:

To develop for airport crisis managers, a prototype simulation training system that will allow users across different organisations and nations to interactively experience and manage crisis and security threats in a simulated airport environment. This will enhance their operational readiness and preparedness to respond to hostile actions at airports. It will also allow users to train on demand, more frequently, and at different levels of the organisation.

PARTNERS	COUNTRY
Middlesex University Higher Education Corporation (MU)	United Kingdom
SHELTERLAND ApS - 3D CONNECTION (CRI)	Denmark
National Aerospace Laboratory (NLR)	The Netherlands
ObjectSecurity Ltd (OS)	United Kingdom
Space Applications Services (SAS)	Belgium
VSL Systems AB (VSL)	Sweden
Linkoping University (LiU)	Sweden
Haskoli Island - University of Iceland (HI)	Iceland
A E Solutions (BI) Ltd (AES)	United Kingdom
Aeroportos de Portugal, SA (ANA)	Portugal
British Transport Police Authority (BTP)	United Kingdom
Flugstodir (ISAVIA)	Iceland

CRISMA / Modelling crisis management for improved action and preparedness

© GYI NSEA - istockphoto.com

RESEARCH
COMPLETED

Information

Grant Agreement N°
284552
Total Cost
€14,397,298
EU Contribution
€10,107,160
Starting Date
01/03/2012
End Date
31/08/2015

Coordinator

VALTION TEKNILLINEN TUTKIMUSKESKUS
Tekniikankatu 1
P.O. Box 1300
FI-33101 Tampere, Finland
Contact
Anna-Mari Heikkilä
Tel: +358 20 722 3490
Mobile: +358 20 722 3490
Fax: +358 20 722 3499
E-mail:
Anna-mari.heikkila@vtt.fi
Crisma.coordinator@vtt.fi
Website: www.crismaproject.eu

Project objectives

CRISMA IP focused on large-scale crisis scenarios with immediate and extended human, societal, structural, and economic, often irreversible, consequences, and impacts. These crisis scenarios cannot be managed just by regular emergency and first responder resources, but instead require multi-organizational and multi-national cooperation including humanitarian aid.

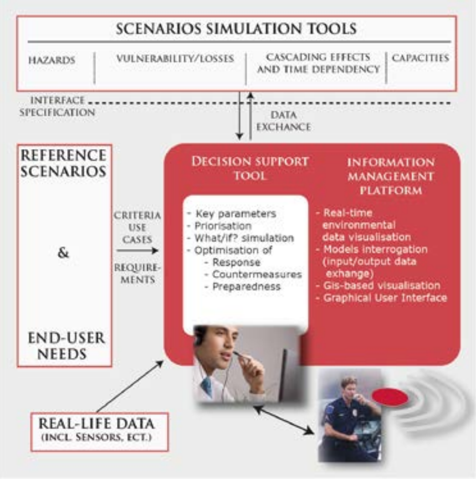
CRISMA planned to develop an integrated planning and decision support tool set that facilitates simulation and modelling of realistic crisis scenarios with possible cascading and multi-risk effects, potential preparation and response actions, and the impact of crisis depending on both the external factors driving the crisis development and the various actions of the crisis management team. The CRISMA tool set aimed to enable decision makers and crisis managers to:

1. Model possible multi-sector crisis scenarios and assess the consequences of an incident
2. Simulate possible impacts resulting from alternative actions
3. Support strategic decisions on capabilities, related investments, reserves, and inventories
4. Optimize the deployment of resources dedicated to crisis response in line with the evolvement of a crisis, and
5. Improve action plans for preparedness and response phases of the crisis management.

Description of the work

CRISMA built upon the existing tools and facilities provided by its research, industry, SME and end-user partners, and took into account the existing structures and practices as well as the research and development work done in the EU and its member states. The work was carried out in close cooperation with the end-user partners who have wide experience in crisis management in complex situations, including national disasters and global response activities.

The CRISMA work plan consisted of several sub-projects (SP) that were divided into several work packages. Those SPs defined Scenarios, Requirements and Criteria for Crisis Management Modelling for the development of CRISMA, and developed components for the Integrated Crisis Modelling System (ICMS) and Models for Multi-Sectoral Consequences. In the middle of the project, the first version of the CRISMA system components was tested and validated by the end-user pilots. End-User pilots should have tested and validated the CRISMA system and its components in two sequences, which provided feedback for the development work. The mid-term and final validation of CRISMA's results were performed in cooperation with the End-User Advisory Board.



© Crisma

Results

Instead of developing individual crisis management solutions, CRISMA developed a generic software framework, based on the methodology for simulation-based decision support. The CRISMA Framework is composed of a range of software components, models, and supporting tools in order to combine them for different simulation applications in various crisis domains.

Within the CRISMA Framework, crisis managers and other decision-makers have multiple possibilities to connect models, data, and expertise with from many sources for improving their understanding of complex crisis scenarios and awareness of alternative preparedness, response, and mitigation actions. Moreover, CRISMA scenario comparisons and visualization tools improve multi-organizational cooperation and common crisis perception as well as communication with other stakeholders and the public.

The feasibility of the Framework, the software components, and the underlying decision-support concepts have been tested and validated in five pilot sites, under monitoring of the CRISMA End-User Advisory Board. This set of illustrative cases demonstrated the benefits of CRISMA for different end-users in various crises, highlighting the flexibility of the CRISMA results.

CRISMA builds upon the existing tools and facilities, taking into account the existing structures and practices as well as the R&D work done in the EU and its member states. This has also been gratefully acknowledged by the end-user community.

PARTNERS	COUNTRY
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Analisi e Monitorraggio del Rischio Ambientale (AMRA)	Italy
AIT Austrian Institute of Technology GmbH. (AIT)	Austria
Association for the Development of Industrial Aerodynamics (ADAI)	Portugal
Tallinna Tehnikaulikool - Tallinn University of Technology (TTU)	Estonia
NICE Systems Ltd (NICE)	Israel
European Aeronautics Defence and Space Company – CASSIDIAN Division (EADS)	Germany
Insta DefSec (INS)	Finland
Spacebel S.A (SpB)	Belgium
Cismet GmbH (CIS)	Germany
Pelastusopisto - The Emergency Services College (ESC)	Finland
Magen David Adom (MDA)	Israel
Public Safety Communication Europe Forum (PSCE)	Belgium
Ilmatieteen laitos - Finnish Meteorological Institute (FMI)	Finland
Deutsches Rotes Kreutz (DRK)	Germany
ARTELIA Eau & Environnement (AEE)	France

DRIVER / Driving Innovation in Crisis Management for European Resilience

Information

Grant Agreement N°
607798
Total Cost
€46,270,988.80
EU Contribution
€33,468,209.00
Starting Date
01/05/2014
Duration
54 months

Coordinator

ATOS SPAIN S.A. (ATOS)
Atos Research and
Innovation (ARI)
C/ Albarracín 25
28037-Madrid-Spain
Contact
Fernando Kraus
Tel: +34 91 214 88 00
Mobile: +34 675 592 006
Fax: +34 91 754 3252
E-mail:
fernando.kraus@atos.net
Website: www.driver-project.eu

Project objectives

DRIVER aims to test and evaluate a wide range of emerging solutions that support professional responders, communities and individuals in crisis management (CM) and help build societal resilience. DRIVER will (i) assess and deliver CM solutions that can be combined to address different types of large-scale crises and (ii) develop better ways of evaluating future solutions via a distributed European test-bed infrastructure and evaluation methodologies. Solutions can be technologies, tools, methods, concepts, or recommendations regarding technical, organizational, procedural, legal, policy, societal, or ethical improvements to the European crisis management domain.

Description of the work

DRIVER investigates three complementary areas: civil society resilience, strengthened responders, and training and learning across borders:

» To improve the resilience of individuals, communities and local governments – especially civil society actors without professional CM training – DRIVER tests organisational and IT solutions for their psycho-social training potential, community engagement and local government assessment, strengthened crisis communication and spontaneous volunteer management aspects.

» To better deal with issues such as interoperability, information sharing, situation assessment, early warning, resource management, capacity building, and interaction with citizens, DRIVER assesses solutions of different maturity (mostly the outcomes of previous EC research projects).

» To enhance the capabilities of trainers and human resources (HR) professionals dealing with those involved in CM at an operational level DRIVER develops and tests a series of training modules and HR means and frameworks.

The DRIVER methodology centres on “campaigns of experiments”, building up step-by-step experience and knowledge with increasingly complex scenarios and combinations of solutions. Involving users, these build an evidence base for practitioners that compares the performance of new and legacy solutions. From initial, simpler campaigns in the three thematic areas, DRIVER proceeds to more complex crisis scenarios to understand how combined solutions interact at local, regional, national or international level. Ultimately joint experiments and a large-scale final demonstration will simulate highly complex scenarios and cross-border crisis situations.

This stepwise methodology will form an iterative route for gradually adapting emerging solutions to operational constraints, creating acceptance among users through their active involvement in the experiments, and providing proof to decision-makers that the solutions are cost-effective. Important advice is also provided by DRIVER’s “assessment and innovation”, which focuses on economic, societal, ethical, legal and standardisation issues of next-generation solutions, experiments, the test-bed and the stakeholder community.

Expected results

1. A distributed European test-bed of virtually-connected exercise facilities and crisis labs where end-users, providers, researchers, policymakers and other CM stakeholders can evaluate new solutions to emerging issues. This will encompass technological solutions, operational concepts, methodological guidelines, approaches and policies.

2. A collection of enhanced next-generation crisis management solutions related to civil society resilience; strengthened responders; training and learning across borders; guidance on ways to improve cost-effectiveness and further steps required for successful implementation (or an informed decision not to implement).

3. A vibrant community of stakeholders concerned by societal and technological innovation in crisis management and a shared common understanding of crisis management in Europe across emergency practitioners, research, first responders, industry and civil society.

PARTNERS	COUNTRY
Atos Spain SA (ATOS)	Spain
Totalforsvarets Forskningsinstitut (FOI)	Sweden
Austrian Red Cross Research Gmbh (ARC)	Austria
Thales Communications & Security Sas (TCS)	France
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Pole Euromediterraneen Sur Les Risques Association (POLE)	France
Arttic (ARTTIC)	France
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FhG)	Germany
Institutt For Fredsforskning Stiftelse (PRIO)	Norway
Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (DLR)	Germany
Dansk Rode Kors (Danish Red Cross) (DRC)	Denmark
The British Red Cross Society Royal Charter (BRC)	United Kingdom
Magen David Adom In Israel (MDA)	Israel
Gemeente Den Haag (THG)	The Netherlands
Bundesministerium Des Innern (THW)	Germany
Myndigheten For Samhallsskydd Och Beredskap (MSB)	Sweden
Ecorys Nederland B.V. (Ecorys)	The Netherlands
Edisoft-Empresa De Servicos E Desenvolvimento De Software Sa (EDI)	Portugal
Gmv Aerospace And Defence Sa Unipersonal (GMV)	Spain
Frequentis Ag (FRQ)	Austria
Hkv Lijn In Water Bv (HKV)	The Netherlands
Itti Sp Zoo (ITTI)	Poland
E-Semble Bv (E-Semble)	The Netherlands
Q4 Pr Limited (Q4PR)	Ireland
Public Safety Communication Europe Forum Aisbl (PSCE)	Belgium
Din Deutsches Institut Fuer Normung E.V. (DIN)	Germany
Ait Austrian Institute Of Technology Gmbh (AIT)	Austria
JRC -Joint Research Centre- European Commission (JRC)	Belgium
Association Pour La Recherche Et Le Developpement Des Methodes Et Processus Industriels - Armines (ARMINES)	France
Westfaelische Wilhelms-Universitaet Muenster (WWU)	Germany
European Union Satellite Centre (EUSC)	Spain
Institute Of Information And Communication Technologies (CSDM)	Bulgaria
Disaster Waste Recovery Lbg (DWR)	United Kingdom

EMILI / Emergency management in large infrastructures

© TebNad- Fotolia.com

Information

Grant Agreement N°
242438
Total Cost
€3,997,230.40
EU Contribution
€3,139,228
Starting Date
01/01/2010
Duration
36 months

Coordinator

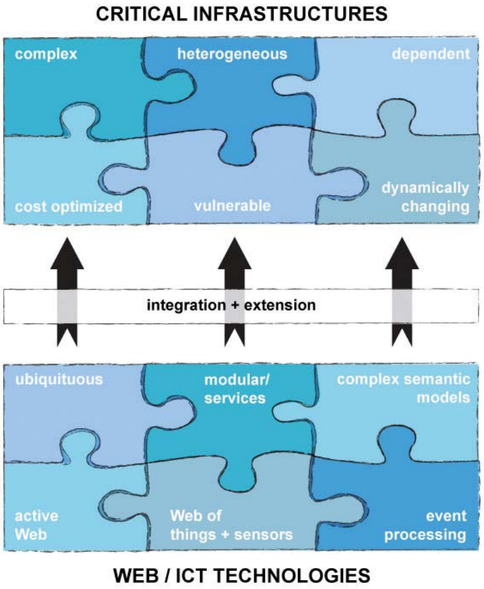
FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Schloss Birlinghoven
D-53754 Sankt Augustin
Germany
Contact
Dr. Rüdiger Klein
Tel.: +49 2241 14 2608
Fax: +49 2241 14 2342
E-mail: Ruediger.Klein@IAIS.Fraunhofer.de
Website: www.emili-project.eu

Project objectives

The project EMILI ("Emergency Management in Large Infrastructures") is a capability project which aims at a new generation of data management and control systems for large infrastructures (CIs) including appropriate simulation and training capabilities. New Internet-based technologies like active and reactive behaviour through complex event processing and event action rules will be developed and adapted. Semantic technologies will allow computer systems to capture the meaning of a large variety of information relevant in emergency management.

Description of the work

This is especially important in the case of emergencies and crises. Large Infrastructures are cost intensive, large, complex technical systems. They are frequently operated at their limits. Today, they are changing their characteristics rapidly in various respects. These CIs depend on each other and interact with each other in many ways. Even small disturbances may trigger avalanches of failures in the same system and in depending ones. Quick and adequate reactions are key factors in safe and efficient operations of Critical Infrastructures today. Currently used data management and control systems of large Infrastructures mainly collect data from their own system and process them in a more or less pre-defined way. In order to adapt today's control systems to the new challenges – especially to an efficient management of emergencies – we need a new generation of these control systems, and their methodology and technology.



© Emili

Expected results

This new generation of control systems is needed in order to improve the security of CIs like power grids and telecommunication systems, airports and railway systems, and oil and gas pipelines, under future technical, economic, organisational, political, and legal conditions. Especially with a view to an efficient management of emergencies – a new generation of these control systems, and their methodology and technology is needed.

EMILI's results will support the need for more complex and sophisticated control systems for CIs. This includes the necessary sophisticated human operator decision support. Training systems built on EMILI's technology will enable effective and efficient preparation of people for all relevant kinds of decision making in critical situations.

Airport, public transport (Metro) and power grid systems will serve as demonstration and validation bases.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAIS)	Germany
Asit AG	Switzerland
Aplicaciones en Informática Avanzada SA	Spain
Skytec AG Consulting in Information Technologies	Germany
Stichting Centrum voor Wiskunde en Informatica (CWI)	The Netherlands
Institut Mihajlo Pupin	Serbia
Ludwig-Maximilians-Universität München	Germany

IDIRA / Interoperability of data and procedures in large-scale multinational disaster response actions

© Tan Kian Khoon - Fotolia.com

Information

Grant Agreement N°
261726
Total Cost
€10,925,164.35
EU Contribution
€8,032,971.06
Starting Date
01/05/2011
Duration
48 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V
Hansastrasse 37C
80686 - Muenchen
Germany
Contact
Andreas Kuester
Tel: +49 (0) 351 4640 667
Mobile: +49 (0) 172 4117655
Fax: +49 (0) 351 4640 803
E-mail: Andreas.Kuester@ivi.fraunhofer.de
Website: http://www.ivi.fraunhofer.de

Project objectives

There are currently no disaster management procedures, tools and systems in the EU which fully take into account the specific requirements of large-scale international cooperation in emergency situations. Those actions are distinguished by many diverse emergency response organisations that need to collaborate across technological systems, organisational borders and language and cultural barriers. Technologies and procedures used and researched so far have provided many solutions for single aspects, but there is no concept available yet which supports the entire process.

In IDIRA we follow the vision of providing a conceptual framework that allows for supporting and augmenting regionally available emergency management capacities (including the existing IT systems) with a flexibly deployable Mobile Integrated Command and Control Structure. This system of technologies and guidelines is designed to help in optimal resource planning and operations across national and organisational borders.

Description of the work

As part of the analysis of the state of the art, the workflow in multinational disaster response actions is being modelled, and based on that a high-level specification of supporting technological components and a system integration concept for interoperability and interfaces is being designed.

As interoperable communication is a prerequisite for successful disaster management, the Consortium works on the integration of communication protocols for data exchange and voice communication interoperability. Furthermore data models for tasks and resources and the quick integration of geographic and attribute data as well as sensor data are being improved.

A core step is the provision of a common operational picture, including structured text communication over language barriers and information interchange for the provision of early situational awareness to unit leaders before leaving their home country. Planning and optimisation tools for missing persons' tracing are being integrated.

In the field of interoperable response management, a decision support system for coordinated multinational response planning and optimisation is provided. This includes micro simulation as an up-to-date technology for decision support. Additional fields of work are improvements in international donation management and multinational resource management for disaster response.

For training and dissemination purposes, local and binational field training sessions are carried out. Finally, three multi-national and multi-organisational exercises are being planned, covering flood, large-scale fire and earthquake or pandemic events.

At the final stage, a description of successful rules and procedures, the Architectural Reference for the Mobile Integrated Command & Control Structure and recommendations for harmonization and standardization in the European Union are being presented.

Expected results

The set of tools, interfaces and procedures developed in IDIRA provides services for data integration, information exchange, resource planning and decision support to disaster response units and decision makers. It is an architectural framework and an exemplary implementation of a Mobile Integrated Command and Control Structure supporting co-ordinated large-scale disaster management. The IDIRA solutions are building on and are being integrated with existing infrastructure and response procedures.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)	Germany
Salzburg Research (SRFG)	Austria
Frequentis (FRQ)	Austria
Brimatech Services GmbH (BRI)	Austria
National and Kapodistrian University of Athens (NKUA)	Greece
Earthquake Planning and Protection Organization (EPPO)	Greece
German Red Cross (branch of the state of Saxony) (DRK-SN)	Germany
University of Greenwich (UOG)	United Kingdom
IES Solutions (IES)	Italy
Flexit Systems (FLEXIT)	Austria
Austrian Red Cross Headquarters (ORK-HQ)	Austria
Hellenic Ministry of Defence (HMOD)	Greece
Department of Fire Brigade, Public Rescue and Civil Defence – Ministry of Interior (CNVVF)	Italy
Satways Ltd. (STWS)	Greece
TLP, spol. s r.o. (TLP)	Czech Republic
World Agency of Planetary Monitoring & Earthquake Risk Reduction (WAPMERR)	Switzerland
Local Government of Achaia Prefecture (NEA)	Greece
Center for Security Studies (KEMEA)	Greece

IMPRESS / IMPROVING PREPAREDNESS AND RESPONSE OF HEALTH SERVICES IN MAJOR CRISES

Information

Grant Agreement N°
608078
Total Cost
€4,280,345.60
EU Contribution
€3,251,315.15
Starting Date
01/05/2014
Duration
36 months

Coordinator

INTRASOFT
International SA (INTRA)
RID
RUE MONTOYER 40
1000 BRUXELLES - Belgium
Contact
BABIS IPEKTSIDIS
Tel: +32 22381717
Fax: +32 22381710
E-mail: Babis.IPEKTSIDIS@intrasoft-intl.com
Website:
www.fp7-impress.eu

Project objectives

The main objectives of the IMPRESS project are to:

» Re-balance the disproportion between response needs and health system capacity, through the proper mobilization of additional resources (material, logistics, and health personnel) and enhanced organization (e.g. e-triage, and interoperability of health services).

» Remediate the information deficit with the rapid collection of relevant data, and exchange of adequate information. Support decision making according to the impact of crisis and incident type to the Health Status of the Community.

» Improve the response and preparedness level of Health services based on efficient planning, integral organization and comprehensive training, using interoperable tools and systems.

» Enhance interoperability within the same, and among different, EMS organizations using a common taxonomy and providing stakeholders in the emergency response domain with a compatible operational framework.

Description of the work

IMPRESS activities began with the definition of health needs in emergency situations, aligned with stakeholders' requirements, and developing the conceptual and organizational framework in which the IMPRESS solution will fit.

Based on that framework, the design and development of the relative system architecture will take place, focusing on real-world cases and user requirements for developing the IMPRESS decision support system (DSS) components and tools.

The development of the IMPRESS DSS components and software tools according to this architecture will take place in an iterative manner and includes the integration of individual components which collectively aim to:

» orchestrate the information flow, strengthen interoperability, and support communication among the components as well as to track the assets of the designated facilities in real time.

» facilitate field data collection and information exchange between medical first responders and emergency management facilities.

The IMPRESS DSS and its components will be tested and validated in a testbed environment and two field trials that will take place in Italy and Bulgaria (the latter in cooperation with Greek partners simulating a cross-border crisis situation).

In addition, the project will develop proper training tools and audio-visual utilities for familiarizing potential stakeholders with public health emergencies and IMPRESS.

Expected results

IMPRESS will improve the coordination of emergency response and shall strengthen the efficiency of decision making in emergency health operations, based on a common taxonomy and conceptual framework. This will have a direct impact on the quality of services provided to European citizens. The DSS of IMPRESS will allow for the use of data from multiple heterogeneous sources, following a consolidated concept of operations, to effectively manage the use of medical resources, and coordinate response activities.

Individual components that introduce medical modelling into emergency management and incident management modules, aimed at improving information sharing and the coordination of public health emergencies, will be validated and delivered.

The IMPRESS solution will provide systems that will facilitate end-to-end communication and information flow between Health Services (including Emergency Responders) at all levels of response. It will assist health services in becoming more proactive, be better prepared and share common information with other emergency response organizations in a standardized way.

PARTNERS	COUNTRY
INTRASOFT International SA (INTRA-BE)	Belgium
Department of Health (PHE)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR)	Italy
ADITESS - Advanced Integrated Technology Solutions and Services Ltd (ADIT)	Cyprus
SATWAYS - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe (STWS)	Greece
Institute of Information and Communication Technologies (IICT-BAS)	Bulgaria
Center for Security Studies (KEMEA)	Greece
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. (IVI)	Germany
ECOMED bvba (ECOMED)	Belgium
European University Cyprus (EUC)	Cyprus
Ministry Of Health (MoH)	Greece
INTRASOFT International SA (INTRA)	Luxembourg

INDIGO / Crisis management solutions

© Galina Pankratova- Fotolia.com

RESEARCH COMPLETED

Information

Grant Agreement N°
242341
Total Cost
€3,835,727
EU Contribution
€2,787,672
Starting date
01/05/2010
End Date
30/04/2013

Coordinator

DIGINEXT SARL
Impasse de la Draille
Parc d'Activités La Duranne
13100 Aix en Provence
France
Contact
Jerome Duchon
Tel: +33 (0)5 61 17 66 66
Fax: +33 (0)5 61 17 65 78
E-mail: Duchon@diginext.no-spam.fr
Website: http://indigo.c-s.fr

Project objectives

The INDIGO project aims to research, develop and validate an innovative system integrating the latest advances in Virtual Reality and Simulation in order to enhance both the effectiveness of operational preparedness and the management of an actual crisis or disaster.

The proposed system will prove an essential and integrated tool for training personnel, planning operations, and facilitating crisis management and co-operation across organisations and nations. It will enable users to:

- display and manipulate an operational visual representation of the situation that is as complete and as easy to understand as possible, for indoor and outdoor situations;
- simulate different evolving scenarios for planning, training, and anticipating future states and impending developments during operations, and analyse events after the crisis;
- involve first responders and emergency field units in simulated exercises;
- enhance the work across organisational boundaries and decision levels.

Description of the work

The INDIGO consortium provides the world-class and complementary competencies required to tackle the following scientific and technological challenges:

- The 3D interactive and realistic visualisation of the complete crisis environment, including data coming from the field, simulation results, and building interiors;
- The intuitive authoring and simulation of different evolving scenarios for planning, training, and anticipating future states and impending developments during operations, and analysing events after the crisis;
- The involvement of multiple participants (field units as well as decision makers and commanders), thanks to its distributed architecture, while offering a unique pictorial way of sharing and communicating complex knowledge across organisation boundaries;
- The preparation of a standard proposition for a European 2D/3D emergency symbology (symbols, indicators, colours) on 2D and 3D maps.

Results

The project developed a system to improve crisis management and crisis training, while improving cooperation across organisations and nations. The system integrates the latest advances in virtual reality and simulation in order to homogenize and enhance both operational preparedness and management of an actual complex crisis.

INDIGO's technology provides for inter-organisation preparation and response to trans-boundary crises and disasters in any environment. It also allows for inter-organisation exercises and information sharing and analysis to improve horizontal and vertical relations. Its features include:

- 3D interactive and realistic visualization of the complete crisis environment, including data coming from the field, simulation results, and building interiors;
- creation and simulation of different evolving scenarios for planning, training, and anticipating future states

and impending developments during operations, and the analysis of events after the crisis;

- simultaneous training of decision makers, crisis managers and first responders influenced by simulated scenario and who would reciprocally influence its evolution;

INDIGO also drew up a European emergency symbology for 2D/3D maps. This will fill an important gap by offering a common visual reference that can be used across Europe for an immediate understanding of a situation, thus improving decision-making across organizational boundaries.

PARTNERS	COUNTRY
Diginext SARL	France
Consiglio Nazionale delle Ricerche	Italy
Centre for Advanced Studies, Research and Development in Sardinia	Italy
Immersion SAS	France
European Committee for Standardization	Belgium
Crisisplan	The Netherlands
Swedish National Defence College	Sweden
Entente pour la forêt méditerranéenne	France

OPSIC / Operationalising Psychosocial Support in Crisis

© Thinkstock

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312783
Total Cost
€4,371,594.28
EU Contribution
€3,333,918
Starting Date
01/02/2013
End Date
31/01/2016

Coordinator

Danish Red Cross (DRC)
IFRC Reference Centre for
Psychosocial Support
Blegdamsvej 27
2100 Copenhagen OE
Denmark
Contact
Martha Margrethe Bird
Tel: +45 3525 9341
Mobile: +45 31 69 65 40
Fax: +45 35 25 92 92
E-mail: mabir@rodekors.dk
Website: www.opsic.eu

Project objectives

Over the past 20 years, psychosocial support (PSS) has played an increasingly important role in responses to crises and a number of high-quality European PSS guidelines and best practice studies have been made. However, none of the existing guidelines are fully comprehensive in terms of psychosocial support for all target groups, in different phases and different types of crisis.

The objective of the project was to design and develop an IT/web-based comprehensive operational guidance system (OGS) based on new research and analysis of existing PSS guidelines and best practices. The OGS operated as a common shared platform and single point of reference for PSS in crisis management, serving multiple target groups with multiple functions.

A static part of the OGS included a comprehensive guideline and a clear overview of existing guidelines, providing crisis managers and other professionals with an IT-based best practice go-to-point for all methods and tools needed to plan, as well as conduct and evaluate PSS interventions throughout all stages and all kinds of crises.

An interactive part of the OGS gave staff, volunteers, victims and affected communities direct access to relevant PSS information and guidance on self-help tools and methods. As PSS crisis managers could access statistical information based on hits and completed questionnaires, this platform could also be used to monitor the resilience and psychosocial well-being of helpers and survivors so that timely support may be provided.

Description of the work

Existing PSS guidelines were identified and analysed in order to assess their practical relevance. Their tools and methods were matched to various target groups, types and phases of crisis (natural or man-made) and gaps were filled-in from literature. Where this was not possible, recommendations for future research were made. Finally, a clear overview of existing guidelines was made.

Focusing on crises which took place in Europe during the past 10-15 years, existing best practice studies were identified and criteria for best practices in PSS assessment, intervention and established, were listed. This resulted in an overview of best practices.

A review of studies on long-term impact of crises was made, including long-term psychological, societal and cultural impact of crises as well as resilience factors at the individual, family, group, community and societal levels in affected populations.

Incorporating all of the above, a comprehensive guideline was made based on recommendations for best practice PSS interventions for all relevant types and phases of crises as well as target groups. Ethical, cultural and gender considerations were taken into account. An IT/web-based operational guidance system (OGS) was designed and developed. It was validated through workshops, demonstrations and simulation tests in three countries with crisis managers, first responders and volunteers. Lessons learned have been incorporated into the comprehensive guidelines as well as the OGS.

Subsequently, the OGS was demonstrated for a governmental end-user and a road map for implementation of the OGS into EU end-users' protocols was prepared.

Throughout the process, the advisory board and the ethical board as well as project partners participated in consultations and give recommendations.

Results

OPSIC successfully developed the Mental Health and Psychosocial Support (MHPSS) Comprehensive Guideline. This quality management instrument points users to relevant guidelines, resources, and tools for planning and implementing MHPSS programmes at all phases of response, in all types of disasters, and with all possible target groups. The guideline contains 51 action sheets, or planning tools, for general crisis managers, psychosocial crisis managers, mental health professionals, and other practitioners. It also contains new academic knowledge on long term consequences of crisis, best practices, and the PSYQUAL assessment tool.

The comprehensive operational guidance system (COMPASS) provides an integrated web-based platform for practical MHPSS guidance in crisis management. Anchored in an advanced IT system, it stores all relevant information, guidelines, and tools in one place. With COMPASS, professionals can share knowledge and ensure a coherent and coordinated approach, and the population can access relevant information and get in touch with MHPSS professionals.

Encouraged by strong, positive, and concrete interest from governmental end-users in several European countries, the consortium has created the COMPASS Foundation to maintain, develop and make COMPASS widely accessible.

PARTNERS	COUNTRY
Danish Red Cross (DRC)	Denmark
University of Innsbruck, Dept. of Psychology (UIBK)	Austria
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)	The Netherlands
IMPACT (IMPACT)	The Netherlands
Academic Medical Centre (AMC)	The Netherlands
University of Zagreb, Faculty of Humanities and Social Sciences (UNIZ)	Croatia
Magen David Adom (MDA)	Israel
General Directorate of Emergency and Civil Protection -Samur (SAMUR)	Spain
Centre for Science, Society and Security (CSSC)	Italy
Crossing Channels (CC)	The Netherlands
The National Centre for Crisis Management Research and Training (CRiSMART)	Sweden

OPTI-ALERT / Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

© S. Hofschlaeger / pixelio.de

Information

Grant Agreement N°
261699
Total Cost
€3,543,462
EU Contribution
€2,531,122
Starting Date
01/01/2011
Duration
36 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Institute for Software and Systems Engineering ISST, Department of Targeted Alerting Systems
Steinplatz 2
10623 Berlin
Germany
Contact
Dr. Michael Klafft
Tel: +49 (0) 30 24306 365
Fax: +49 (0) 30 24306 599
E-mail: Michael.Klafft@isst.fraunhofer.de
Website: www.opti-alert.eu

Project objectives

The Opti-Alert project strives to improve the alerting of the general public in crisis situations through personalized, culturally sensitive multi-channel communication. The objective of this project is to develop an alerting suite that:

- » allows for a rapid simulation of the impact of different alerting strategies (depending on the selected media-mix and current availability of communication media);
- » supports the composition of the optimal mix of communication channels (individualized alerting channels and mass media);
- » improves alert compliance through social and cultural adaptation and personalization of alert messages and communication channels;
- » supports the rapid and automated implementation of a selected alert strategy;
- » can simultaneously address a large variety of communication channels to facilitate efficient high-throughput alerting; and
- » can be integrated with existing tools and legacy systems via well-defined interfaces.

Description of the work

The objectives of the Opti-Alert project are supported by the following key research activities:

- » an in-depth analysis of the impact that social and cultural and regional factors have on risk perception and risk communication;
- » an analysis of the influence which the observed socio-cultural differences have on regional alerting strategies;
- » an analysis of the impact of individualized alerting (via SMS, E-Mail, etc.) and alerting via the mass media;
- » the identification of best-practices in alerting via mass media;
- » a definition of appropriate algorithms for the simulation of alert propagation within the population (in general, but also inside critical infrastructures such as metro stations), depending on the selected mix of communication channels and communication patterns between humans.

One goal of Opti-Alert is to improve the impact of alerts by developing alerting strategies that take socio-cultural characteristics of the message recipients into account. This can refer to both differences in risk perceptions and different usage patterns with respect to media and communication channels. Based upon the situational and socio-cultural context of an alert situation, the authorities will be able to simulate different alerting strategies (in terms of communication channels and media mix). This will allow authorities to re-assess alert procedures and processes and to improve impact and coverage of alerts. Another goal of Opti-Alert is the adaptation of alert content to the socio-cultural milieu of the message recipients. This refers, e.g., to the wording of the messages, or layout and design. The idea is to improve the compliance of alert recipients with the proposed protective actions by creating trust and, if necessary, a sense of urgency (or calm) among those who have been warned.

Expected results

In addition to in-depth and interdisciplinary studies of sociologists and media scientists on the perception of crisis communication, Opti-Alert will develop a demonstrator to test the proposed socio-culturally adaptive alerting tool and the corresponding alert simulation component in practice. Furthermore, an interface definition will be specified so that existing as well as new and emerging communication channels can be connected to the Opti-Alert toolsuite. The goal is to provide an alerting platform that can later be used internationally in order to efficiently address the information needs of the population in times of crisis.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FHSS)	Germany
e*Message Wireless Information Services Deutschland GmbH (EMESS)	Germany
UBIMET GmbH (UBIMET)	Austria
Proteo S. p. A. (PROTEO)	Italy
UNIQA Versicherungen AG (UNI)	Austria
Göteborgs Universitet (UGOT)	Sweden
Süddeutsches Institut für empirische Sozialforschung e.V. (SINE)	Germany
Regione Sicilia (SIC)	Italy
Nederlands Instituut Fysieke Veiligheid (NIFV)	The Netherlands
Università degli Studi di Perugia (UNIPG)	Italy
THALES Services SAS (THALES)	France

POP-ALERT / Population Alerting: Linking Emergencies, Resilience and Training

Information

Grant Agreement N°
608030
Total Cost
€1,134,770.80
EU Contribution
€998,848.38
Starting Date
01/04/2014
Duration
24 months

Coordinator

UNIVERSITY OF GREENWICH
School of Computing and Mathematical Sciences
Old Royal Naval College,
Park Row, Greenwich
SE10 9LS, LONDON,
UNITED KINGDOM
Contact
Elisabeth Bacon
Tel: +44 2083318544
Fax: +44 2083318824
E-mail: e.bacon@gre.ac.uk
Website: www.gre.ac.uk

Project objectives

The main objective of POP-ALERT is to prepare societies and populations for crises and disasters in a rapid, effective and efficient way by blending traditional Crisis Preparedness and First-Reaction strategies with the use of innovative tools. POPALERT's conceptual approach focuses on how best to alert and support action by citizens under crisis conditions, in familiar and unfamiliar surroundings using mechanisms that will follow intuitive human behaviour.

POP-ALERT's objectives recognise that in most circumstances the number of personal response options are limited and the correct responses may have to be initiated without any prior knowledge of the surroundings or threats.

The project will aim to achieve the following:

» Gain insight into society's understanding of large scale disaster events, their willingness to accept risk probabilities and engage in preparedness, and their behavioural responses to diverse situations by measuring expectations in both domestic and foreign situations;

» Identify success stories within existing and past community preparedness programmes – both at the local and EU level – and compile a portfolio of case studies on social networking and community initiatives which could potentially be replicated in crisis;

» Undertake evidence-based research on the most effective existing delivery routes for informing European citizens in a situation of crisis and to assess the overarching authority strategies of local and national administrations to contribute to the preparedness of citizens;

» Study the best ways to blend contemporary tools with the existing practices in order to create flexible and easily deployable toolkits for preparing and alarming the European population in case of a crisis, taking into account social and cultural differences;

» Propose a pilot project by designing criteria for selection of the area and population to be involved in the pilot, developing scenarios and objectives;

» Provide a generic methodology to assess the effectiveness in raising an improved level of preparedness of the community.

Description of the work

POP-ALERT proposes to undertake thorough behavioural research and Crisis Management research in order to create a framework to facilitate the assessment of the population's capacity to make use of different Crisis Management strategies and technologies developed at the EU level.

The project will seek to study the best ways to blend contemporary tools with the existing practices identified in order to create flexible and easily deployable toolkits for preparing and alarming the European population in case of a crisis. The approach this project proposes for improving the current practices revolves around the use of messaging and cultural sharing technologies to create awareness.

POP-ALERT will propose a pilot project in order to test the generic methodologies and to assess their effectiveness in raising an improved level of preparedness of the community.

Expected results

1. A classification of the drivers, constrains and complexities of population preparedness in domestic and foreign situations and the creation of a framework for assessing and understanding community preparedness at the EU level.

2. A model for presenting, blending and disseminating community preparedness practices in order to promote transfer of knowledge and replicability to a larger scale.

3. A collection of sample training curriculums and tools to be used by authorities, organisations and first responders for preparing the community to cope with large scale crisis situations.

4. A set of methodologies for effectively communicating with populations using contemporary messaging and social networking tools to notify modern societies of risks and strategies related to large scale crisis situations.

5. A toolkit for preparing and alerting populations, including the best forms of accessibility to different communities, reaching through to citizens, strategies for achieving acceptance and indicators for evaluating the success of the strategies proposed.

6. A project demonstrating the efficiency and effectiveness of the tools developed, including an evaluation and recommendations for future actions to ensure these practices reach the market.

PARTNERS	COUNTRY
University of Greenwich	United Kingdom
European Organisation For Security SCRL (EOS)	Belgium
Association Comité National Français du Comité Technique International de Prévention et d’Extinction du Feu (CTIF)	France
Altran BV (ALTRAN)	The Netherlands
Camara Municipal de Lisboa (CML)	Portugal
Training 4 Resilience (T4R)	United Kingdom
Siemens Schweiz AG (SIEMENS)	Switzerland
Empresa de Servicos e Desenvolvimento de Software SA (EDISOFT)	Portugal
Center for Security Studies (KEMEA)	Greece
University of Chester	United Kingdom
Service Départemental d’Incendie et de Secours de la Haute-Corse (SDIS 2B)	France

PREDICT / Preparing for the Domino Effect in Crisis Situations

Information

Grant Agreement N°
607697
Total Cost
€4,635,020.99
EU Contribution
€3,460,192.99
Starting Date
01/04/2014
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)
CEA Centre Gramat
46 500 Gramat - FRANCE
Contact
Dominique Sérafin
Tel: +33 (0) 5 65 10 54 46
Mobile:
+33 (0) 6 76 73 54 22
E-mail:
Dominique.serafin@cea.fr
Website:
www.predict-project.eu

Project objectives

The general goal of the PREDICT project is to deliver a comprehensive solution for dealing with cascading effects in multi-sector crisis situations. Its objectives are:

» gather and analyse available domain knowledge;

» develop a common framework;

» create conceptual and executable models of cascading effects and interdependencies;

» develop a suite of software tools;

» validate the solution through running simulations;

» disseminate project results and build appropriate liaisons among stakeholders.

Description of the work

The PREDICT solution comprises three pillars: methodologies to consider cascading effects, creation of models and, finally, development of tools.

PREDICT's work consists of:

» WP1 provides organisational basis and on-going overall management for all project activities;

» WP2 delivers basis for modelling in a form of taxonomy and scenario and inputs for system design as a technical specification;

» WP3 uses the basis from WP2 in order to provide understanding of cascading effects by defining models and methodologies;

» WP4 delivers overall system design (system architecture) and manages iterative system realisation and integration;

» WP5 and WP6 develop together crucial elements of the PREDICT Incident Evolution Tool i.e. Foresight and Prediction Tool (WP5), Decision Support Tool (WP6) and Expert Integration Network Module (WP6);

» WP7 provides the Training Module for Incident Evolution Tool and manages end-users involvement in a form of continuous evaluation;

» WP8 End-user network will organise a series of 5 workshops throughout the project, involving external end-users;

» WP9 Dissemination & Exploitation provides the necessary website and workshop to liaise with other projects and organise the final conference. It will also look at ways to exploit the results of the project after it ends.

Expected results

The PREDICT solution is:

- expected to increase the awareness and understanding of cascading effects in crisis situations;
- expected to enhance the preparedness for cascading effects;
- expected to improve the capability to respond of various levels decision makers (local, regional, national or international).

PARTNERS	COUNTRY
Commissariat à l'Energie Atomique (CEA)	France
ITTI Sp. Zo.o. (ITTI)	Poland
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V. (Fraunhofer)	Germany
THALES SA (Thales)	France
Compagnie Européenne d'Intelligence Stratégique (CEIS)	Belgium
Netherlands Organisation for Applied Scientific Research (TNO)	The Netherlands
Technical Research Centre of Finland (VTT)	Finland
Veiligheids regio Zuid-Holland Zuid (Safety region South-Holland South) (VRZHZ)	The Netherlands
Suomenympäristökeskus (Finnish Environment Institute) (SYKE)	Finland
Union Internationale des Chemins de Fers (UIC)	France
Thales Netherlands (TRT-NL)	The Netherlands

PSYCRIS / PSYcho-Social Support in CRISis Management

© Shutterstock

Information

Grant Agreement N°
312395
Total Cost
€4,774,842.99
EU Contribution
€3,827,525.79
Starting Date
01/07/2013
Duration
36 months

Coordinator

Ludwig-Maximilians-Universitaet Muenchen – (LMU)
Department Psychologie
Geschwister-Scholl-Platz 1
80539 – MÜNCHEN
GERMANY
Contact
Dr. Christine Adler
Tel: +49 89 2180 5175
Fax: +49 89 2180 5224
E-mail:
Christine.adler@psy.lmu.de
Website:
www.uni-muenchen.de

Project objectives

The aim of PsyCris is to develop and provide a roadmap as a bottom-up strategy to improve the psycho-social support infrastructure and the transnational cooperation of psycho-social emergency response services after a major incident in Europe. Within this overall objective, the proposed project PsyCris (36-months) has the following goals: (1) status quo analysis of psychological and medical support in crises in European countries, (2) improvement of support strategies for victims and crisis managers, (3) enhancement of psycho-medical preparedness for major incidents (contingency planning), (4) development of interventions to deal with stress and reduce stress related disorders of crisis management personnel and authorities, (4) providing efficient self-help strategies to communities affected by crises and (5) investigation of long-term psychosocial, societal and cultural impact of crises.

Description of the work

The PsyCris project will be executed over a 36-month period in three stages. The first stage is characterised by the concept development of three reference disaster scenarios. The opinion and comments of end-users will be included in this process. The actual needs of end-users will be carefully identified. This will ensure high quality user requirements specification and a realistic operational concept accepted by the end-users. An evaluation of effective psycho-medical interventions and of longer term societal, psychological and cultural impact of a crisis will be carried out. In the second stage, the development and design of the components of the PsyCris tool kits will take place. In the third stage, the various components (e.g. stress assessment, stress management, contingency planning, help the people help themselves) will be integrated in an overall PsyCris tool kit demonstrator, which will be based on a comprehensive knowledge system (PsyCris Preparedness-Planning-Prevention (PPP) Platform).

The PsyCris PPP Platform will be developed on the grounds of our understanding of prevention, which is based on three stages: primary, secondary and tertiary prevention. Finally, the effectiveness of PsyCris PPP Platform will be evaluated, once again involving end-users in this process.

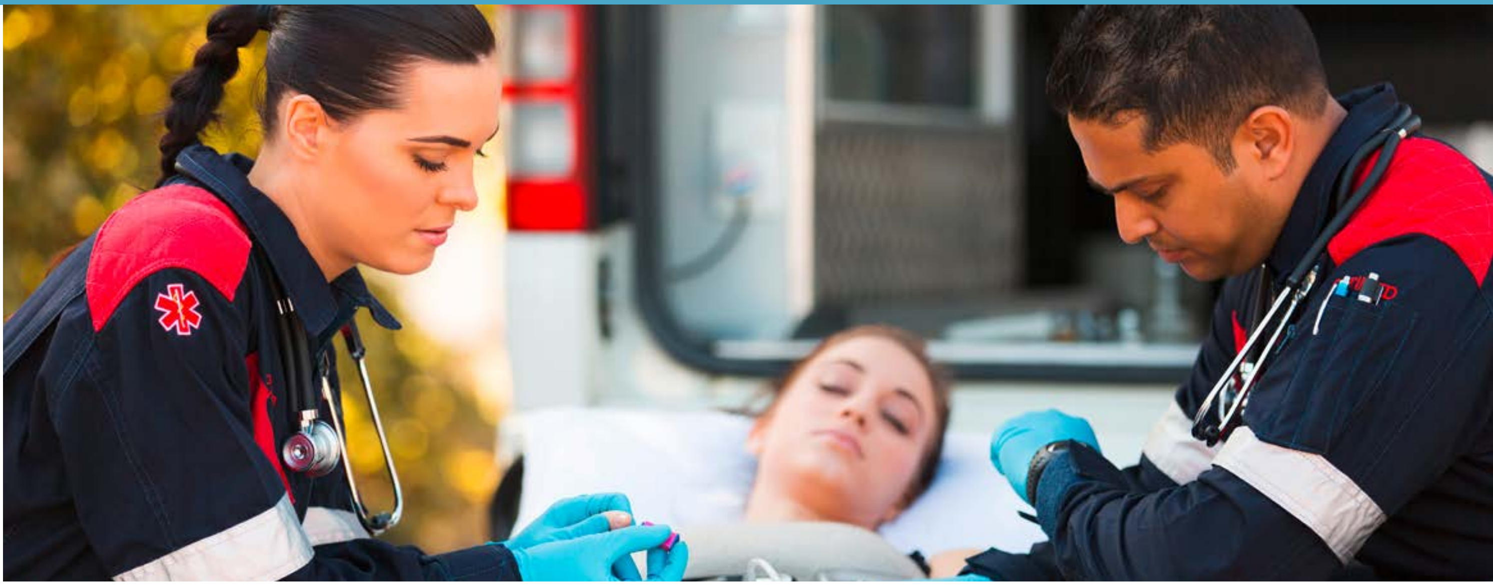
Research and development are based on a multi-disciplinary approach including methods from psychology (e.g. stress management, human resources management, psycho-trauma intervention), education sciences (e.g. knowledge management), informatics (e.g. decision making heuristics), engineering, sociology and health sciences. Current and possible changes in society, health systems and climate as well as cross-cultural and gender aspects are carefully considered. The 11 partners of the consortium comprise research centres, public bodies, small / medium enterprises and stakeholder / end-user organisations from Germany, Spain, Israel, Lithuania, Luxembourg and Austria.

Expected results

As its main product, the project will provide a set of tool kits enabling (1) efficient handling of relevant data, (2) transfer of knowledge and practical competences relevant for crisis management, stress control and social support and (3) rapid decision-making in crises. The tool kits are integrated within a computerised knowledge system combining e-learning and face-to-face teaching. PsyCris will propose guidelines for preparedness, prevention and intervention for crises: it is expected that the results will have a significant impact on public health, community resilience, international cooperation and cost containment.

PARTNERS	COUNTRY
Ludwig-Maximilians-Universitaet Muenchen (LMU)	Germany
Universidad de Granada (UGR)	Spain
UMIT-Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT)	Austria
Viesoji Istaiga Kitokie projektai (KKP)	Lithuania
Blended Solutions GmbH (BSO)	Germany
Bayerische Forschungsallianz (Bavarian Research Alliance) GmbH (BayFOR)	Germany
Amuta LeYeladim beSikun - Cohen-Harris Resilience Center for Trauma and Disaster Intervention (CHC)	Israel
Unfallkasse Thüringen (UKT)	Germany
Insight Instruments (ISI)	Austria
Protection Civile Luxembourg Groupe de Support Psychologique ASBL (GSP)	Luxembourg
Colegio Oficial de Psicólogos de Andalucía Oriental (COPAO)	Spain

PULSE / Platform for European Medical Support during major Emergencies



Information

Grant Agreement N°
607799
Total Cost
€3,921,640.00
EU Contribution
€2,789,940.00
Starting Date
01/05/2014
Duration
30 months

Coordinator

SKYTEK + (SKYTEK)
Research and Development
51 Fitzwilliam Square
D2 – Dublin - Ireland
Contact
Sarah Bourke
Tel: +353 - 16787660
Fax: +353-1-6787636
E-mail:
Sarah.bourke@skytek.com
Website: www.skytek.com

Project objectives

In Europe, one of the core emergency response services to deadly threats such as pandemic disease and major terrorism attacks is the European Health Services (EHS). The EHS comprises key stakeholders that include hospitals, community health services, pre-hospital emergency care services, medical suppliers, rescue services, health related voluntary services and others. It is crucial to the EHS that it remains in an excellent state of preparedness supported by first-class planning and decision support tools. Moreover, in the response phase, EHS need consistent, coordinated and standardised advanced support methods and tools providing support in critical tasks such as early threat detection, common operational picture, creation of surge capacity etc. Finally, at a pan-European level, EHS need an interoperable framework with the ability to provide a coordinated European response to any major medical incident.

PULSE aims to meet these challenges.

Description of the work

The project will begin by comprehensively studying the procedures, processes and training requirements in current operation at the EHS, using the support of end users available to the project. It will then:

» Develop standard and consistent response procedures and processes;

» Provide tools to support decision making in both preparedness and response phases;

» Provide a framework to ensure decision makers have access to timely key data, planning and decision support tools and international best practice and policies;

» Present innovative training techniques to improve personnel response training;

» Develop an ‘emergency app’ for smart phones to allow users fast and flexible access to emergency resource availability information;

The PULSE framework solution will be validated by two pilot scenarios based on multiple exercises and demonstrations: a) a biological attack in Italy and b) a major stadium ‘crush’ at a Dublin concert. Both will involve cross border support from neighbouring countries

Expected results

The primary benefit will be to:

- Reduce administration, bureaucracy and ensure better use of resources;

- The project will also build on research results from previous EU projects which have developed usable analysis of societal and political criteria and their relevance to security measures

- Record and assess previous policies

PARTNERS	COUNTRY
Skytek Ltd (SKYTEK)	Ireland
Centre for European Security Strategies (CESS)	Germany
Onest Solutions Srl (ONEST)	Romania
Trilateral Research & Consulting LLP (TRILATERAL)	United Kingdom
Universita Cattolica Del Sacro Cuore (UCSC)	Italy
Selex ES SPA (SES)	Italy

SECURENV / Assessment of environmental accidents from a security perspective

© SECURENV

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218152
Total Cost
€1,205,870
EU Contribution
€850,596.50
Starting Date
01/05/2009
End Date
30/04/2011

Coordinator

Geonardo Environmental Technologies Ltd.
Záhony utca, 7
1031 - Budapest
Hungary
Contact
Balazs Bodo
Tel: +36 1250 6703
Mobile: +36 20 317 2087
Fax: +36 1 436 9038
E-mail: coordinator@securenv.eu
Website: www.securenv.eu

Project objectives

SECURENV aimed to develop a knowledge base and research agenda for future threats associated with possible deliberate attacks on the environment – including 'environmental terrorism' or attempts to amplify the damage inflicted on environmental elements by conventional security incidents.

The ultimate goal of the project was to catalogue and prioritise potential threats in this area, support the development of appropriate policy counter measures and mitigation strategies.

Results

The initial project output was a review and assessment of past environmental accidents, catastrophes and examples of deliberate attacks on the environment. This created a database of 330 entries. Though this database catalogued substantial anecdotal evidence of deliberate environmental destruction throughout history, the actual number of incidents described as direct 'environmental terrorism' is limited.

However, environmental damage as the result of organised crime appears to be an emerging phenomenon, whilst increasingly strict environmental regulations are generating larger numbers of notable incidents: ie., the threshold of tolerance for incidents has been lowered, with a corresponding decrease in investment for causing such an incident.

Several examples of environmental warfare were also identified, with special attention being given to incidents such as the potential release of invasive species by a would-be attacker. These findings have been integrated to a 'foresight model', through which the inherent risk and likelihood of an incident manifesting can be calculated.

These models were used to develop a systematic security foresight approach. The resulting methodology is a combination of assessment methods including input and expertise from a survey addressing more than 600 experts in Europe and beyond, as well as scenario-building workshops involving 15-20 consortia experts.

The policy recommendations and mitigations strategies related to these findings, due to the sensitive nature of this topic area, are largely classified.

© SECURENV

PARTNERS	COUNTRY
Geonardo Environmental Technologies Ltd.	Hungary
Adelphi Research	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden

S-HELP / Securing Health.Education.Learning.Planning

Information

Grant Agreement N°
607865
Total Cost
€4,436,136.72
EU Contribution
€3,496,836.15
Starting Date
01/02/2014
Duration
36 months

Coordinator

UNIVERSITY COLLEGE CORK + (UCC)
Business Information Systems
O'Rahilly Building
Cork – Ireland
Contact
Karen Neville
Tel: 353 + 21 + 4903668
Mobile: 353 + 863952582
Fax: 353 + 21 4271566
E-mail: KarenNeville@UCC.ie
Website:
http://www.fp7-shelp.eu/

Project objectives

S-HELP aims to develop and deliver a holistic approach to healthcare preparedness, response, and recovery by:

» Defining an interoperability standard to enable communication and coordination across different geographical areas and cultural settings

» Facilitating a collaborative end user and supporting partner driven solution to meet the needs of different users from four countries in Europe and beyond.

» Defining and applying an interoperability standard for multiple agencies jointly responding to a disaster.

» Advancing the design and application of current available solutions to improve preparedness, response, and recovery in emergency situations.

» Delivering decision supporting tools for emergency preparedness, response, and recovery, tested, evaluated, and enhanced through quality, end user designed emergency scenarios.

Description of the work

By leveraging decision support (DS) the project's solution will advance the knowledge base required for the development of a range of DS tools and a Decision Support System (DSS) for the management for all of emergency medicine activities.

S-HELP DSS will use a seven-stage methodological framework consisting of one coordination and project management work package and six targeted work packages.

Expected results

The S-HELP Decision Support System (DSS) will bring significant benefits to the management of emergencies, from learning and preparing for emergency incidents and analyzing threats, to post evaluation, reporting and logistics management.

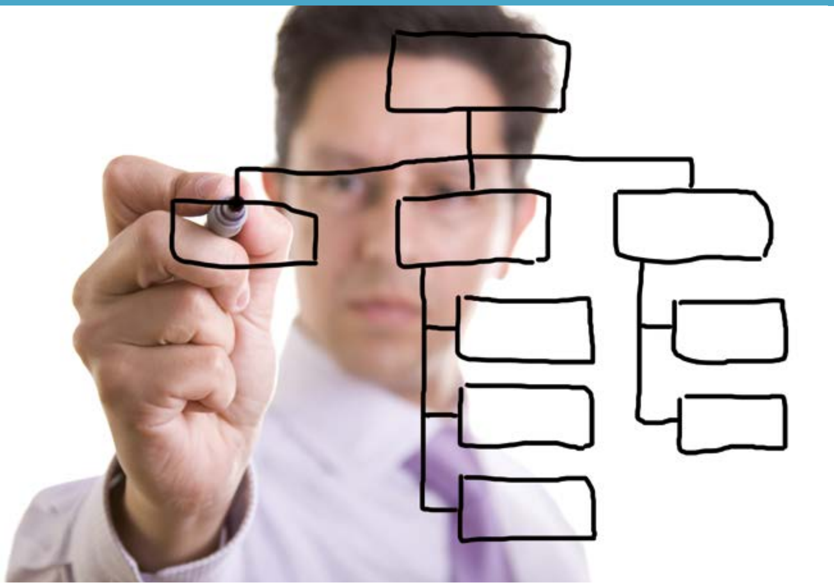
S-HELP will provide a unique mechanism to assist stakeholders and end users to work together for co-ordinated, effective, evidence based decisions at all stages of emergency management (EM). It therefore plays an essential role in the response to emergency situations that in many cases have negative impacts on human‘s health.

The tools delivered (which will be validated in three key scenarios) through S-HELP will result in improved preparedness and response of health services involved in large scale and/or cross border emergency situations.

An interoperable knowledge base for responder and decision-makers will be developed, thereby supporting the EU regulation CEN BT/WG 161, Protection and Security of the Citizen‘.

PARTNERS	COUNTRY
Application of Science to Simulation, Education and Research on Training for Health Professionals + (ASSERT)	Ireland
Future Analytics Consulting Limited (FAC)	Ireland
accelopment AG(ACCEL)	Switzerland
Magen David Adom in Israel (MDA)	Israel
Health Service Executive (HSE)	Ireland
Public Health Agency (PHA)	United Kingdom
Lunds Universitet (LU)	Sweden
Technische Universität Graz (TUGraz)	Austria
Vectorcommand LTD.(VCL)	United Kingdom
Universität Wien (UVIE)	Austria

SICMA / Simulation of crisis management activities



© Helder Almeida - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217855
Total Cost
€3,902,633.33
EU Contribution
€2,566,330
Starting Date
01/03/2008
End Date
31/08/2010

Coordinator

ELSAG DATAMAT SPA
2 Via G. Puccini
IT-16154 Genova
Italy
Contact
Giuseppe La Posta
Tel: +39 06 5027 2612
Fax: +39 06 5027 2250
E-mail: giuseppe.laposta@elsagdatamat.com
Website: http://www.sicma-project.eu/SicmaProject-Site2008/index.html

Project objectives

The SICMA project was a 30 months capability project focused on computer assisted decision making for Health Service crisis managers. It aimed at improving decision-making capabilities through an integrated suite of modelling and analysis tools providing insights into the collective behaviour of the whole organisation in response to crisis scenarios.

Description of the work

The response to the crisis is the result of the activities of:

» Different services (e.g. police, medical care, rescue forces, fire fighting, etc);

» interacting vertically (i.e. with components of the same organization) and horizontally (i.e. with components of other organizations);

» in a complex environment characterized by both “predictable” factors (e.g. the crisis responders’ behaviour according to procedures) and “unpredictable” ones (e.g. human/crowd behaviour).

© Sicma

As a consequence, the decision making process both in the preparedness and in the response phase is hard and complex due to the impossibility to estimate the effects of alternative decisions. Within this context, decision making support was provided addressing the following key aspects:

» “bottom-up” modelling approach building independent model components and then combining them,

» unpredictable factors modelling (e.g. human/ crowd behaviour),

» procedure support to provide the user with the correct procedures to solve the problem, and

» computation of the “distribution” of the effectiveness of a certain “decision” rather than the effectiveness of that solution deterministically dependant on the preconceived scenario.

The combined effects of the above points allowed a documentation of both the unexpected bad and good things in the organization(s) thus leading to better responses, fewer unintended consequences and greater consensus on important decisions.

Application scenarios

The following scenarios were selected:

Conventional weapons terrorist attack: being the most common and hence the most likely threat in the future. This scenario was used to evaluate the decision support achievable with the SICMA prototype in the management of casualties. The focus was on the management of the most likely category of casualties that can be generated by a large number of different types of disasters that is: trauma casualties.

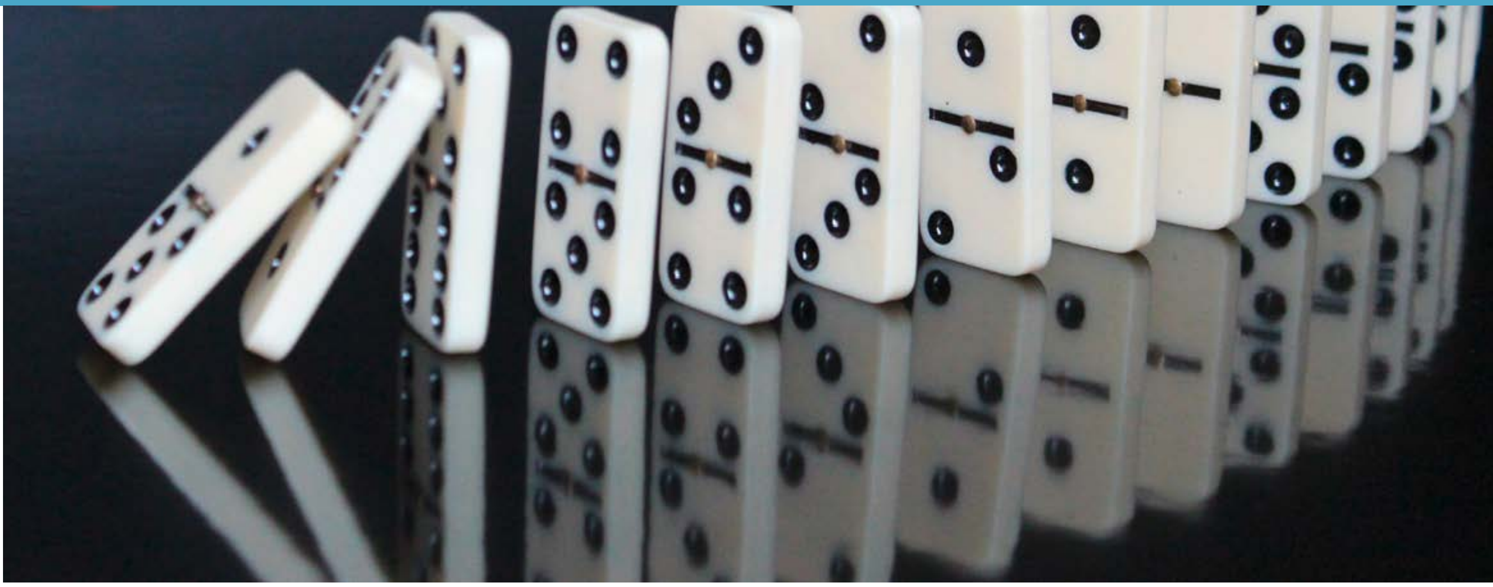
Chemical weapons terrorist attack: specific types of disasters may result in additional decision making activities to be carried out by the crisis manager. This scenario was used to highlight the additional support that can be provided to decision making activities specifically related to the kind of accident. The decontamination-station deployment and hazard estimate/update was used as case study in the chemical attack Scenario.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
ELSAG DATAMAT S.P.A. (ED)	Italy
SKYTEK LTD (SKYTEK Ltd)	Ireland
Centre for European Security Strategies GMBH (CESS)	Germany
IFAD TS A/S (IFAD)	Denmark
ELBIT SYSTEMS LTD (ESL)	Israel
ITTI Ltd (ITTI)	Poland
INDUSTRIEANLAGEN BETRIEBSGESELLSCHAFT MBH (IABG)	Germany
UNIVERSITA CATTOLICA DEL SACRO CUORE (UCSC)	Italy
CONSIGLIO NAZIONALE DELLE RICERCHE (CNR-IASI)	Italy
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy

SNOWBALL / Lower the impact of aggravating factors in crisis situations thanks to adaptative foresight and decision-support tools



Information

Grant Agreement N°
606742
Total Cost
€5,205,926.70
EU Contribution
€3,882,462.70
Starting Date
01/03/2014
Duration
36 months

Coordinator

STE GENERALE DE DISTRIBUTION ET DE COMMUNICATION - GE DI COM (GEDICOM)
Avenue Maurice Bertaux 91
94420 - Le Plessis Trevise
France
Contact
Jean Bruma
Tel: +33 (0)1 45 93 23 28
Mobile:
+33 (0)6 70 61 05 40
Fax: +33 (0)1 45 76 01 07
E-mail: jbruma@gedicom.fr
Website: www.gedicom.fr

Project objectives

The project's first objective is to help decision-making bodies make the most efficient decisions in times of crisis to minimize the effects of a crisis and its casualties. Snowball's main innovation is to integrate the cascading effects of a crisis in simulations, including post-communication to the public, therefore providing more accurate simulations and decision support.

To better predict cascading effects, the project will focus on three areas: the study and deeper understanding of cascading effects; the collection and storage of data and its availability; and the simulation of probable events occurring in the cascading chain.

Predicting cascading effects implies a better understanding of previous large-scale crisis and how these effects occurred. The project will study a wide history of crises to gain this understanding. One objective will be to study how population behaviour may become a cascading effect and an aggravating factor within a crisis.

Data availability is also crucial to the project. This is a real problem for crisis analyzing tools because data for studying a crisis, whether public or private, is not always reliable or consistent. Since cascading effects involve a variety of events across various fields (climate, networks, and human), this problem of data availability will be central to Snowball's work.

Thus, a key objective will be to provide access to all the data needed by the consortium. This will imply checking the reliability of data and unifying data formats so that all be integrated in the same tool.

The project will not only gather information while analyzing the mechanisms of cascading effects, it will also forecast via simulation the evolution of a crisis and its cascading effects. To do this, a methodology to integrate cascading effects will be developed by the project partners.

This methodology will break down the crisis into elementary "bricks". This approach relies on the fact that, whatever the crisis - earthquake, volcanoe, storm, etc.- the resulting sequence of events is often similar (damages to networks, changes in population behaviour, etc.). In other words, a large portion of events from each type of crisis is the same. Thus globally, from one crisis to another, the originators may be different, but the events cascading from it are more or less similar.

One of the project's central ideas is to insert into one structural database all the possible events, broken down into their elementary bricks, and to make it possible for any crisis to be modelled in the database.

The advantage of such approach is that two different crisis can be modelled at the same time, with their consequences gathered into one. More importantly, the tool will be generic to allow monitoring of all types of crisis. Another advantage is that the tool could subsequently be extended to integrate more and more crisis events/bricks, thus refining the accuracy of its simulations.

The project's global solution will be tested via a demonstration that will serve two goals. First, the project will validate the functioning of the solution. Second, the partners will use the solution in different case scenarios to assess the preparedness of public bodies and first responders to manage and contain a crisis, including its cascading effects.

Description of the work

To develop a platform dedicated to monitoring a crisis and predicting its cascading effects, Snowball will analyse the needs and practices of potential end-users (decision makers, governments). An extensive study of previous crises and events whose effects and thus impact were amplified will be conducted to define a road map for forecasting cascading effects.

On the basis of these two studies, Snowball will determine the necessary data to be fed into the tool to establish the links between crises and how they can be predicted.

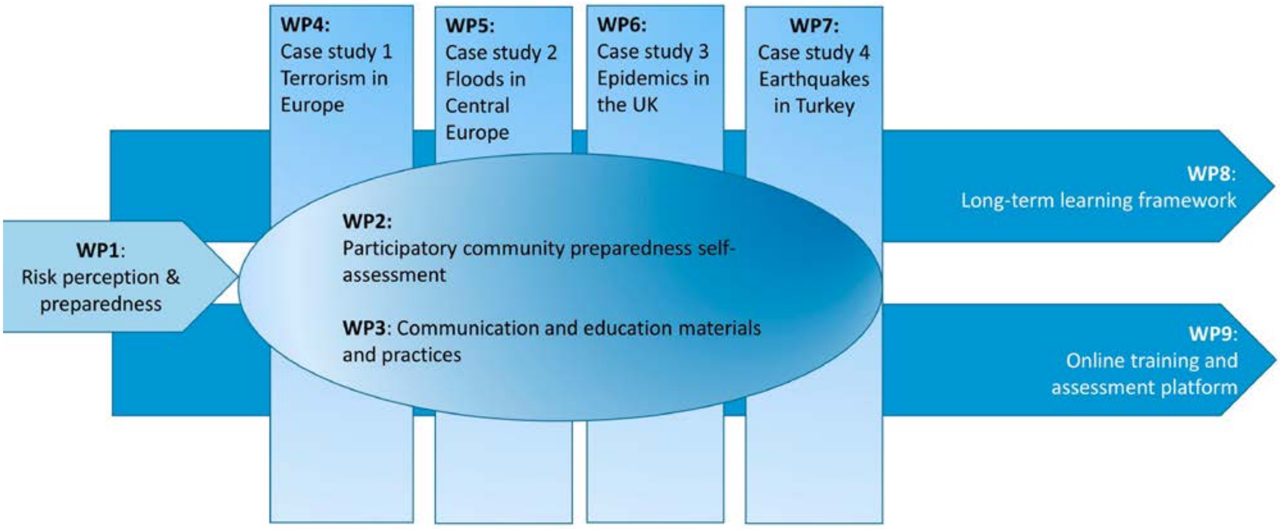
Expected results

A methodology for containing cascading effects which is adaptable to different levels of data availability.

A platform for assessing a crisis, predicting cascading effects, simulating its evolution, displaying the events and providing support to decision-makers.

PARTNERS	COUNTRY
Ste Générale de Distribution et de Communication (GEDICOM)	France
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (Fraunhofer)	Germany
Istituto Superiore Mario Boella sulle Tecnologie dell'Informazione e delle Telecomunicazioni (ISMB)	Italy
Universita degli Studi di Napoli Federico II (LUPT-PLIVINS)	Italy
Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)	Germany
Université Catholique de Louvain (UCL)	Belgium
Inéo Engineering & Systems SNC (INEO)	France
Szkola Glowna Sluzby Pozarniczej (SGSP)	Poland
Pelastusopisto, Emergency Services College (ESC)	Finland
Evroproject ood (EP)	Bulgaria
Magyar Voroskereszt Tarsadalmi Szerverzet (HRC)	Hungary

TACTIC / Tools, methods And training for CommuniTIes and society to better prepare for a Crisis


WP4: Case study 1 Terrorism in Europe
WP5: Case study 2 Floods in Central Europe
WP6: Case study 3 Epidemics in the UK
WP7: Case study 4 Earthquakes in Turkey
WP1: Risk perception & preparedness
WP2: Participatory community preparedness self-assessment
WP3: Communication and education materials and practices
WP8: Long-term learning framework
WP9: Online training and assessment platform

Information

Grant Agreement N°
608058
Total Cost
€1,321,427.10
EU Contribution
€999,083.52
Starting Date
01/05/2014
Duration
24 months

Coordinator

Helmholtz Centre for Environmental Research (UFZ)
Department of Urban and Environmental Sociology
Permoserstrasse 15
04318 - Leipzig – Germany
Contact
Christian Kuhlicke
Tel: +49 341 235 1751
Fax: +49 341 235 2825
E-mail:
christian.kuhlicke@ufz.de
Website: www.ufz.de

Project objectives

TACTIC's aim is to increase preparedness for large-scale and cross-border disasters amongst communities and societies in Europe. This will be achieved by drawing on state-of-the-art literature related to risk perception and preparedness, and by creating a catalogue of good practices in education and communication. This information will draw on community preparedness self-assessment.

Rather than taking a top-down approach to preparedness, TACTIC pursues a collaborative project strategy by including different stakeholder groups in the development, testing and validation of self-assessment and materials throughout the project. It will do this by conducting four case studies focusing on terrorism, floods, pandemics and earthquakes.

Description of the work

TACTIC's workflow is divided into three parts:

Phase 1: state-of-the-art research on risk perception and community preparedness

» Literature reviews and building stakeholder networks (WP1).

Phase 2: interaction

» Development and validation of preparedness self-assessment and good practices, together with stakeholders in the four case studies (WP4-7).

Phase 3: finalizing main outputs

» Fusing the theoretical and practical findings to develop a long-term learning framework for preparedness within a multi-hazard context via an online-learning platform (WP 8-9).

Expected results

Many organizations have a range of risk communication tools and methods that they use before, during and after disastrous events. Only a few, however, select their practices based on an analysis of their communication aims, the message they would like to present and the needs and capabilities of their user groups.

TACTIC will provide a strategic framework for those working in disaster risk management and for populations potentially affected by disasters. This will help: a) revise existing communication strategies and b) exchange needs and expectations regarding communication between disaster risk managers and the general public and c) learn about specific methods in risk communication ("good" practices). This aims to improve preparedness through communication with the general public about the risk(s) it faces and about actions and methods whereby all can improve disaster preparedness.

TACTIC is developing a self-assessment and learning tool for risk preparedness to allow organisations to evaluate the strengths and weaknesses of their own risk communication practices. It will suggest "best fit" solutions to improve risk communication. For the general public, the platform will offer opportunities to learn about risks and how to prepare, respond and recover from disastrous events. The platform also allows the general public to formulate their risk communication requirements regarding desired communication channels and content of information, while enbabling organizations to use this feedback to actively improve the existing communication strategy.

PARTNERS	COUNTRY
Helmholtz Centre for Environmental Research GmbH (UFZ)	Germany
Trilateral Research and Consulting LLP (TRI)	United Kingdom
Northumbria University (UoN)	United Kingdom
European Dynamics (ED)	Greece
Institute of Meteorology and Water Management (IMGW-PIB)	Poland
Middle East Technical University (METU)	Turkey
Saxon State Office for the Environment, Agriculture and Geology (LfULG)	Germany

ACRIMAS / Aftermath Crisis Management System-of-systems Demonstration - Phase I

© Federal Office of Civil Protection and Disaster Assistance (BBK), Germany

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261669
Total Cost
€1,666,022
EU Contribution
€1,109,381
Starting Date
01/02/2011
End Date
31/05/2012

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Technological Trend Analysis (INT), Department for Meta-Analyses and Planning Support
Appelsgarten 2
PO Box 14 91,
53879 Euskirchen
Germany
Contact
Hans-Martin Pastuszka
Tel: +49 (0)2251 18 298
Fax:
+49 (0)2251 18 38 298
E-mail: hans-martin.pastuszka@int.fraunhofer.de
Website: www.acrimas.eu

Project objectives

The Phase I project ACRIMAS, a 15-month Support Action with 15 partners from 10 European countries, elaborates a systematic integration process for crisis management (CM) systems, procedures and technologies in Europe, to be implemented within a Phase II demonstration programme. The process will allow for gradual evolvement of CM capabilities through demonstration and experimentation (DE) activities, facilitating Europe wide collaboration, cooperation and communication in CM at different levels of decision making, and respecting the different CM approaches and ambitions of the EU Member States. This process will improve the transfer of related knowledge between stakeholders and promoting an environment for co-development of CM technology and methodology in R&D where users and providers work together.

ACRIMAS further emphasises community-building which will be considerably supported by the execution of the subsequent Phase II, bringing together the various key stakeholders and the available DE infrastructures in a case-by-case demonstration or experimentation activity.

Description of the work

Large-scale incidents (man made and natural) inside and outside the EU require a coordinated response from crisis managers and first responders across Europe and with resources from all levels of government. Among others, a common operational picture, well trained and equipped teams, secure communications, and mission flexibility are core assets for successful CM.

Currently, CM in the EU can be regarded as a highly diversified ‘system-of-systems’ integrating organisations and components with different cultures, policies and assets, and various stakeholders and procurement schemes. This ‘system-of-systems’ incorporates technology, procedures, organisational concepts, and human factors. To identify the relevant/critical/ urgent areas and topics within this current CM ‘system-of-systems’ which need to be addressed by the demonstration programme in Phase II, ACRIMAS follows a scenario-based and user-centric work approach.

ACRIMAS is scenario-based in the sense that characteristic CM scenarios will be identified, selected and developed to constitute a sound basis for ensuring the work of posing user needs and requirements, identifying current weaknesses and gaps in CM in Europe, looking at potential solutions and documenting corresponding demonstration topics and R&D needs to be integrated in a roadmap for Phase II. The scenario approach embraces an all-hazard view, including the EU external dimension.

ACRIMAS is user-driven in the sense that users and other stakeholders in terms of first responders, authorities and governmental bodies as well as the supply side are actively involved throughout the project process, some of them as full partners, most of them linked to the project through a supporting Expert Group and dedicated project workshops. They play a central part in complementing and validating the scenario analysis by expressing their needs and requirements regarding the identification of relevant CM topics, which should be addressed by DE activities in Phase II, and the demonstration concept to be elaborated.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-INT)	Germany
CRISIS MANAGEMENT INITIATIVE (CMI)	Finland
NATIONAL CENTER FOR SCIENTIFIC RESEARCH “DEMOKRITOS” (NCSRD)	Greece
NEDERLANDS INSTITUUT FYSIEKE VEILIGHEID (NIFV)	The Netherlands
T-SOFT AS (TSOFT)	Czech Republic
TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)	Sweden
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO)	The Netherlands
TURKIYE KIZILAY DERNEGI (TRCS)	Turkey
TECHNOLOGIES SANS FRONTIERES ASBL (TSF)	Belgium
UNITED NATIONS UNIVERSITY (UNU-EHS)	Germany
Cassidian S.A.S. (EADS)	France
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
PUBLIC SAFETY COMMUNICATION EUROPE FORUM AISBL (PSCE)	Belgium

CAERUS / Evidence based policy for post-crisis stability: bridging the gap

Information

Grant Agreement N°
607960
Total Cost
€4,080,027
EU Contribution
€3,249,999
Starting Date
01/03/2014
Duration
36 months

Coordinator

UNIVERSITÉ CATHOLIQUE DE LOUVAIN (UCL)
Centre for Research on the Epidemiology of Disasters, Institute of Health and Society
Clos-Chapelle-aux-Champs, 30
B1.30.15
1200 Woluwe Saint Lambert, Brussels, Belgium
Contact
Debarati Guha Sapir
Tel: +32 2764 3327
Mobile: +32 475 617 019
Fax: +32 2 764 3441
E-mail: debarati.guha@uclouvain.be
Website: www.uclouvain.be
www.cred.be
http://caerus-info.net

Project objectives

The CAERUS consortium aims to identify humanitarian relief actions that pave the way for human development and stability in post-crisis societies. In particular, we aim to:

1) improve policies for transitional situations at global and regional level as well as strengthen operational policies in the field;

2) better understand the role of health and education as a drivers of stability in post-crisis settings;

3) adapt and apply existing European technologies to improve the efficiency of relief to development action.

Description of the work

Our research focuses on health and education in post-conflict and post-disaster settings. We will investigate how improved sectoral policies and delivery channels can help shape overall policies addressing the transition from fragility to resilience and development.

We will also implement population-based studies in key crisis-affected areas to obtain field evidence regarding the effects of such policies on populations. We will combine quantitative and qualitative data to investigate health equity, provision of health services by non-state armed actors, and the role of education in post-conflict. We will map vulnerabilities through geocoded information.

We will also seek to detect barriers to the provision of basic services in post-crisis settings. The CAERUS project will assess how European technologies, especially field telecommunications and mobile laboratory capacities, can be used to increase the timeliness and effectiveness of service provision in remote areas. At the same time these activities will increase European capacities to respond to outbreaks of rare and emerging diseases with pandemic potential.

Expected results

- Policy and operational recommendations for transition to development phases;
- Evidence from field studies on health equity, provision of health services by non-state armed actors, and the role of education in post-conflict areas;
- Guidelines on the use of technologies, such as mobile laboratories and rapid diagnostic tests, in fragile settings to improve service delivery.

PARTNERS	COUNTRY
Université Catholique de Louvain (UCL)	Belgium
Forskningstiftelsen FAFO (FAFO)	Norway
European Center for Development Policy Management (ECDPM)	The Netherlands
Norsk Institut for Luftforsking (NILU)	Norway
Paris-Lodron-Universität Salzburg (PLUS)	Austria
The Royal Institute of International Affairs (RIIA)	United Kingdom
Jadavpur University (JU)	India

COBACORE / Community Based Comprehensive Recovery

© Thinkstock

Information

Grant Agreement N°
313308
Total Cost
€4,378,908.70
EU Contribution
€3,497,636.07
Starting Date
01/04/213
Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK – (TNO)
TNO Defense, Safety and Security
Oude Waalsdorperweg 63
2597 AK The Hague
THE NETHERLANDS
Contact
Paul A.J. Tilanus
Tel: +31 88 866 72 92
Fax: +31 88 866 73 75
E-mail: paul.tilanus@tno.nl
Website: www.tno.nl

Project objectives

The Community Based Comprehensive Recovery (COBACORE) project aims to support common needs assessment and recovery planning efforts in complex multi-sectorial, multi-stakeholder crisis environments by building upon the community as an important source of information and capabilities. COBACORE aims to help bridge the so-called collaboration gap: failure of collaboration through insufficient information sharing among partners, incompatible work practices and misaligned decision making processes. In the field of humanitarian needs assessment, this collaboration gap is ubiquitous and detrimental to the efficiency of many recent relief efforts. Closing this gap is the key to reduce the time needed for needs assessment, better needs monitoring, and planning.

The COBACORE project has four specific objectives: 1) Understand the domain of common needs assessments, 2) Develop a supporting environment for common needs assessment processes, 3) Evaluate the COBACORE workspace in a realistic setting and 4) Achieve transfer of concepts and tools to stakeholder communities.

Description of the work

COBACORE is a set of interconnected modules and mechanisms that maintain three state models: the community model, the context model, and the needs model. The information contained in these models is accessible for users through a collaborative workspace, customized to suit their needs and preferences. The models are built up post-crisis through collected data from the affected area, through collaborative manual completion and maintenance, and through use of existing information sources, and based upon generic frames that are developed in advance for different scenarios. Various supporting functions monitor and manage the models, and respond to demands from users.

The project has three major phases: the preparatory phase, the concept development phase and the evaluation and dissemination phase. In the preparatory phase, activities are mainly aimed at understanding the domain, preparing the case studies and setting the boundaries of work. In the concept development phase, project activities are geared at knowledge acquisition and user requirements analysis, whereas the evaluation and dissemination phase is mostly focused on concept evaluation and dissemination activities. Concept development and evaluation with end-users take places during every phase of the project.

Expected results

The COBACORE project will develop a platform through which greater cross-jurisdictional and joined-up delivery mechanisms can enhance the preparedness and response model to disasters (both natural and man-made) at different geographic scales (national, regional and community). The COBACORE platform is a web-based, information-driven workspace that is readily accessible from mobile devices, operational centers and remote locations. The platform will have different interfaces for the different stakeholders in the damage and post-crisis needs assessment community, tailored to suit user-specific demands and capabilities.

The COBACORE suite of tools will support common needs assessments efforts – damage recovery needs, economic needs, health and social needs, and other critical humanitarian needs. The COBACORE assets will stimulate community-wide involvement in information gathering, sensemaking, and needs assessment practices. The COBACORE will not replace but complement existing practices and tools, and will stimulate a community-based approach to needs assessment processes.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
University of Ulster (UU)	United Kingdom
Het Nederlandse Rote Kruis (NLRC)	The Netherlands
Deutches Rotes Kreuz EV (GRC)	Germany
Stichting Katholieke Universiteit Brabant Universiteit van Tilburg (TU)	The Netherlands
Downey Hynes Limited (DHP)	Ireland
Integrasys SA (INT)	Spain
Causeway Data Communications LTD (GEOP)	United Kingdom
Žilinska Univerzita v Žiline (UZ)	Slovakia

DESTRIERO / A DEcision Support Tool for Reconstruction and recovery and for IntEroperability of international Relief units in situations, including CBRN contamination Risks

Information

Grant Agreement N°
312721
Total Cost
€4,171,403.71
EU Contribution
€2,933,015.58
Starting Date
01/09/2013
Duration
36 months

Coordinator

E-GEOS (EG)
Product Development and Programs - Defence and Security
Via Stanislao Cannizzaro 71
00156-Rome-Italy
Contact
Maria Michela Corvino
Tel: +39 06 4079 6363
E-mail: michela.corvino@e-geos.it
Website: www.destriero-fp7.eu
www.egeos.it

Project objectives

DESTRIERO's objective is to develop a next generation post-crisis needs assessment tool for reconstruction and recovery planning. This will include: structural damage assessment and related data integration and analysis based on international standards; and novel (automated) data and information interoperability across organisations and systems in combination with an advanced multi-criteria decision analysis tool and methodology for multi-stakeholder information analyses, priority setting, decision making and recovery planning.

DESTRIERO aims to develop an advanced net-centric information management tool to support damage and needs assessment and the reconstruction and recovery phases in post-crisis situations.

» DESTRIERO envisions an integrated framework with the following innovative functionalities: support continuous damage and contamination assessment, monitoring and updating through a combination of satellite data and aerial photos enriched with data from the field

» Boost information sharing by "automated" data and information interoperability between relief organisations and their information systems for coordinated PDNA (post-crisis damage and needs assessment) and RRP (reconstruction and recovery plan) processes

» Visualisation of these data in a common operational picture with links to needs assessments and recovery planning information within a multilayer GIS type user interface

» Support prioritisation and joint decision making with a novel tool, based on a recently developed decision support methodology and prototype software

» Centralise management information in a single location, including PDNA and RRP frameworks

Description of the work

Today more people than ever are threatened by disasters, with no regards if natural or man-made. DESTRIERO aims at developing a next generation post-crisis needs assessment tool for reconstruction and recovery planning.

Earth observation images will contribute to fast damage assessment and monitoring of the areas, together with data acquired by relief units on the field using novel smart-phone apps.

Identified needs will be recorded, stored and made available to all organisations involved.

Coordination and collaborative work at all levels of the organisations and among different ones will be possible through a network centric approach for the interoperability of information and service and the decision support tool. Critical infrastructure recovery will be considered a priority, as it's essential for the recovery of social and economic aspects (roads, bridges, schools, hospitals, plants, etc.), CBRN contamination and humanitarian aspects will also be taken into consideration, as aggravating circumstances, while support to accountability of humanitarian aid contributions will be facilitated.

Preliminary and Expected results

The DESTRIERO Project expected results are the following:

» Faster and better damage assessment for planning and monitoring of progress of recovery also integrating a dedicated Decision Support System to prioritize the recovery activities;

» Improved damage assessment by integrating open data (e.g. Copernicus emergency mapping), satellite data, aerial photos, data from the field (e.g. from mobile devices) and feeds from the social networks into a coherent information management tool.

- CBRN in-depth area contamination evaluation. The DESTRIERO tool offers the capability to define, adopting consolidated propagation models, and exact contour lines of contaminated areas after a CBRN disaster has occurred.
- Fast and intuitive access for distributed users to visualize the dynamic "common operational picture" by a web and user-friendly HMI.
- Tagging of geographical areas and damaged buildings on satellite images will enable distributed users in control rooms or on the field to drill down to different layers
- Support standardisation of assessment data, interoperability between different information systems thanks to the extension of MIP standards
- Enable better collaborative decision making during the planning and reconstruction phase also adopting a dedicated communication component to provide SMS exchange and teleco capabilities
- DESTRIERO tool will offer standard damage assessment templates, built on internationally agreed procedures and standards (e.g. DaLa), to collect data in homogeneous formats

PARTNERS	**COUNTRY**
e-GEOS (EG)	Italy
Consorzio Interuniversitario Nazionale per L'Informatica (CINI)	Italy
Thales (TRT)	France
Amper Programas de Electronica y Comunicaciones (AMPER)	Spain
Universitat Politecnica de Valencia (UPVLC)	Spain
Fraunhofer Institute for Industrial Engineering IAO (FHG)	Germany
Asociacion de Empresas Tecnologicas Innovalia (INNO)	Spain
Sesm Soluzioni Evolute per la Sistemistica e i Modelli S.C.A.R.L. (SESM)	Italy
ITTI Sp Zoo (ITTI)	Poland
Saadian Technologies Limited (SAADIAN)	Ireland
Fundação Assistência Médica Internacional (AMI)	Portugal
Police Service of Northern Ireland (PSNI)	United Kingdom
Slozkola Glowna Sluzby Pozarniczej (SGSP)	Poland

HELP / Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems

© Rafal Olechowski - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261659
Total Cost
€1,352,219
EU Contribution
€991,255
Starting Date
01/02/2011
End Date
30/04/2012

Coordinator

UNIVERSITAT POLITÉCNICA DE CATALUNYA
Signal Theory and Communications
Jordi Girona 31
08034- Barcelona-
Spain
Contact
Oriol Sallent
Tel: +34 93 4017197
Mobile: +34 619 35 16 54
Fax: +34 93 4017200
E-mail: sallent@tsc.upc.edu
Website:
www.fp7-sec-help.eu

Project objectives

It is generally acknowledged that existing wireless communication networks frequently fall short of meeting users' needs and cannot properly support the management of emergency and disaster relief scenarios. HELP will establish a comprehensive solution framework for supporting public safety communications aspiring to significantly enhance the communications in emergency situations. The envisioned solution framework consists of significantly strengthening the role and commitment of commercial wireless infrastructures in the provision of public safety communications. Only a solution framework targeted at creating and exploiting synergies of composite radio systems encompassing commercial and professional mobile radio networking technologies can address the complex requirements of modern emergency communications. HELP will define and establish the foundations for the development of network and spectrum sharing concepts between networks. HELP will identify the key features and functional building blocks of the operations and management system needed to achieve a synergic and holistic operation of the composite radio systems.

Description of the work

HELP will firstly identify operational user requirements, scenarios and overall system requirements. The scenarios will be created jointly with a User Advisory Board (UAB), formed by public safety users from diverse emergency service organisations. Then, HELP will define a solution framework (system concept) for the provision of public safety communications over diverse wireless infrastructures.

This will include, e.g.:

» determining internetworking solutions,

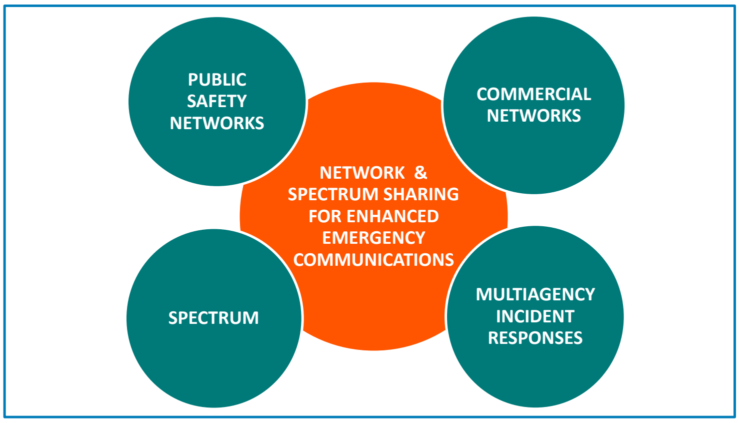
» determining the required features and functionalities that will enable the use of commercial systems for public safety communications in emergency and disaster relief operations, and

» determining new spectrum usage models to enhance communications in emergency scenarios by means of proper spectrum management mechanisms.

An Operator Advisory Board (OAB) will be established to validate the envisioned system concept. Following this, a framework for the management of the composite emergency network will be defined. Besides, the economic impact that the novel technical solutions proposed in HELP may have on the involved stakeholders will be investigated. HELP will eventually establish a consolidated basis and roadmap for the realisation of the envisioned solution framework.

Results

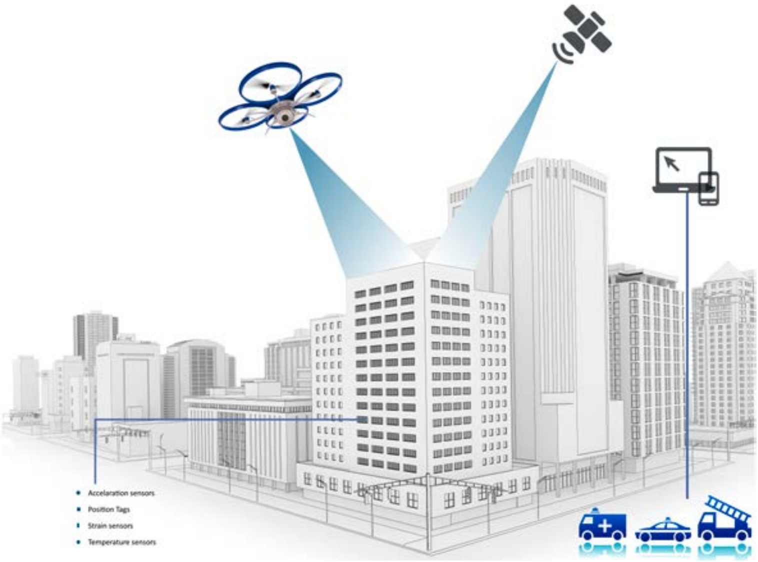
The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.


PUBLIC SAFETY NETWORKS
COMMERCIAL NETWORKS
NETWORK & SPECTRUM SHARING FOR ENHANCED EMERGENCY COMMUNICATIONS
SPECTRUM
MULTIAGENCY INCIDENT RESPONSES

© Project HELP Consortium

PARTNERS	COUNTRY
Universitat Politècnica de Catalunya (UPC)	Spain
DataX Sp. z o.o. (DTX)	Poland
Cassidian S.A.S. (EADS DS)	France
BAPCO LBG (BAPCO)	United Kingdom
European Commission - Joint Research Centre (JRC)	Belgium

RECONASS / Reconstruction and REcovery Planning: Rapid and Continuously Updated COnstruction Damage, and Related Needs ASSessment



Information

Grant Agreement N°
312718
Total Cost
€5,479,160.80
EU Contribution
€4,260,240.00
Starting Date
01/12/2013
Duration
42 months

Coordinator

INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS, (ICCS)
I-SENSE Group
9, Iroon Politechniou Str.
Zografou
Building of Electrical Engineers, Office 2131
GR-15773, Athens GREECE
Contact
Angelos Amditis
Tel: +30 210 772 2398
Fax: +30 210 772 2291
E-mail:
A.Amditis@iccs.gr
Website:
http://www.iccs.gr/eng/
http://i-sense.iccs.ntua.gr/

Project objectives

This work aims to develop a monitoring system for constructed facilities to provide a reliable, near real-time assessment of the structural condition and damage of both the structural components and the structural system of the monitored facility as a whole, after a disaster.

The scientific and technological objectives include:

1. SotA analysis for post-crisis damage and needs assessment tools;
2. Development of an indoor, automated, real-time, wireless, local positioning system by using 3D localization of tags for information gathering;
3. Development of method and software for assessment of economic loss, building functionality, volume of debris, duration of repairs and needs in manpower and materials;
4. Use of sensor-based damage assessment of the monitored buildings for calibrating and validating the remote sensing methods;
5. Demonstration of the RECONASS system in a 1:2 scale 3-storey reinforced concrete building;
6. Deployment of UAV for data analysis and evaluation;
7. Conceptualize the use of sensor-equipped buildings for additional threat detection (e.g. chemical or biological contamination).

Description of the work

RECONASS' main work packages include:

» User Requirements and System Architecture;

» RECONASS Monitoring System-Accurate Positioning-Secure Communication;

» Damage, Loss and Needs Assessment;

» Synergistic Damage Assessment with Air- and Space-borne Remote Sensing- Synoptic and Building-Specific Integration;

» The PCCDN Tool;

» System Integration;

» System Evaluation.

Expected results

RECONASS is expected to deliver:

- A combination of FMCW radar techniques with RF beam-steering and/or a multi band RF front end;
- A stable/portable gateway will be developed having extended capabilities to offer ubiquitous connectivity and seamless services;
- Photogrammetric processing of oblique airborne imagery taken from an UAV or satellite.

Its social and economic consequences include speeding up restoration and reconstruction efforts, providing updated information to response crews, reducing disaster costs and promoting safety.

PARTNERS	COUNTRY
Institute of Communication and Computer Systems (ICCS)	Greece
Technische Universität Dresden (TUD)	Germany
Swedish Defense Research Agency (FOI)	Sweden
RISA Sicherheitsanalysen GMBH (RISA)	Germany
Technice e Consulenze Nell' Ingegneria Civile SPA (TECNIC)	Italy
D. Bairaktaris & Associates Structural Design Office (DBA)	Greece
GEOSIG AG (GS)	Switzerland
University of Twente, Faculty of Geo-Information Science and Earth Observation (ITC)	The Netherlands
Bundesanstalt Technisches Hilfswerk (THW)	Germany

SAFE-COMMS / Counter-terrorism crisis communication

© Loren Rodgers - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218285
Total Cost
€1,397,232
EU Contribution
€1,088,244
Starting Date
01/04/2009
End Date
31/03/2011

Coordinator

BAR-ILAN UNIVERSITY
Department of Political Studies
Bar-Ilan Campus
Ramat Gan 52700
Israel
Contact
Dr. Shlomo Shpiro
Tel: +972 3 531 7061
Mobile: +972 544 550 840
Fax: +972 3 736 1338
E-mail: sshpiro@bezeqint.net
Website:
http://faculty.biu.ac.il/~sshpiro

Project objectives

The goal of this project was to help public authorities in Europe better react to terror incidents by providing effective communication strategies for the aftermath of terror attacks.

Results

During the initial stages of the project, the SAFE-COMMS partners undertook a comprehensive review of literature already published on the topic. The review examined articles in the area of crisis communication and those focused on communication following a terrorist attack.

This provided an overview of the key terms and variables relevant to this area. The project also conducted stakeholder interviews with police, fire brigades, armed forces officers, emergency medical services personnel, government officials, journalists from both public and private TV stations, and spokespersons of major hospitals.

In the next stage of SAFE-COMMS' research, actual examples of terrorist incidents in Europe were selected for incorporation into the project's case-study phase. The case studies were chosen to reflect the full range of possible terrorist attacks.

Conclusions drawn by the project's consortium partners from their analysis argue that:

» there is a need for a coherent crisis management plan that includes clear strategies for communication with other emergency services;

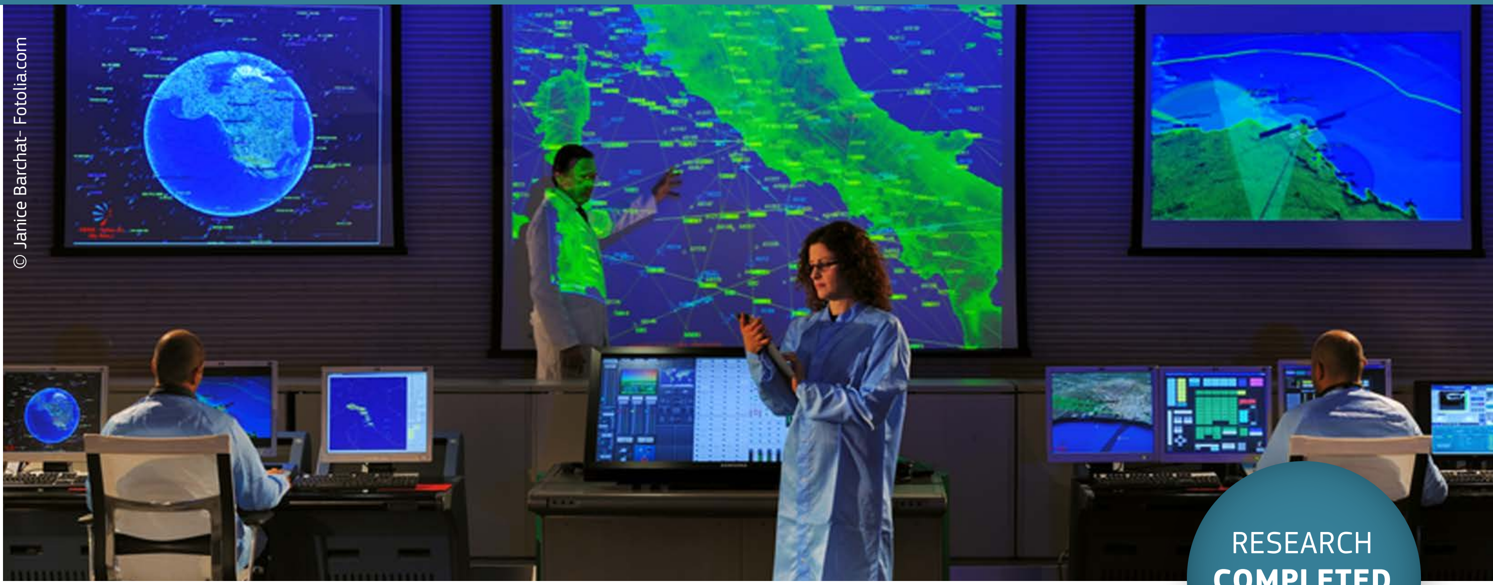
» plans should be effectively and widely disseminated in preparation for an attack;

» it is important to develop strategies to protect victims from the media;

» time, space and support are needed for public authorities to assess and come to terms with traumatic incidents.

PARTNERS	COUNTRY
Bar-Ilan University	Israel
A&B One GmbH	Germany
Research Institute for European and American Studies	Greece
University of Ulster	United Kingdom
Universidad de Burgos	Spain
University of Rousse Angel Kunchev	Bulgaria

CRISYS / Critical Response in Security and Safety Emergencies



© Janice Barchat- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261682
Total Cost
€805,852
EU Contribution
€740,945
Starting Date
01/02/2011
End Date
31/05/2012

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Avenue de Tervuren 270
B-1150 Brussels,
Belgium
Contact
Nicola Iarossi
Tel: +32 (0)2 7770255
Mobile: +32 (0)472990751
Fax: +32 (0)2 7758112
E-mail:
nicola.iarossi@eos-eu.com
Website:
www.crisys-project.eu

Project objectives

To build in this Phase (Phase I) a roadmap capable of full implementation to show specific demonstration actions in Phase II, whilst establishing contacts and awareness with the main public and private stakeholders in the field of Crisis Management.

The work done in the actual phase is aimed at full understanding of the issues surrounding effective operational needs (e.g. interoperability of technical solutions, commonality of procedures, decision and crisis decision tools, the importance of languages; common training approaches; homogeneous risk assessment methodologies etc.) for the most significant demonstration actions.

Description of the work

It is imperative to understand how the civil protection sector operates. Firstly we need to review presently adopted solutions, procedures and the operational, legal, societal, political and, legacy environments in which those mechanisms are set. We can then establish parameters of operations, not simply scenarios but how to create wider capability and capacity.

Users and citizens are the critical success key for the project. Building a respected relationship is a vital part of the project. That requires the creation of a public-private dialogue with local, national and international users, first responders and national governments and citizens.

The role of CRISYS Partners is therefore to gather these requirements via specific MEETINGS with USERS and SUPPLIERS around Europe, thus establishing a sound network of contacts for Phase II whilst also gathering the key elements to develop the requirements for the Roadmap.

This process will be followed by a gap analysis activity of the collected results, in two steps, from a preliminary roadmap to a final roadmap which will be presented at a final conference.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
European Organization for Security (EOS)	Belgium
EDISOFT SA (EDI)	Portugal
Center for Security Studies (KEMEA)	Greece
National Center for Scientific Research, “Demokritos” (NSCRD)	Greece
ALTRAN BV (ALTRAN)	The Netherlands
International Association of Fire and Rescue Services (CTIF)	France
Teletron Euroricerche SRL (TLT)	Italy
Compania nationala de transport al energiei eletrice Transelectrica SA (TRA)	Romania
Société Françoise de Medicine de Catastrophe (SFMC)	France
THALES Security Solution & Service SAS (T3S)	France
Indra Sistemas S.A (INDRA)	Spain
Istituto Affari Internazionali (IAI)	Italy
University of Central Lancashire (UCLAN)	United Kingdom
Ministry of the Interior, Department for Rescue Services, SISAASIAINMINISTERIO (FMOI)	Finland
Zanasi Alessandro SLR (ZAN)	Italy

DARIUS / Deployable SAR Integrated Chain with Unmanned Systems (SAR = Search and Rescue)

© alxpin - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284851
Total Cost
€10,688,505
EU Contribution
€7,475,830
Starting Date
01/03/2012
End Date
28/02/2015

Coordinator

BAE SYSTEMS (OPERATIONS) LTD
BAE Systems, Engineering
Marconi Way
Rochester, Kent, ME1 2XX,
United Kingdom
Contact
Richard Cross
Tel: +44 1634 844400
E-mail: contact@darius-fp7.eu
Website: www.darius-fp7.eu

Project objectives

» Interoperability of unmanned platforms

» Seamlessly integrate unmanned platforms in the

» command-and-control loop (i.e. C2/C4I platforms)

» Provide the necessary communication structure without relying on existing infrastructure

» Support interaction between humans and systems, i.e. FRs, victims, unmanned vehicles and payloads

» Develop a generic ground station

» Define the capability, deployability and sustainability requirements for future SAR unmanned vehicles

» Define and evaluate operational performance improvements of current deployed solutions

» Reduce the cost of unmanned SAR solutions

Description of the work

DARIUS' work was broken down into seven work packages (WPs).

WP1: Project management.

WP2: User Needs and Concept of Operations

WP3: Integration Design. Generation of requirements and interoperability standards

WP4: Components Development. Adaptation of existing unmanned platforms and ground system to meet DARIUS requirements.

WP5: Integration. Integration and testing of the DARIUS platforms and ground stations prior to evaluation and trials.

WP6: Evaluation and Trials: Testing the DARIUS solution in urban/indoor, forest fire and maritime SAR scenarios.

WP7: Exploitation. Dissemination of project results, exploitation issues and final standards, and legal recommendations.

Results

The project delivered a fully working, modular, scalable and sustainable prototype of a system-of-systems formed by heterogeneous and diverse unmanned platforms equipped with various payloads.

This objective was achieved by designing a Generic Ground Station (GGS) to provide command and control tasking of multiple unmanned vehicles simultaneously, with overall situation awareness and visualisation of the sensor outputs of the multiple unmanned vehicles. Associated data interface standards have been defined to ensure interoperability with a smooth and transparent data flow between the GCS of the unmanned platforms and the GGS where this information is orchestrated to providing the operator with a continuously updated common operational picture. The system was fully integrated in the command and control chain with a consistent communication network.

The consortium also delivered several components that can significantly enhance SAR operations, either individually or in the context of the integrated system of systems. The project's prototype required the adaptation and enhancement of the ground control station software of several unmanned platforms (aerial, ground and marine) and payloads to enhance their capability and compliance with the DARIUS common protocol to deliver a fully interoperable solution.

A number of side products, having their own potential in SAR, were developed and delivered by members of the consortium. These include the DARIUS common protocol, a portable tactical command post (Generic Ground Station), a portable sensor for detecting levels of dangerous chemicals, a 4G wireless telecommunication network (WiMAX), a command-and-control module for integrating SAR operations data with legacy command and control systems, and a mobile application.

Throughout the project there was continuous engagement with end users to ensure that the systems developed were fit for their intended purpose and will add real value to SAR missions.

A comprehensive exploitation plan was developed, and the project team was committed to ensure that all stakeholders achieved maximum benefit from the research project.

PARTNERS	**COUNTRY**
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Cassidian S.A.S. (CASS)	France
DFRC AG (DFRC)	Switzerland
SKYTEK LTD (SKY)	Ireland
TELINT RTD Consultancy Services LTD (TEL)	United Kingdom
FUTURE INTELLIGENCE EREVNA TILEPIKINONIAKON KE PLIROFORIAKON SYSTIMATON EPE (FINT)	Greece
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONE)	France
STIFTELSEN SINTEF (SIN)	Norway
ECA SA (ECA)	France
NATIONAL TECHNICAL UNIVERSITY OF ATHENS (NTUA)	Greece
CENTER FOR SECURITY STUDIES (KEM)	Greece
ECOMED bvba (ECO)	Belgium
CORK INSTITUTE OF TECHNOLOGY (NMCI)	Ireland
CEREN	France

ELITE / Elicit To Learn Crucial Post –Crisis Lessons

© Baloncici - photodune

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312497
Total Cost
€1,185,911.40
EU Contribution
€940,418
Starting Date
01/01/2013
End Date
18 months

Coordinator

UNIVERSIDAD DE NAVARRA (TECNUN)
Paseo Manuel de Lardizabal 13
20018 Donostia-San Sebastian
Spain
Contact
José María Sarriegi
Tel: +34 943 21 98 77
Fax: +34 943 31 14 42
E-mail: coordinator@elite-eu.org
Website: www.elite-eu.org/

Project objectives

The overall objective of the ELITE project was to improve European emergency preparedness, response and recovery from natural disasters such as floods, large scale forest fires and earthquakes. For this purpose several sub objectives were defined:

» To establish a Community of Practice (CoP) in Crisis Management to improve the sharing of lessons learned and disaster knowledge among different organizations involved in the crisis management process such as responders, civil protection agencies, NGOs, critical infrastructures, private firms and industries etc.

» Create a tested and validated ELITE living document of crisis management. The ELITE living document is a publicly available web solution comprised of:
- + A "living" repository of best practices
- + A "living" repository of guidelines
- + Social media features where authorised agents can freely operate and interact

» Implement the ELITE living document gathering information from experts through three scenario based workshops, a table-top exercise and interviews.

» Analyse the learning process from lessons learned to lessons implemented to identify the existing difficulties

» Deliver recommendations for future research. The project will deliver recommendations for future research in these topics:
- + Knowledge gathering, categorisation and analysis processes
- + Best practices and guidelines for each individual analysed disaster type: floods, earthquakes and fires.
- + Integration of common aspects of different disaster types.
- + Use of social media for learning and cooperation purposes.

Description of the work

The project was divided into six workpackages:

WP1: Management

WP2: ELITE Community of Practise –Workshops
Four scenario based workshops were arranged for each disaster scenario (Fires, Earthquakes, Floods and Holistic). The ELITE CoP contributed to the founding of the lessons learned database, to required validations and to dissemination and continuous update of the living document.

WP3: ELITE living document of crisis management
WP3 built upon information from WP2 and comprised all the tasks needed to develop the living document, including requirement specification, design and programming.

WP4: Knowledge gathering, categorisation and analysis
WP4 included knowledge gathering, categorisation and analysis in order to develop a holistic analysis of lessons learned.

WP5: Learning process analysis
Through WP5 a framework for knowledge and experience transfer, and learning process improvement across organizations and countries within the EU were developed

WP6: Dissemination of lessons learned
It included the dissemination activities carried out by all partners at workshops, meetings, etc. and by building relations with major actors involved in natural disasters.

Results

- The establishment of the ELITE CoP involves relevant stakeholders in crisis management from a wide variety of backgrounds with the desire to share experiences and learn from others.

- A tested and validated living document, which integrates the lessons learned in previous disasters and facilitates the sharing of this knowledge among the members of the ELITE CoP. The content of the living document is being continuously updated by the members of ELITE CoP

- A holistic framework for post-crisis lessons learned reporting that serves experts at different levels in the crisis management sector to identify and categorize lessons learned and best practices from different disasters. It also provides solutions to transfer knowledge between disaster areas.

- A set of evaluation criteria to analyze the transfer of knowledge and experiences within the learning processes identifying their benefits and weaknesses. ELITE project has achieved to extract the underlying knowledge and the process to transfer experience in crisis management with the goal of guaranteeing continuous improvement.

- Dissemination in journals, conferences and media of the guidelines and recommendations for improving the learning process developed on the ELITE project.

PARTNERS	COUNTRY
Universidad de Navarra (TECNUN)	Spain
Forsvarets Forkninginstitutt (FFI)	Norway
Hogskolen I Gjovik (GUC)	Norway
Forschungsinstitut des Rotten Kreuzes (FRK)	Austria
I.S.A.R. Germany Stiftung Gemeinnutzige Ug (Haftungsbeschrankt) Gmbh	Germany
Thales S. A. (TRT)	France
Szkola Glowna Sluzby Pozarniczej (SGSP)	Poland
Consiglio Nazionale delle Richerche (IMAA-CNR)	Italy
Associazione dei Comuni Dell'Umbria	Italy

E-SPONDER / A holistic approach towards the first responder of the future

© E-SPONDER

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242411
Total Cost
€12,922,363.40
EU Contribution
€8,790,044
Starting Date
01/07/2010
End Date
31/12/2014

Coordinator

EXODUS S.A.
6-10 Farandaton Street
11527, Athens
Greece
Contact
Dr. Dimitris Vassiliadis
Tel: +30 210 7450321
Fax: +30 210 7450399
E-mail: dvas@exodussa.com
Website: www.e-sponder.eu

Project objectives

The proposed system addresses the need for an integrated personal digital support system to support first responders in crises occurring in various types of critical infrastructures under all circumstances. E-SPONDER proposes modular terminal and overall open system architecture in order to facilitate the need for enhanced support provision in all cases. It deals with the study, design and implementation of a robust platform for the provision of specialized ad-hoc services, facilities and support for first responders that operate at crisis scenes located mainly within critical infrastructures. In order to address the diverse needs stemming from the complexity of operations, a three-layer approach is proposed. Modularity is a key issue to the overall system design whether it refers to the mobile/dispersed units of the first responders or the back-office applications, systems and services.

» *First Responder Units (FRU).* As far as the first responders' units are concerned, different operational needs have to be addressed according to the origin of the first responder. In other words, there are different functional, performance and specific requirements for different users including police officers, paramedics, rescuers and fire brigade crews;

» *Mobile Emergency Operations Centre (MEOC).* The Mobile Emergency Operations Centre is a vital part of the entire system. It provides a common operational picture of the situation as well as a communication bridge between the first responders that operate in the field and the main, remotely located Emergency Operations Centre (usually located at Civil Protection Headquarters);

» *Emergency Operations Centre (EOC).* The Emergency Operations Centre is the heart of the E-SPONDER platform. It contains the entire necessary infrastructure (communications, GIS, data processing modules, database) suitable and selected for crisis management purposes;

» *Training of First Responders.* The goal of the E-SPONDER platform is to provide, at both a state and local level, an up-to-date list of available trained personnel that can be identified and deployed quickly in the event of a crisis situation. In that sense, E-SPONDER will help the authorities to better define first responder job profiles and technical competencies. These profiles and competencies will then be managed by the e.Learn platform that will link individual competency gaps to learning and development, and create a central repository of resources and associated skill sets for proactive selection and succession planning;

» *Logistics of First Responders.* A full and comprehensive analysis and study of the current situation as well as the one derived from E-SPONDER outcomes will be performed in order to set up the conceptual design parameters of an Emergency Management Process based on ERS&LS (Emergency Resource Support & Logistics System) capable of providing comprehensive situational awareness to decision makers to ensure a timely, co-ordinated and effective response to large scale disasters.

Results

1. Provide a new generation First Responder Support Platform:

   a. A complete First Responder Unit (FRU) comprising of:
   - Interoperable wireless communication system
   - Ubiquitous and seamless localisation and navigation
   - Protective garment engineered to accommodate wearable chemical and physiological sensors and motion detection and activity classification

- A mobile computing element (a smartphone and a custom designed communication board)

b. Design and implementation of a centrally-located Emergency Operation Centre (EOC) having full control over remote operations:
   - Flexible communications infrastructure
   - Customisable communication management
   - Logistics Management System

c. A Mobile Emergency Operations Centre (MEOC) acting as an ad-hoc replica of the EOC; a mobile command post

d. A flexible architecture with improved data fusion, interconnection and interoperability between different system elements

e. Integration of different innovative and existing devices

2. The project studied the underlying socio-economic environment where E-SPONDER technology may operate by addressing:

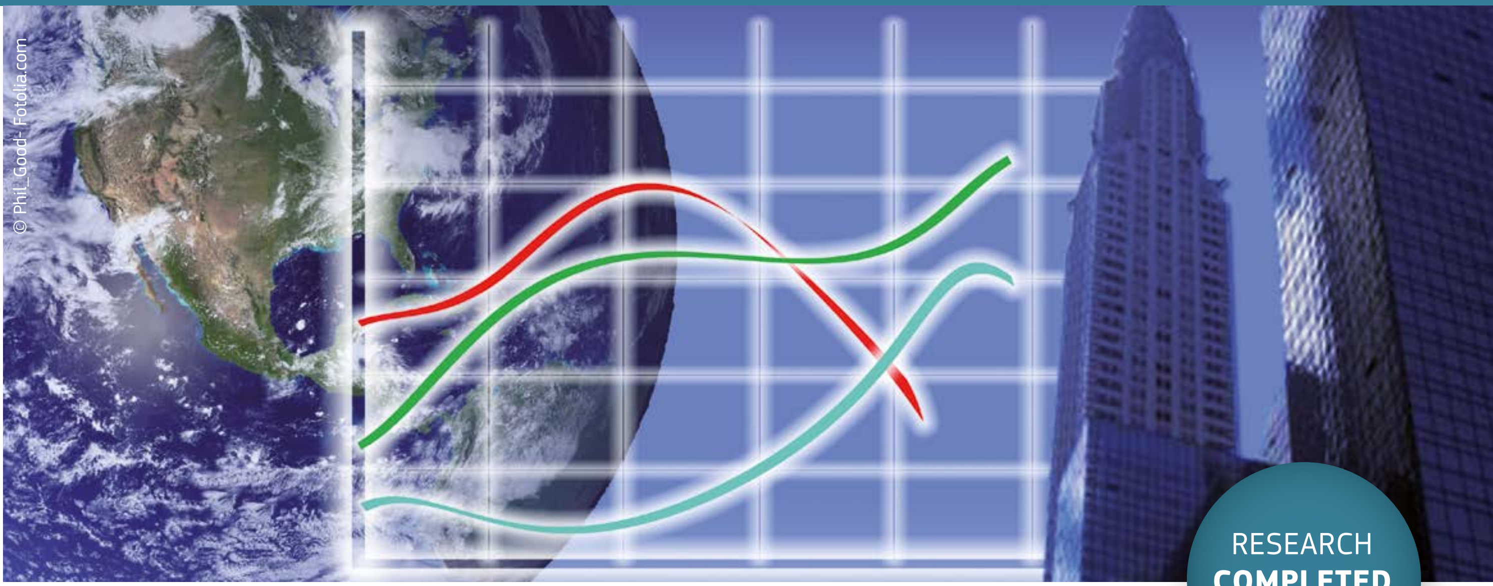
a. The emerging training needs for increased operational efficiency

b. The regulation framework, legal and standardization issues relevant to E-SPONDER's objectives and research

3. E-SPONDER demonstration and validation in full-scale pilots (aircraft crash, building collapse and vessel fire)

PARTNERS	COUNTRY
Exodus S.A.(EXO)	Greece
University of Modena and Reggio Emilia (UNIMORE)	Italy
CrisisPlan B.V. (CPLAN)	The Netherlands
Prosyst Software GmbH (PROS)	Germany
Immersion S.A. (IMM)	France
Rose Vision (ROSE)	Spain
Telcordia Poland Sp. z.o.o. (TARC-PL)	Poland
Centre Suisse d'Electronique et de Microtechnique S.A. (CSEM)	Switzerland
Smartex Srl (SMTX)	Italy
Technische Universität Dresden (TUD)	Germany
YellowMAP AG (YA)	Germany
PANOU S.A. (PANOU)	Greece
Telcordia Taiwan (TARC-TW)	Taiwan
Institute for Information Industry (III)	Taiwan
Entente pour la forêt Méditerranée (EPLFM)	France

ESS / Emergency support system



© Phil_Good- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217951
Total Cost
€14,025,624.80
EU Contribution
€9,142,126
Starting Date
01/06/2009
End Date
31/05/2013

Coordinator

VERINT SYSTEMS LTD
Mr. Gideon Hazzani
33 Maskit St Herzliya,
46733 Israel
Contact
Mr. Gideon Hazzani
Email: Gideon.Hazzani@verint.com
Website: www.ess-project.eu

Project objectives

The purpose of ESS is to enable improved control and management of major crisis events such as natural disasters, industrial accidents, terror attacks etc. The idea guiding the development of ESS is a portable, modular and autonomous system which fuses in real-time various forms of field-derived data including video, audio, weather measurements, location tracking, radioactivity, bio-chemical, telecom derived data, affected population reports and other information. The data is collected and communicated via both portable and fixed platforms, including wireless communication devices, Unmanned Aerial Vehicles (UAV), Unmanned Ground Systems (UGS), air-balloons and field-vehicles. The fusion of the data is handled within a central system which performs information analysis and provides decision support applications for web based command and control systems. This provides flexible, yet comprehensive coverage of the affected area.

Once available to the market, the ESS concept will offer real time synchronization and information sharing between first responders and support forces at the site of the incident. ESS will also enable the commanders to communicate with the affected on-site personnel by sending text (SMS) or recorded voice messages.

Description of the work

The ESS consortium intends to develop a revolutionary crisis communication system that will reliably transmit filtered and pre-organized information streams to the crisis command system, which will provide the relevant information that is actually needed to make critical decisions.

The information streams in ESS will be organized in such a way that they can be easily enhanced by and combined with other available applications and databases (thus enabling the coupling of the ESS system with crisis decision support systems currently under development). The ESS will provide an open API in order to allow any public authority, if needed, to add more applications customized to its particular needs. ESS interfaces are open as they are based on OGC standards. Each commercial application which will adopt OGC standards will be able to connect to ESS in a plug and play manner.

Any abnormal event may register as a sudden change or cumulative changes in one or several mediums which it interacts with (Telecom, Air, Spatial, Visual, Acoustic and more). Therefore, effective control of such an abnormal event means: monitoring each medium independently in real-time, activating an alarm when sudden or cumulative changes in one or more mediums are detected, and when necessary contacting the affected population and providing mass evacuation capabilities. ESS will integrate all these means to one central system which will enable crisis managers to respond to these challenges.

In order to validate the system it will be tested in three different test fields: a fire in a forested area, an event in a crowded stadium and a toxic waste dump accident. Operating ESS under different scenarios is needed in order to test the system's capabilities in different kinds of crises using a variety of collection tools.

The partners in the ESS project are at the forefront of technological development. Each of the partners brings important and complementary expertise to the project. Three partners represent the end users for ESS technologies, solutions and perspectives.

Results

The aim of the ESS project was to provide crisis managers with information needed to inform their decisions, and to mount an effective response. ESS' specific objectives included improving on-scene data collection, expanding the dissemination of accurate data and minimising the uncertainty inherent to crises.

The ESS project achieved the following:

- » The development and improvement of front-end data collection tools
- » The creation of a centralised data fusion system that connects to all front-end sensors activated in the system.
- » The synchronised dissemination of relevant data

Sensors are often hard to put in place in crisis situations, which leads to insufficient or broken data. To counter this problem, ESS worked on the integration of current technologies to generate portable sensor platforms (UAVs, air balloons, blimps, tripods, etc.), which are especially hardy and reliable in the face of extreme conditions.

To connect and harmonise all the information flowing from the sensors, ESS developed the "Data Fusion Mediation System" (DFMS) as a centralised database connected to all front-end sensors activated in the system. ESS improved communication between sensors and database, data fusion of data from different types of sensors and spatial data localisation.

To improve dissemination the project developed a web-based portal. The idea behind the ESS portal was to create an efficient synchronisation framework to manage data and information flows between different public authorities involved in emergency management operations and the crisis managers (rescue forces, police, fire-department, homeland-security, municipality, etc.). The ESS portal provided the involved actors with a common, uniform and ubiquitous platform for collecting, analysing and sharing real time data for supporting management decisions.

PARTNERS	**COUNTRY**
VERINT SYSTEMS LTD (VRNT)	Israel
Wind Telecomunicazioni SpA (WIND)	Italy
International Geospatial Services Institute GMBH (IGSI)	Germany
Intergraph CS (ING)	Czech Republic
GMV Sistemas S.A. (GMV)	Spain
CS Systèmes d'Information (CS)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAIS)	Germany
ITIS Holdings plc. (ITIS)	United Kingdom
Algosystems SA (ALGO)	Greece
Alcatel-Lucent Italia (ALI)	Italy
APD Communications Ltd. (APD)	United Kingdom
Anonymos Etaireia Antiprosopeion Emporiou Kai Viomichanias (ANCO)	Greece
FAENZI srl. (FNZI)	Italy
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
The Imego Institute (IMEGO)	Sweden
Magen David Adom (MDA)	Israel
Ernst & Young (EY)	Israel
Aeronautics Defense Systems (AERO)	Israel
DIGINEXT SARL (DXT)	France
Entente pour la forêt méditerranéenne (CEREN)	France

eVACUATE / A holistic, scenario-independent, situation-awareness and guidance system for sustaining the Active Evacuation Route for large crowds

© kwerensia_iStock

Information

Grant Agreement N°
313161
Total Cost
€13,135,530.71
EU Contribution
€8,583,311.91
Starting Date
01/04/2013
Duration
48 months

Coordinator

EXODUS S.A (EXO)
Department of Business
Developement and Delivery
73-75 Mesogeion Av &
Estias Str 1
115 26 Athens,
Greece
Contact
Dimitrios Vassiliadis
Tel: +30 2107450300
Mobile: +30 6947566676
Fax: +30 2107450399
E-mail: dvas@exus.co.uk
Website: www.exus.co.uk

Project objectives

The dynamic capture of situational awareness concerning crowds in specific mass gathering venues and its intelligent enablement into emergency management information systems, using smart communication devices and spaces is critical for achieving rapid, timely guidance and safe evacuation of people out of dangerous areas. Humans could be overwhelmed by fast changes of potentially dangerous incidents occurring at confined environments with mass-gathering. They could fail to make objective decisions to find their way to safety. This condition may lead to mass panic and make emergency management more challenging. To cope with these incidents, eVACUATE yields a holistic system:

- To provide a valuable tool to guarantee enhanced Situational Awareness both to the crowds involved during a crisis but also to the crews operating in situ as well as in remote locations (security crews, first responders, crisis managers)
- To adapt dynamically evacuation plans according to current conditions
- To provide an easy to use (visual, multi-lingual) set of safe evacuation instructions available over a multitude of alternative and complementary presentation channels under a resilient, reliable and robust way, regardless of the functionality of the “global network”
- To support civil protection authorities in the formation and validation of proper safety procedures for crowd management (Reconstruction of Experiences)
- To set a cornerstone for the standardization of equipment, processes and methodologies for evacuation purposes on an EU level, addressing the cross-cultural issues emerging from diversity imposed by citizens

Description of the work

The overall mission of the eVACUATE consortium is to research, develop and demonstrate the capabilities of a framework that will enhance the effectiveness of complex crowd evacuation operations by:

1. Defining a full architecture and developing underlying necessary technological backbone, designed to provide improved data fusion, interconnection and interoperability between the different system elements and layers, reducing data ambiguity to a minimum.

2. Providing a full-set of systems and services built in accordance to innovative, integrated standards and peer-to-peer architecture, supporting a variety of complex crowd evacuation operations. This will be achieved with:

- Monitoring crowd behavior, surveying current environmental conditions, controlling the evacuation flow and predicting incidents that could cause problems to the overall operations
- Dynamically simulating an evacuation in a faster than real-time way so as to predict potential (future) incidents evolving as a consequence of other current events, through a game awareness framework
- Developing a centralized Data Fusion Mediation System (DFMS) to provide together with the command and control modules, the web portal and the back-end applications, an accurate and intelligent coordination of activities during evacuation operations and decision making

3. Integrating different innovative and existing modules such as:

- Multiple types of sensors ranging from visual cameras and hyper-spectral imaging to RFIDs and pervasive technologies,
- Sophisticated early location devices, based on Wireless Sensors Networks consisting of low-power sensors nodes
- Communication between first responders, command

centers and the crowd itself with integrated networking platforms and ad-hoc mechanisms to guarantee resilient communications

and performing the necessary hardware and software enhancements, so that all involved system elements can be seamlessly integrated to the main platform while interoperability is ensured.

4. Studying and developing the underlying socio-economic environment by addressing ethics, legal issues, regulation societal context, standardization and National and International operating procedures

5. Demonstrating the developed system and validating its operational characteristics in full-scale field trials that will simulate realistic emergencies and crises. The whole system will be tested involving four different evacuation scenarios: a Football Stadium Scenario, an Airport scenario, a Cruise ship scenario and an Underground (Metro) scenario.

Expected results

eVACUATE foresees to develop an evacuation platform and strategy which through enhanced situational awareness will guide people away from the dangerous situations. In addition, eVACUATE is anticipating to increase effectiveness of forces responding to crisis in view of leading crowd to safer zones while reducing collateral damage, human errors and achieving faster restoration of security at the events venue and its affected proximities.

PARTNERS	COUNTRY
EXODUS S.A (EXO)	Greece
University of Southampton IT Innovation Centre (ITINNOV)	United Kingdom
Institute of Communications and Computer Systems (ICCS)	Greece
HKV LIJN in Water BV (HKV)	The Netherlands
Telesto Technologies (TEL)	Greece
Tekniker-Ik4 (TEK)	Spain
Athens International Airport S.A (AIA)	Greece
Vitrociset s.p.a (VITRO)	Italy
Crowd Dynamics International Limited (CDI)	United Kingdom
INDRA SISTEMAS S.A. (INDRA)	Spain
Katholieke Universiteit Leuven (KUL)	Belgium
Diginext SARL (DXT)	France
Politechnico Di Torino – Dipartimento di Matematico (POLITO)	Italy
STX France S.A (STX-FR)	France
Technische Universität Dresden (TUD)	Germany
Technische Universität Chemnitz (TUC)	Germany
Real Sociedad De Futbol S.A.D (ASRS)	Spain
Metro Bilbao S.A (METB)	Spain
Telecom Italia S.p.A (TIM)	Italy

FASTID / Fast and efficient international disaster victim identification

© FASTID

RESEARCH
COMPLETED

Information

Grant Agreement N°
242339
Total Cost
€2,990,190
EU Contribution
€2,270,476
Starting Date
01/04/2010
End Date
31/03/2013

Coordinator

THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION – I.C.P.O.
INTERPOL,
General Secretariat
200, Quai Charles de Gaulle
69006 Lyon,
France
Contact
Peter Ambs, Operational Police Support Directorate
Tel: +33 (0)4 72 44 72 92
Fax: +33 (0)4 72 44 73 80
E-mail: p.ambs@interpol.int
Website: http://www.interpol.int/FASTID.asp

Project objectives

» Development of an information management and decision support system for disaster victims and missing person identification satisfying end user requirements enabling the storing and comparison of different characteristics which may lead to the identification of any one individual;

» To develop an internationally acceptable format and training for accurate and repeatable data recording in the system;

» To test and evaluate the system;

» To develop exploitation strategies.

Description of the work

The project will start by collecting detailed end-user requirements.

It will be necessary to consider not only the performance of the system itself for international and national police work but also its interface with INTERPOL's present network and channels for uploading and distributing data and other identification software.

These requirements will feed into the design of the overall system and the specific specifications for system modules and interfaces.

A core system will be developed taking INTERPOL's paper Ante-Mortem (AM) Disaster Victim Identification (DVI) form and Post-Mortem (PM) DVI together with its Yellow Notice and Black Notice forms, which use the minimum international standards agreed to date for the collection of data for identification of victims and present software as a basis and these will be extended with Rich Internet Application methods and further identification techniques.

An 'aide aside' will be designed to facilitate a commonality of reporting and understanding of the terms in the INTERPOL forms leading to a better understanding of the nature of the data being recorded and its true international translation. This will form the starting point for a full online training programme which will be developed utilising the most effective and efficient means of ensuring operational commonality between countries and organisations.

Research will be carried out into image retrieval methods for assisting forensic identification with respect to faces, body modifications (e.g. tattoos), decorations, property and clothing. 3D morphing and craniofacial reconstruction and superimposition approaches will be investigated for this application. The best results are planned to be implemented into the core system.

There will be extended testing and evaluation of the results and these will allow for some development reiteration. Exploitation strategies will be developed.

Results

FASTID focused on developing a prototype database to support Interpol's "Disaster Victim Identification" (DVI) forms since the latter represent massive amounts of paperwork that are hard to navigate. To improve Interpol's database's search function several matching techniques were developed as part of the project whose research included DNA matching techniques and "image" matching techniques.

FASTID created methods to search image databases by content-based image retrieval methods, using tattoo images as a secondary means of identification, for example. It also explored identification of human skeletal remains using face recognition software (FRS) and craniofacial reconstruction (CFR) and superimposition (CFS).

The team developed face recognition methods to aid the identification of persons based on images through biometric algorithms. The project also created training material in support of global common operational methodologies regarding data recording in INTERPOL member countries.

The prototype system has been implemented on Interpols hosted platform in Lyon. Its conversion into actual production would aid international police cooperation for both disaster victim identification and for daily police work. The database has decentralized access for use in conjunction with mass fatality events and everyday policing requirements, for example.

PARTNERS	COUNTRY
International Criminal Police Organization - I.C.P.O. (INTERPOL)	France
Bundeskriminalamt (BKA)	Germany
Plass Data Software A/S (Plass Data)	Denmark
University of Dundee (UNIVDUN)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Crabbe Consulting Ltd (CCLD)	United Kingdom

ICARUS / Integrated Components for Assisted Rescue and Unmanned Search operations

© AllenVanguard - Calzoni - Francois Pomerlau

Information

Grant Agreement N°
285417
Total Cost
€17,554,528.49
EU Contribution
€12,584,933.45
Starting Date
01/02/2012
Duration
48 months

Coordinator

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
Department of Mechanics
Av. De La Renaissance 30
1000 Brussels, Belgium
Contact
Geert De Cubber
Tel: +32 2 7426553
Mobile: +32 478 640652
Fax: +32 2 7426547
E-mail:
geert.de.cubber@rma.ac.be
Website:
http://www.fp7-icarus.eu/

Project objectives

» Development of a light sensor capable of detecting human beings;

» Development of cooperative Unmanned Aerial System (UAS) tools for unmanned SAR;

» Development of cooperative Unmanned Ground Vehicle (UGV) tools for unmanned SAR;

» Development of cooperative Unmanned Surface Vehicle (USV) tools for unmanned SAR;

» Heterogeneous robot collaboration between Unmanned Search And Rescue devices;

» Development of a self-organising cognitive wireless communication network, ensuring network interoperability;

» Integration of Unmanned Search And Rescue tools in the C4I systems of the Human Search And Rescue forces;

» Development of a training and support system for the developed Unmanned Search And Rescue tools for the Human Search And Rescue teams;

» Communication and dissemination of project results.

Description of the work

In the event of a large crisis, a primordial task of the fire and rescue services is the search for human survivors on the incident site. This is a complex and dangerous task, which often leads to loss of lives. The introduction of unmanned search and rescue devices can offer a valuable tool for saving human lives and speeding up the search and rescue process. Therefore, ICARUS concentrates on the development of unmanned search and rescue technologies for detecting, locating and rescuing humans. In this context, there is vast literature on research efforts towards the development of unmanned search and rescue (SAR) tools. However, in the field, unmanned SAR tools still have great difficulty finding their way to the end-users.

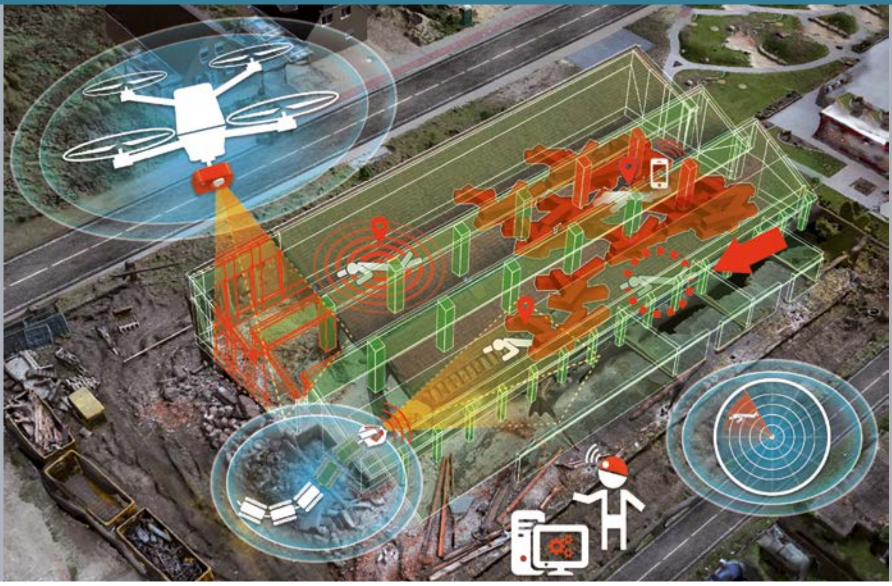
The ICARUS project addresses these issues, aiming to bridge the gap between the research community and end-users, by developing a toolbox of integrated components for unmanned search and rescue. The objective of the ICARUS project is to develop robots which have the primary task of gathering data. The unmanned SAR devices are foreseen to be the first explorers of the area, as well as in situ supporters to act as safeguards for human personnel. In order not to increase the cognitive load of the human crisis managers, the unmanned SAR devices will be designed to navigate individually or cooperatively and to follow high-level instructions from the base station. The robots connect wirelessly to the base station and to each other, using a wireless self-organising cognitive network of mobile communication nodes which adapts to the terrain. The unmanned SAR devices are equipped with sensors that detect the presence of humans. At the base station, the data is processed and combined with geographical information, thus enhancing the situational awareness of the personnel leading the operation with in-situ processed data that can improve decision-making. The Haitian experience has shown the importance acquired by the geographic component in the management of human and technical resources in crisis situations. Similarly, it has highlighted that a suitable distribution of thematic maps allows optimisation and interoperability of these resources and accelerates the access to victims. All this information will be integrated in existing C4I systems, used by the forces involved in the operations.

Expected results

The overall purpose of the ICARUS project is to apply its innovations for improving the management of a crisis and by doing so to reduce the risk and impact of the crisis on citizens. The use of unmanned search and rescue devices embedded in an appropriate information architecture and integrated into existing infrastructures will help crisis personnel by providing detailed and easy to understand information about the situation. The proposed system will inform crisis personnel about real dangers present on the ground, and will thus increase their performance in resolving the situation.

PARTNERS	COUNTRY
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
SPACE APPLICATIONS SERVICES NV (SPACE)	Belgium
ESTUDIOS GIS S.L. (E-GIS)	Spain
Centre de Tecnologia aerospacial (CTAE)	Spain
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IZM)	Germany
INSTYTUT MASZYN MATEMATYCZNYCH (IMM)	Poland
JMDTHEQUE SARL (JTH)	France
TECHNISCHE UNIVERSITAET WIEN (TUV)	Austria
INTEGRASYS, S.A. (ISYS)	Spain
Skybotix AG (SBX)	Switzerland
QUOBIS NETWORKS SL (QUOBIS)	Spain
INESC PORTO - INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES DO PORTO (INESC)	Portugal
ALLEN-VANGUARD LIMITED (AV)	United Kingdom
UNIVERSITE DE NEUCHATEL (UNINE)	Switzerland
Eidgenössische Technische Hochschule Zürich (ETH)	Switzerland
ATOS SPAIN SA (ATOS)	Spain
TECHNISCHE UNIVERSITAET KAISERSLAUTERN (UKL)	Germany
NATO Undersea Research Centre (NURC)	Italy
CALZONI SRL (CAL)	Italy
METALLIANCE SA (META)	France
ESRI PORTUGAL - SISTEMAS E INFORMACAO GEOGRAFICA SA (ESRI)	Portugal
SPACETEC PARTNERS SPRL (STP)	Belgium
ESCOLA NAVAL (CINAV)	Portugal
Federale overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking (BFAST)	Belgium

INACHUS / Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localization to Support Search and Rescue Teams



Information

Grant Agreement N°
607522
Total Cost
€13,944,267.76
EU Contribution
€9,885,037.58
Starting Date
01/01/2015
Duration
48 months

Coordinator

INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)
I-SENSE Group
9, Iroon Politechniou Str.
Zografou, Athens GREECE
15773 Zografou, Athens
GREECE
Contact
Dr. Angelos Amditis
Tel: +30 210 772 2398
Fax: +30 210 772 3557
E-mail: a.amditis@iccs.gr
Website: www.iccs.gr

Project objectives

INACHUS aims to achieve a significant time reduction related to urban search and rescue (USaR) by providing wide-area situation awareness solutions for improved detection and localization of the trapped victims. This relies on simulation tools for predicting structural failures and a holistic decision support mechanism incorporating operational procedures and resources of relevant actors.

Description of the work

The INACHUS methodology is user-centric, involving end-users as much and as often as possible. First responders (FRs) and URaR teams) are regularly consulted to collect insights, needs and remarks. Based on these requirements, the project carefully designs, implements and evaluates a seamlessly integrated platform that provides the appropriate tools to enable FRs and USaR crews to respond to varied abnormal events, including those beyond a specific emergency case or crisis event. INACHUS is organized into 12 work packages (WPs), each with a set of deliverables and milestones. The WPs include consortium management and assessment of progress and results.

Expected results

INACHUS aims to achieve a significant time reduction and an increase of efficiency in USaR operations by providing:

1. Simulation tools for estimating the locations of survival spaces (after a structural collapse) and identifying the location of survivors for different construction types and building materials
2. Decision and planning modules for advanced casualty and damage estimation based on input coming from airborne and ground-based laser-scanning and imaging data
3. Integration of: i) existing and novel sensors (electromagnetic, vision, chemical) for detecting and high-accurate localization and ii) mobile phones signals for estimating the number of the trapped humans
4. A snake robot mechanism (integrated with the sensors) to penetrate inside rubble to locate more accurately trapped victims
5. A robust, resilient and interoperable communication platform to ensure that sensors data can reach the command center
6. An enhanced data analysis techniques and 3-D visualization tool of the mission site to be operated by crisis managers and decision makers. A suitable decision support system will be used for planning & managing complex USaR operations
7. System integration of all the aforementioned software and hardware subcomponents (INACHUS platform)
8. Contribution to standards: interaction with international organisations and public authorities in the fields of USaR via an early defined and developed User Group to ensure strong links with the user communities and standardisation bodies
9. Consideration of societal impacts and legal/ethical issues of the proposed solution at the onset of the project to feed into the technical solutions
10. Numerous field and simulated tests designed and

executed for presenting the capabilities of the INACHUS integrated platform

11. An appropriate training package and extensive training courses for first responders.

PARTNERS	COUNTRY
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)	Greece
EXODUS A.E. (EXODUS)	Greece
TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)	Sweden
Crisisplan B.V. (CBV)	The Netherlands
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONERA)	France
FUNDACION TEKNIKER (TEK)	Spain
FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (FHG)	Germany
CINSIDE AB (CINSIDE)	Sweden
APPLIED SCIENCE INTERNATIONAL EUROPE SRL (ASI)	Italy
DIGINEXT SARL (DXT)	France
Laurea-ammattikorkeakoulu oy (LUAS)	Finland
ENTENTE POUR LA FORÊT MÉDITERRANÉENNE (EPLFM)	France
ANKARA BUYUKSEHIR BELEDIYE BASKANLIGINA (TCABBITF)	Turkey
STIFTELSEN SINTEF (SINTEF)	Norway
UNIVERSITEIT TWENTE (ITC)	The Netherlands
SCHUSSLER-PLAN INGENIEURGESELLSCHAFT MBH (ScPl)	Germany
SODERTORNS BRANFORSVARSFORBUND (SBFF)	Sweden
TELINT RTD Consultancy Services LTD (TELINT)	United Kingdom
BYTE COMPUTER ANONYMI VIOMICHANIKIEMPORIKI ETAIREIA (BYTE)	Greece
MIKROSYSTIMATA MIKROROIS GIA GENETIKOUS ELEGKOUS KAI MORIAKI DIAGNOSTIKI EPE (M2G)	Greece

NMFRDISASTER / Identifying the Needs of Medical First Responders in Disasters

© Dmitry Pistrov – Fotolia.com

RESEARCH COMPLETED

Information

Grant Agreement N°
218057
Total Cost
€815,079.25
EU Contribution
€815,079.25
Starting Date
01/05/2008
End Date
30/06/2009

Coordinator

MAGEN DAVID ADOM
Yigal Alon 60
67062 Tel-Aviv
Israel
Contact
Chaim Rafalowski
Tel: +972 3 6300292
Fax: +972 3 7396541
E-mail: chaimr@mdais.co.il
Website:
http://www.mdais.org

Project objectives

NMFRDISASTER aimed to research and recommend new methodologies for medical first-response organisations, so as to allow them to better train and prepare for disaster response tasks. It also sought to identify appropriate medical tools.

This research focused on five key areas:

» training methodology and technology used to train medical first responders for disasters;

» understanding the human impact of disaster on medical first responders;

» ethical and legal issues influencing the medical response to disasters;

» personal protective equipment (PPE) used in chemical, biological and radiological (CBR) incidents;

» use of blood and blood products in disasters.

Results

A key finding of NMFRDISASTER was that although medical preparedness for disasters in most organisations surveyed was high, evidenced-based material for training was limited.

NMFRDISASTER thus proposes the creation of a formal, evidence-based curriculum based on successful case studies, determined evaluation criteria and a training simulation programme for both medical treatment and management issues.

In view of the fact that employment frameworks for the use of medically trained volunteers are highly irregular across Europe, the project recommends creating and adopting a basic charter in this area. Provisions of the charter would include common minimum standards and a “rights and duties” agreements that could be signed between volunteers and medical organisations.

NMFRDISASTER also found a lack of procedural preparation for the use of personal protective equipment to shield medical first-responders from chemical, biological or radiological contamination. The project thus proposes the development of standard decontamination procedures, enhanced communications regimes and more stringent safety procedures for handling CBR incidents.

The project also proposed the development of new portable blood delivery technologies, and the formal set-up of emergency blood donation schemes to overcome the rapid decline in blood stocks instigated by a large-scale medical incident.

Finally, the project considered some of the ethical, emotional, legal and media communication aspects of medical first response tasks. NMFRDISASTER concludes that a lack of public understanding of medical tasks in an emergency, combined with sensitivity towards issues such as blood donation and medical “triage” prioritisation, may place medical responders at great risk of legal liability charges and emotional trauma.

Public awareness campaigns, cultural sensitivity training and further legal research is encouraged in these areas.

PARTNERS	COUNTRY
Magen David Adom	Israel
SAMUR Protección Civil, Ayuntamiento de Madrid	Spain
AmbulanceZorg Nederland	The Netherlands
Danish Red Cross	Denmark
Sinergie S.r.l	Italy
Fundación Rioja Salud	Spain
Center for Science, Society and Citizenship	Italy
Shield Group Inc.	Aruba
Charles University	Czech Republic
Al-Quds Nutrition and Health Research Institute	Palestinian-administered areas

PEP / Public Empowerment Policies for Crisis Management

© James Brey - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284927
Total Cost
€1,065,206
EU Contribution
€950,023
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

UNIVERSITY OF JYVÄSKYLÄ
Agora Center
Seminaarinkatu 15
PO Box 35
40014 University
of Jyväskylä, Finland
Contact
Prof. Marita Vos
Tel: +358 50 4410 358
Mobile: +358 50 4410 358
Fax: +358 14 260 1021
E-mail: marita.vos@jyu.fi
Website: www.projectPEP.eu

Project objectives

The purpose was to investigate how the crisis response abilities of the public can be enhanced and identify what public empowerment policies can be utilised for this purpose. The project had the following objectives.

» To identify potential key enablers for public empowerment for crisis management, by 3 studies:

- providing an overview of best practices showing strategies and tools used by authorities to enhance individual, family and community crisis response;
- clarifying in depth how community approaches, involving social groups in crisis preparedness and response, are used, including success factors in how to connect with community needs;
- assessing how and what technologies can enhance human resilience in crisis situations taking perceptions and social acceptance of the technologies and mobile services into account.

» To construct a Road Map charting promising areas for future R&D and implementation, supporting human resilience;

» To ensure dissemination of the project results in order to raise awareness of the importance of public resilience, and how this can be achieved.

Description of the work

In work package 1 the aim was to provide *best practices* in how authorities currently enhance human resilience and what strategies and tools are used to promote individual and community crisis response. A desk study was conducted and an online questionnaire sent to international experts.

In work package 2 the focus was on *community approaches* involving social groups in crisis preparedness and response. An analysis of quantitative data and in-depth interviews was done in Sweden, focusing on remote areas where storms may cause long power cuts and isolation. Interviews with members of the International Expert Panel were also conducted to scrutinise international applicability.

In work package 3 the aim was to assess how and what *technologies* could enhance human resilience in crisis situations, taking into account technology acceptance models and inclusion requirements (diversity of publics). In Finland focus group interviews were organised to clarify what kind of communication technology citizens prefer for this purpose. The applicability of the conclusions was scrutinized in interviews with members of the International Expert Panel.

In work package 4 the focus was on constructing a *Road Map* charting directions for further research and implementation supporting human resilience. A preparation workshop was organised at the International Disaster and Risk Conference (IDRC) 2012. In addition, a web platform was used to expose the preliminary conclusions for review. During an *international symposium* within the framework of IDRC Davos 2014 the future orientation of the Road Map will be discussed.

In work package 5 the dissemination gets attention. An online toolbox will be produced with the *guides* about key enablers for public empowerment in crisis situations, concentrating on a) best practices, b) community approach and c) human technology. Furthermore, a *theme issue* of the open access journal 'Human Technology' will be prepared to disseminate the project results to crisis managers and communication experts working for public authorities and non-governmental organizations, as well as European policymakers in the security area.

Results

The project clarified best practices and showed guidelines in the form of an accessible tool, the 'Crisis communication WIKI for professionals'. Dialogue about the research results was initiated via the International Disaster and Risk Conferences in Davos. An open call of the reference journal, Human Technology, led to the publication of a special issue on 'Community resilience in crises: Technology and social media enablers'.

PEP also focused on policy recommendations. The report 'Roadmap public empowerment policies for crisis management' advocates clear directions for further action of public empowerment policies for crisis management in the areas of practice, policymaking, and research. Without structural inclusion of the public in resilience enhancing activities, the increased expectations of citizens of two-way communication will not be met.

The website www.projectPEP.eu offers the 'Crisis communication WIKI for Professionals', research outcomes and the 'Roadmap public empowerment policies for crisis management'.

PARTNERS	COUNTRY
University of Jyväskylä (JyU)	Finland
Mid Sweden University (MIUN)	Sweden
Global Risk Forum (GRF)	Switzerland
Inconnect (Inconnect)	Netherlands
Emergency Services College Finland (ESC)	Finland

SGL FOR USAR / Second generation locator for urban search and rescue operations

© puck - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217967
Total Cost
€6,218,278
EU Contribution
€4,859,026
Starting Date
01/10/2008
End Date
31/10/2012

Coordinator

NATIONAL TECHNICAL UNIVERSITY OF ATHENS
Heroon Polytechneiou
15780 Zographou
Greece
Contact
Milt Statheropoulos
Tel.: + 30 210 7723109
Fax: + 30 210 7723188
E-mail:
stathero@chemeng.ntua.gr
Website: www.sgl-eu.org

Project objectives

SGL for USaR is mission oriented towards solving critical problems following large scale structural collapses in urban locations. The devotion, courage and expertise of rescuers need to be matched by procedures and technology that will enable safe and effective responses.

This project will combine chemical and physical sensors integration with the development of an open ICT platform for addressing mobility and time-critical requirements of USaR Operations. The project will also focus on medical issues and on the relevant ethical dilemmas.

Description of the work

» To use video images (image analysis), sound (sound signatures), field chemical analysis (marker compounds), optical sensors (spectral analysis), data fusion and wireless communication in order to develop integrated, stand-alone early location devices for entrapped people and dead bodies, and to employ the same kind of devices for monitoring and identifying hazardous conditions in voids of collapsed buildings due to the construction's physical damage, flaming or smoldering fires and gases released;.

» To develop integrated remote early location and monitoring systems for localization purposes based on the deployment of networks of probes. Such systems will also be capable of receiving other types of data (e.g. sonar);

» To integrate early location and monitoring systems with communication and information management applications that can provide multi-level processing and data fusion and will support relevant USaR services and logistics (medical support, mobilization, tools, transportations, communications). The SGL for USaR project will use multidisciplinary approaches, optimize existing cutting-edge technologies and make the best use of available resources.

The project is targeted at delivering next generation systems for USaR operations.

For that purpose, relevant technical, scientific and operational issues will be addressed.

The project focuses on rapid location of entrapped or buried victims (alive or deceased) and the continuous monitoring of the air conditions in the voids of damaged and partially collapsed structures. Entrapped people and voids are associated with characteristic visual, sound and chemical profiles, due to specific images or spectral emissions, and to acoustic signatures and chemical markers.

The adaptation of crisis management USaR services (logistics) with the early location and monitoring systems in a mobile command and control operational center is employed.

The project is formed by eight sub-projects (work packages) running in parallel. These WPs address: the development of simulation environments; the development and validation of portable devices for location operations; the development and validation of a smart sensors environment for monitoring the situation under the ruins; the management of medical information, including privacy and bioethics; and finally the development of an ICT platform that will integrate all the previous data, ensure interoperability and control the flow of the information from the field to the operational center.

Results

The project developed two tangible product prototypes: FIRST and REDS.

FIRST is a portable rescue device to monitor hazardous conditions or locate entrapped victims/dead bodies within collapsed buildings. It can be used for:

- » locating trapped victims
- » detecting unconscious victims using human scent
- » surveillance and monitoring of confined spaces
- » environmental monitoring of hazardous conditions

The second prototype, REDS, is a network of remotely controlled sensors that can be installed in a collapsed building for unattended monitoring and to detect life signs or hazardous conditions. It consists of eleven nodes: four fixed anchors and seven mobile probes. The latter comprise a gas sensor system, video camera, audio sensor, vibration sensor, medical locator, telemedicine probe and) field portable GC/IMS instruments. REDS was designed to:

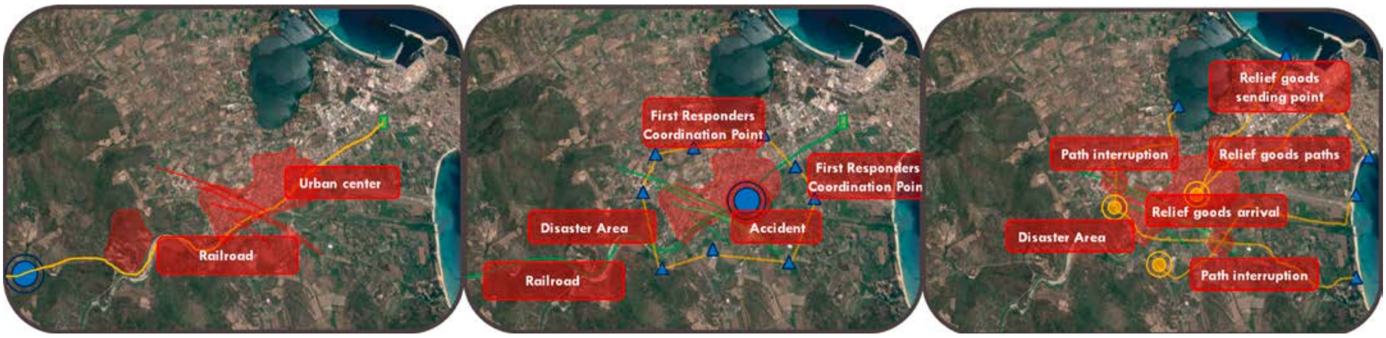
- » monitor confined spaces
- » check for life signs or hazardous conditions
- » remotely monitor a victim's vital signs
- » monitoring safety conditions during search and rescue
- » augment the capabilities of rescue teams

The project also developed a centralized command-and-control system to integrate the two prototypes and an environmental test chamber to simulate collapsed buildings, an alarm module and a digital library to identify image and sound signatures.

Finally, SGL for USAR investigated bioethics in rescue operations and created an online technology forum for discussion and collaboration between interested parties.

PARTNERS	COUNTRY
National Technical University of Athens	Greece
Service Départemental d'Incendie et de Secours du Vaucluse	France
Direccio General De Prevencio I Extincio D'incendis I Salvaments	Spain
FAENZI s.r.l.	Italy
Valtion Teknillinen Tutkimuskeskus	Finland
Gesellschaft zur Förderung der Analytischen Wissenschaften e.V.	Germany
ECOMED bvba	Belgium
Environics Oy	Finland
Austrian Academy of Sciences	Austria
Entente Interdépartementale en vue de la Protection de l'Environnement et de la Foret contre l'Incendie	France
ANCO S.A. Agencies, Commerce & Industry	Greece
University of Dortmund	Germany
TEMAI Ingenieros S.L.	Spain
G.A.S. Gesellschaft für analytische Sensorsysteme mbH	Germany
Universidad Politecnica de Madrid	Spain
Savox Communications Ltd	Finland
University of Athens	Greece
Markes International ltd	United Kingdom
Bay Zoltan Foundation for Applied Research	Hungary
Critical Links SA	Portugal
The University of Loughborough	United Kingdom

SPARTACUS / Satellite Based Asset Tracking for Supporting Emergency Management in Crisis Operations



Information

Grant Agreement N°
313002
Total Cost
€4,497,612
EU Contribution
€3,175,396
Starting Date
01/11/2013
Duration
36 months

Coordinator

D'APPOLONIA S.P.A. (DAPP)
Innovation Consulting Division
Via San Nazaro 19
16145, Genova, ITALY
Contact
Clemente Fuggini
Tel: +39 02 51800562
Mobile: +39 3332090873
Fax: +39 02 51800563
E-mail: clemente.fuggini@dappolonia.it
Website: www.dappolonia.it

Project objectives

Motivated by the opportunity to develop industrial "pull" applications and services for the European EGNOS and GALILEO satellite systems, SPARTACUS will design, develop, test and validate in simulated and real world scenarios GALILEO-ready tracking/positioning solutions for critical asset tracking and crisis management. At a general level, SPARTACUS will implement solutions for location awareness for crisis management based on existing (GPS, EGNOS, EDAS) and incoming (GALILEO) satellite services and technologies. This will provide precise tracking/positioning by ensuring no gaps in communication or coordination information. This will be done in three application areas, namely to:

» track, trace, and localise critical transport assets especially in times of crisis and in case of major failure of existing networks;

» track the flow of relief support goods from the sending side to the receiving/end place;

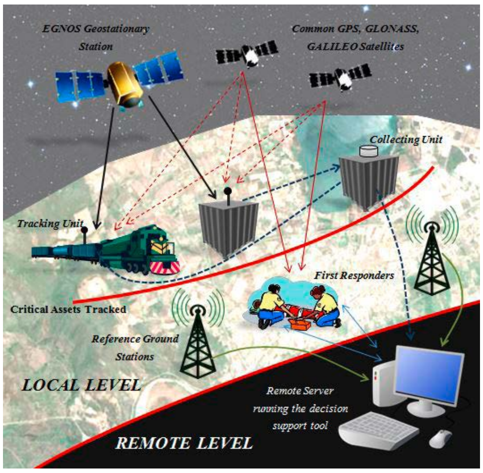
» support and ensure the safety of first responders in crisis management operations.

SPARTACUS end-users are rail and infrastructure managers, companies involved in logistic operations during crisis context, and first responders involved in emergency coordination and management.

Description of the work

The project's methodology will progress through identification, development, implementation and exploitation. Based on identification of end-user requirements, the functional and technical specifications of components and those at system level will be defined, followed by development of positioning, timing and communication technologies. The components will be integrated to achieve the system's full functionalities for demonstration in test beds, trials and practical exercises. Exploitation of the project results as well as training activities constitute the final actions SPARTACUS will carry out to ensure the solutions' deployment and to raise end-users' awareness and market acceptance.

SPARTACUS will work toward innovative hardware and software. This will include hardware adaptations, algorithms to improve the accuracy in tracking assets and persons, integration of the receivers with inertial platforms to provide dead-reckoning functionalities, and the availability of communication networks during emergencies via satellite backhauling.


EGNOS Geostationary Station
Common GPS, GLONASS, GALILEO Satellites
Collecting Unit
Tracking Unit
First Responders
Critical Assets Tracked
Reference Ground Stations
LOCAL LEVEL
Remote Server running the decision support tool
REMOTE LEVEL

Expected results

The main expected results are:

- a GNSS-based unit for tracking critical assets and tracing first responders in disaster areas;
- a communication networks that integrates terrestrial (4G-LTE) and satellite communications which will be made available during emergencies to provide a local communication network for first responders operating in disaster areas;
- a set of decision support tools to be used for fleet management regarding the tracking of critical assets and for coordination in the case of first-responder operations;
- a set of smartphone applications to improve location awareness and decision support as fed with operationally relevant information;
- a fully integrated platform for critical assets tracking and coordination of first responders.

PARTNERS	COUNTRY
D’Appolonia S.p.A. (DAPP)	Italy
University of Pavia (UNIPV)	Italy
University of Bologna (UNIBO)	Italy
Newcastle University (UNEW)	United Kingdom
Romanian Railway Authority (AFER)	Romania
Institut Mihajlo Pupin (IMP)	Serbia
Disaster Management Advice and Training (DMAT)	Austria
AnsuR Technologies (ANSUR)	Norway
TriaGnoSys GmbH (TGS)	Germany
GlobalGPS (GLOB)	Bosnia
Akkon University (AKKON)	Germany

S(P)EEDKITS / Rapid deployable kits as seeds for self-recovery

© s(p)eedkits

Information

Grant Agreement N°
284931
Total Cost
€9,021,302
EU Contribution
€6,117,066
Starting Date
01/03/2012
Duration
48 months

Coordinator

CENTRE SCIENTIFIQUE & TECHNIQUE DE L'INDUSTRIE TEXTILE BELGE
Technologiepark 7
BE-9052 Zwijnaarde,
Belgium
Contact
Guy Buyle
Tel: +32 9 220 41 51
Mobile: +32 492 73 76 19
Fax: +32 9 220 49 55
E-mail: gbu@centexbel.be
Website: www.speedkits.eu

Project objectives

The main objective of S(P)EEDKITS is to develop kits for emergency response units, i.e. *SPEED*KITS. Following best practice guidelines from humanitarian organisations, these solutions will also be *SEED*KITS, i.e. kits that form the seeds for the long term self-recovery process after a disaster strikes.

Humanitarian organisations like the Red Cross or MsF have sleeping emergency response units which start acting immediately after disaster strikes. Each unit has a specific function, e.g. medical care, sanitation, energy provision, or water supply.

S(P)EEDKITS targets a smart (re-)design of existing / novel kits via smart packaging and via introduction of the latest technological developments from a wide range of domains like coated textile materials, ICT, material development, tensile structures and construction.

Some examples: lightweight, durable and thermally isolating tent materials, novel concepts for energy supply (biogas from sanitation), smart packaging (matryoshka doll principle), kits for debris recuperation, and rapidly deployable container solutions for a mobile hospital or command centre.

Description of the work

S(P)EEDKITS will design, develop, test and demonstrate units for emergency response in the following four domains:

Shelters:

Design and development of novel shelter kits for four different basic shelters:

» *ultra lightweight safe house unit*, a short term solution for the very first hours, to be deployed by the affected communities;

» *collective unit*, an emergency shelter which could be removed or re-used for other purposes later;

» *family house unit*, the first version of a real house, to be used in the transitional period and later;

» *multipurpose unit* for the humanitarian organizations, to be used for storage, offices and medical centres.

Water and Sanitation:

Research, development and testing of prototypes of flexible sanitation systems and low tech, low cost, small scale potable water kits, based on the use of "add-ons" for tuning to local needs and future application.

Sustainable infrastructure:

Develop container-based command, communication and medical centre units, based on existing prototypes. The units can be reused or handed over to the local medical authorities.

Design and testing of a biogas system for energy for ca.200 people based on faeces and household kitchen waste collection.

Development of mobile debris recycling kit for producing easily usable building materials from the existing debris.

Deployment and Tracking:

Development of a deployment decision tool (DDT) to determine immediately which kits and support have to be deployed. As well as the development of a tracking system, tagging the individual transported packages – suitable for central operational planning & for local assessment of the situation.

For the different kits, the goal is to (re-)design existing and novel emergency response kits using the Matryoshka doll principle; this nesting principle will inspire the packaging optimization of smaller robust packages in large ones, allowing splitting up according to the transportation means available.

Three different levels of packaging are anticipated within S(P)EEDKITS: container-level, pallet-level and bag-level based as much as possible on the use of flexible textile materials.

We aim mostly at the bag-level, i.e. solutions for where more conventional transport means fail.

Expected results

The expected outcomes are novel emergency kits that are modular and adaptable, low-cost, and high-tech in their conceptions yet low-tech in their use. The planned kits have the potential to improve the lives of millions of people during the first hours, days and weeks after a major disaster.

PARTNERS	COUNTRY
CENTRE SCIENTIFIQUE & TECHNIQUE DE L'INDUSTRIE TEXTILE BELGE (CTB)	Belgium
AIDE INTERNATIONALE DE LA CROIX-ROUGE LUXEMBOURGEOISE ASBL (SRU)	Luxembourg
HET NEDERLANDSE RODE KRUIS (NLRC)	The Netherlands
SIOEN INDUSTRIES NV (SIOEN)	Belgium
VRIJE UNIVERSITEIT BRUSSEL (VUB)	Belgium
TECHNISCHE UNIVERSITEIT EINDHOVEN (TU/e)	The Netherlands
POLITECNICO DI MILANO (POLIMI)	Italy
De Mobiele Fabriek B.V (DMF)	The Netherlands
STICHTING WASTE (WASTE)	The Netherlands
STICHTING PRACTICA (PRACTICA)	The Netherlands
D'APPOLONIA SPA (DAPP)	Italy
IBBK FACHGRUPPE BIOGAS GMBH (IBBK)	Germany
MILLSON BV (MIL)	The Netherlands
ARTSEN ZONDER GRENZEN (MEDECINS SANS FRONTIERES NEDERLAND) VERENIGING (MSF)	The Netherlands
STIFTELSEN FLYKTNINGERADET (NRC)	Norway

BEAT / Biometrics Evaluation and Testing

© yewkeo - iStockphoto

Information

Grant Agreement N°
284989
Total Cost
€4,738,788.40
EU Contribution
€3,499,784
Starting Date
01/03/2012
Duration
48 months

Coordinator

IDIAP RESEARCH INSTITUTE
RUE MARCONI 19
592
1920 Martigny, Switzerland
Contact
Sebastien Marcel
Tel: +41 27 721 7727
Fax: +41 27 721 7712
E-mail: marcel@idiap.ch
Website:
https://www.beat-eu.org

Project objectives

The goal of BEAT is to propose a framework of standard operational evaluations for biometric technologies.

The BEAT project will provide standardized criteria (and metrics) to evaluate biometric systems for both academic and commercial entities. This standardization is currently lacking and would likely lead to: an improved communication between academic and commercial entities in the field of biometrics by providing a common basis for comparison, and an improvement in the state-of-the-art for biometric systems by providing a fair and centralized method to evaluate systems.

The standardization would include methods to evaluate: 1) the performance (accuracy) of a biometric system, 2) the vulnerability of a biometric system to direct attacks (spoofing) or indirect attacks (hill-climbing attacks), and 3) the performance of privacy preservation techniques.

Description of the work

Identity management using Biometrics is a reality because of the e-passport (Biometric passport). Similar biometric technology has also become more prevalent on personal computers with more biometric-enabled functions, and soon applications to recognize nomadic users through biometrics will also emerge as mobile devices are equipped with more sensors. Unfortunately the reliability of these biometric technologies is not always known and therefore can not be guaranteed. In particular the three criteria of (1) the performance of the underlying biometric system, (2) the robustness regarding vulnerabilities such as direct (spoofing) or indirect attacks, and (3) the strength of privacy preservation techniques, are often unknown or impossible to compare to competitors.

The lack of standard operational evaluations is the reason that we cannot measure the reliability of these biometric technologies. Some initiatives exist in Europe, the United States of America, and Asia. However, these initiatives are: isolated (focusing only on one or two biometric modalities), disorganized (teams from the same institution can work on different biometrics without talking to each other), or limited in time (very few are organizing ongoing evaluations). This leads to discontinuous and non-integrated efforts which have a limited life span. Thus the BEAT project will establish a framework to evaluate, in a systematic way, the performance of biometric technologies using several metrics and criteria (performance, vulnerability, privacy).

The goal of BEAT will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations.

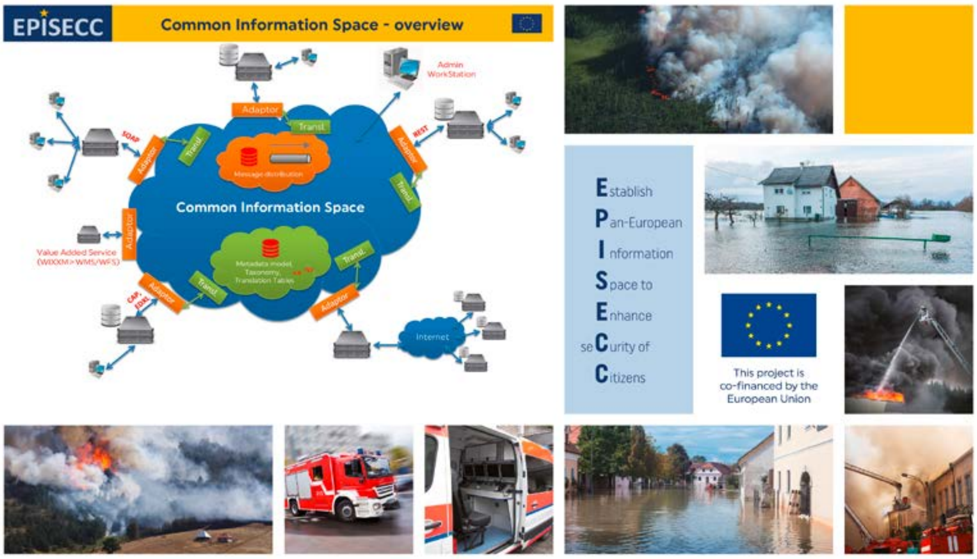
Additionally, legal aspects will be considered to address the issues of both privacy data protection and Intellectual Property and so ensure that the BEAT framework can be used by the research community and companies.

Expected results

There will be three outcomes of this project. The first is that the reliability of biometric systems will be measurable and thus should lead to a meaningful increase in performance. The second is that technology transfer from research to companies will be much easier as there will be an interoperable framework. Finally, decision-makers and authorities will be informed about the progress that is made in biometrics as the results will have an impact on standards. Given these outcomes we expect that BEAT will significantly contribute to the development of a European Identification Certification System.

PARTNERS	COUNTRY
Idiap Research Institute (IDIAP)	Switzerland
Universidad Autonoma de Madrid (UAM)	Spain
University of Surrey - CVSSP (UNIS)	United Kingdom
Ecole Polytechnique Federale de Lausanne - LASEC (EPFL)	Switzerland
TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU (TUBITAK)	Turkey
Commissariat à l'énergie atomique et aux énergies alternatives - LETI (CEA)	France
Morpho (MPH)	France
TÜViT (TUVIT)	Germany
Katholieke Universiteit Leuven (KULeuven)	Belgium

EPISECC / Establish Pan-European Information Space to Enhance seCurity of Citziens



Information

Grant Agreement N°
607078
Total Cost
€5,133,543.80
EU Contribution
€3,764,547.26
Starting Date
01/06/2014
Duration
36 months

Coordinator

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)
DIGITAL SAFETY
& SECURITY
Donau-City-Strasse 1
Tech Gate Vienna Donau-City-Strasse 1
1220 – Vienna – Austria
Contact
GEORG NEUBAUER
Tel: +43 (0) 50 550 2807
Mobile:
+43 (0) 664 620 77 52
Fax: +43505502813
E-mail:
Georg.Neubauer@ait.ac.at
Website: www.episecc.eu

Project objectives

The project EPISECC aims to define a concept for a common “European Information Space”. This space intends to become the key element in a future integrated pan-European crisis and disaster response capacity. Besides developing a common taxonomy and ontology model to address semantic interoperability issues, EPISECC will also focus on Iinteroperability at the physical (i.e. network) and syntactical (i.e. automated information exchange) levels. Indeed, one of the project’s main purposes is to allow analysis of interoperability at all levels.

EPISECC has the following objectives:

» Develop a pan-European historical inventory of critical events/disasters and their consequences with a focus on the performance of processes, data exchange and organizational boundaries;

» Develop a concept for a common information space that included appropriate semantic definitions by taxonomies and/or ontologies;

» Analysis of existing concepts of interoperability across different domains as the basis for common information space concept, and the identification of new emergency and crisis management models;

» Validation of the architecture and the elaboration of new emergency and crisis management models.

Description of the work

EPISECC’s work is structured in nine workpackages (WPs), which address the following:

» WP1 – Coordination and Management

» WP2 – Analysis of past crisis management approaches

» WP3 – Pan European Inventory of events/disasters

» WP4 – Taxonomy building

» WP5 – Architecture of Common Information space

» WP6 – Proof of Concept & Validation

» WP7 – Legal & Ethic aspects

» WP8 – Dissemination

» WP9 – Exploitation & Standardisation

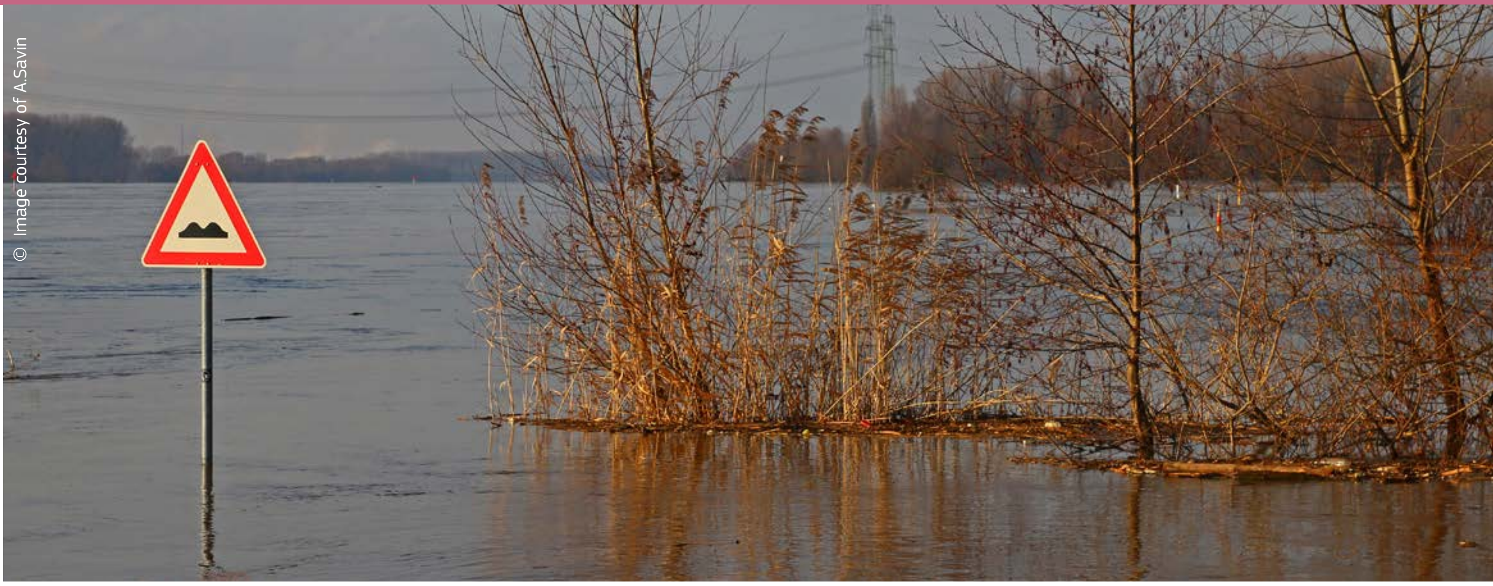
Expected results

EPISECC aims to:

- support the implementation of the European Commission's 2010 guidelines with the concept of the common information space
- strengthen and improve the effectiveness and adequacy of emergency and disaster response in Europe and beyond
- auxiliary benefit in various areas such as ICT technology, quality of information, field level co-ordination, preparedness, safety and security of citizens, security forces, etc.

PARTNERS	COUNTRY
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Airbus Defence and Space OY. (ADS OY)	Finland
Airbus DS SAS (ADS SAS)	France
University of Split (UNIST)	Croatia
Public Safety Communication Europe Forum AISBL (PSCE)	Belgium
HITEC Luxembourg S.A. (HITEC)	Luxembourg
Frequentis AG (FRQ)	Austria
Deutsches Zentrum für Luft- und Raumfahrt EV (DLR)	Germany
HW Communications Limited (HWC)	United Kingdom
TETRA MoU Association Ltd (TCCA)	United Kingdom
Katholieke Universiteit Leuven (KU Leuven)	Belgium
Intelligence for Environment and Security SRL (IES)	Italy
Technische Universität Graz (TUG)	Austria

FORTRESS / Foresight Tools for Responding to cascading effects in a crisis



© Image courtesy of A.Savin

Information

Grant Agreement N°
607579
Total Cost
€4,716,286.60
EU Contribution
€3,400,665.70
Starting Date
01/04/2014
Duration
36 months

Coordinator

TECHNISCHE UNIVERSITÄT BERLIN (TUB)
Center for Technology and Society
Hardenbergstrasse 16-18
10623 – Berlin – Germany
Contact
Dr. Leon Hempel
Tel: +49-30-314 25373
Mobile:
+49-0176 111 20400
Fax: +49-30-314 26917
E-mail:
hempel@ztg.tu-berlin.de
Website: fortress-project.eu

Project objectives

Given the increasing interdependencies between different infrastructural sectors and countries, FORTRESS aims to improve crisis management practices by identifying the diversity of cascading effects that flow from the interrelations of systems. Here, crisis management refers to a process of actions, decisions, and communications that are launched and implemented when an organisation has to cope with a major event with its consequences. Given the diversity of such organisations involved, a common understanding of the current situation, unfolding events, structures and processes is essential in order to achieve coordinated action and to avoid misunderstandings during crises.

The empirical results will be consolidated to create the FORTRESS Incident Evolution Tool (FIET). Thiswill help forecast potential cascading effects. The tool integrates system and spatial data as well as sociological, human decision-making data.

Description of the work

FORTRESS is divided into three phases.

Phase 1 of the project will begin with a knowledge review around crisis situations. This includes the current understanding of cascading and cross-border effects of vulnerability and resilience as well as existing tools for crisis management.

In phase 2, an empirical database for the FIET will be developed. FORTRESS will combine case studies of historical crisis (from both Europe and International cases) with real-time scenario case studies of crisis management. The real-time scenario case studies consist of four crisis exercises.

1. A dam disruption in the border region of France and Italy
2. multiple infrastructure breakdowns due to a pan-European blackout in Berlin
3. cross-border flooding scenario in the Netherlands
4. a massive flooding in the Paris area with international impacts

Finally, in phase 3, a scenario builder tool for cascading and cross-border effects and further elements of the FIET will be developed.

Expected results

FORTRESS will develop a collaborative and accessible modelling platform for cascading and cross-border effects as well as a demonstrator of the FORTRESS Incident Evolution Tool (FIET) that can be used as a foresight tool to assist decision-makers in understanding the potential effects of their decisions in training environments.

PARTNERS	COUNTRY
Technische Universität Berlin (TUB)	Germany
Trilateral Research & Consulting LLP (TRI)	United Kingdom
Treelogic, Telemática y Lógica Racional para la Empresa Europea S.L. (TREE)	Spain
Electricité de France S.A. (EDF)	France
Dialogik gemeinnützige Gesellschaft für Kommunikations- und Kooperationsforschung mbH (DIA)	Germany
IRKS Research GmbH (IRKS)	Austria
Ritchey Consulting AB (RCAB)	Sweden
University College London (UCL)	United Kingdom
Istituto Superiore sui Sistemi Territoriali per l'Innovazione (SITI)	Italy
GMV Sistemas S.A.U. (GMV)	Spain
Veiligheidsregio Kennemerland (VRK)	The Netherlands
Service Départemental d'Incendie et de Secours des Alpes de Haute-Provence (SDIS 04)	France
Berliner Wasserbetriebe (BWB)	Germany

REDIRNET / Emergency Responder Data Interoperability Network

Information

Grant Agreement N°
607768
Total Cost
€4,327,171.80
EU Contribution
€3,498,968.00
Starting Date
01/03/2014
Duration
30 months

Coordinator

ARDACO, A.S.
EU department
Polianky 5
841 01 – Bratislava –
Slovakia
Contact
Peter Dohanyos
Tel: +421 (2) 3221 2311
E-mail: peter.dohanyos@ardaco.com
Website: www.redirnet.eu

Project objectives

Over the recent years the majority of the REDIRNET consortia have participated in Projects SECRICOM and FREESIC, involving partners engaging significantly with a wide range of public safety officers across the EU. A benefit of this engagement has been the recognition that in addition to agency interoperability of communications a pressing need exists for agency interoperability of additional IT systems such as databases, sensor systems and cameras.

REDIRNET provides a framework for addressing this need with detailed mapping of user preferences and related legal requirements using innovative technologies. The consortium is aware that frequently it is non-technical issues that hinder agency interoperability, regardless of the quality of technical solutions. Consequently, user engagement across a range of agencies EU-wide will be ongoing throughout the duration of REDIRNET.

Description of the work

In recent years, first responder organizations across Europe have considerably improved their communications and IT systems with the deployment of new technologies. These include such innovations as unmanned surveillance and sensor systems that assist preventative actions and enhance responses to major crisis events.

Nevertheless, a number of recent major incidents have highlighted the challenges first responders face, most notably concerning interoperability barriers. These challenges are all the more difficult against the current economic and financial situation, where agencies are under considerable budgetary pressures and cannot invest significant sums of money to enhance their interoperability. Even if inter-agency cooperation is not required on a frequent basis, enhancing agency interoperability has to be done through cost-effective solutions.

The project's work is divided into 7 work packages:

» WP 1 – Project management;

» WP 2 – Issues and Requirements;

» WP 3 – Definition of pan-European interoperability framework;

» WP 4 – Implementation of interoperability platform;

» WP 5 – Integration of end users systems;

» WP 6 – Acceptance and scenario testing by users;

» WP 7 – Dissemination and exploitation.

The REDIRNET interoperability platform will be built as an extension of the FREESIC platform which aimed to resolve interoperability issues between first responder communication systems in the same manner. REDIRNET will inherit the security features of the FREESIC platform (i.e., ability to interconnect systems with certain levels of classification) and develop new features and modules enabling the interoperability of access to data fields and streams.

Furthermore the previous collection of interoperability issues undertaken by FREESIC will be used as the baseline of inventory of issues that will be added during the REDIRNET project.

Expected results

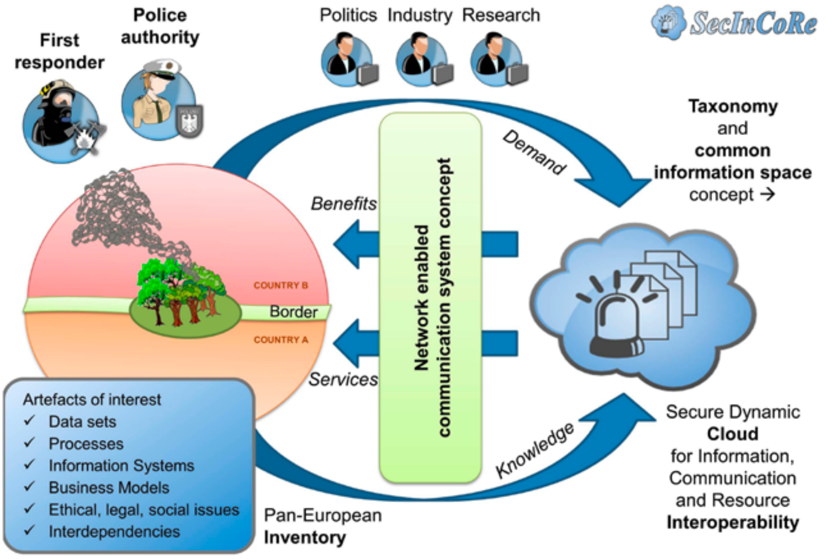
REDIRNET introduces an interoperability system that provides seamless interoperability for participating agencies at a minor investment, but with great flexibility (in term of settings which data are visible for which partner agency) via a REDIRNET socio-professional web.

Agencies will be able link up to partner agencies of their choice and operational need, while being able at the same time to manage the scope of such interoperability.

To help set up these link-up arrangements REDIRNET will be enhanced with semantic web methods by relying on the vocabulary and processes of the user community. Inter-operating agencies will need only to develop one gateway (to REDIRNET) leading to a cost effective solution; agency technologies will also be developed to facilitate the integration of user systems into REDIRNET. A content management system is software will allow the easy creation and management of webpages by separating the creation of content from the mechanics required to present it on the web.

PARTNERS	COUNTRY
Ardaco, a.s. (ADO)	Slovak republic
Britisch Association of Public-Safety Communications Officials (BAPCO)	United Kingdom
Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)	Belgium
Institut Jožef Stefan (JSI)	Slovenia
Nextel S.A. (NEXTEL)	Spain
Pramacom Prague spol. s r.o. (PMC)	Czech Republic
Ústav Informatiky, Slovenská akadémia vied (UISAV)	Slovak Republic
Université du Luxembourg (UL)	Luxembourg
Verde, s.r.o. (VERDE)	Slovak Republic

SECINCORE / Secure Dynamic Cloud for Information, Communication and Resource Interoperability based on Pan-European Disaster Inventory



Information

Grant Agreement N°
607832
Total Cost
€4,275,105.70
EU Contribution
€3,124,666.11
Starting Date
01/05/2014
Duration
36 months

Coordinator

UNIVERSITAET PADERBORN (UPB)
Computer Application and Integration in Design and Planning (C.I.K.)
Pohlweg 47-49
33098 Paderborn, Germany
Contact
Dr.-Ing. Jens Pottebaum
Tel: +49 5251 60-2234
Mobile: +49 174 3426932
Fax: +49 5251 60-3206
E-mail:
pottebaum@cik.upb.de
Website: www.secincore.eu

Project objectives

SecInCoRe will design a Secure Dynamic Cloud based concept for Information, Communication and Resource Interoperability in multi-agency crisis management, including information exchange and access to a 'Common Information Space'. This will be based on a pan-European disaster inventory collating information about stakeholders, processes, information systems, business models, resources and data sets used in regional, national as well as cross European emergencies and disasters. SecInCoRe develops concepts for sustainable access to the inventory for different users, taking into account models from open access to commercial service provision. The Common Information Space concept will be provided in an accessible form to be implemented and operated by European institutions, first responders and Police authorities, from European Member States, for collaborative work along the emergency management cycle.

Description of the work

SecInCoRe research is structured to four major scientific and technological lines of activity:

» The domain analysis, collaborative design and research on ethical, legal and social issues (ELSI) are dedicated to an even deeper understanding of the domain of first responders and Police authorities. SecInCoRe draws specific attention to the analysis of ELSI and the evaluation of possible implications of SecInCoRe concepts. This is based on an analysis of historical data from past disaster events.

» The Pan-European inventory of data sets, information systems and business models builds upon representative past incidents and performs empirical research on data used by practitioners, command structures and information management processes, available and used information systems as well as business models for services and systems.

» The design of a Secure Dynamic Cloud for Information Communication and Resource Interoperability targets the transfer of results into a solution oriented design of a 'common information space' concept complementing user centred and demand oriented research. Research brings together various existing approaches and complements them by a secure cloud and communication infrastructure.

» The integration, validation and evaluation envisages the implementation of the 'common information space' concept, the application to use cases for the inventory, the validation towards requirements and the evaluation towards the expected impact including community building activities.

Based on these activities, SecInCoRe intends to foster collaboration and interaction with other projects.

Expected results

SecInCoRe follows its objectives as a cross-cutting activity to provide results to various stakeholder including practitioners, researchers, policy makers and the European industry. The envisaged results subsume the

» creation of a pan-European inventory of past critical events and disasters as well as their consequences, data sets, process models, information system categories and business models

- design of a taxonomy of all aforementioned parts of the inventory leading to a semantic model to be applied in the 'common information space'
- design of a secure, dynamic cloud based knowledge base and communication system concept including the ability to use emergency information by means of a trans-European communication infrastructure
- conceptual integration of available technology from the field of information and communication technology into patterns of infrastructure found in first responder organisations
- validation and evaluation of all results in representative fields of application and identification of utilization approaches including standardization

PARTNERS	COUNTRY
Universitaet Paderborn (UPB)	Germany
Technische Universitaet Dortmund (TUDO)	Germany
Lancaster University (ULANC)	United Kingdom
T6 Ecosystems SRL (T6 ECO)	Italy
Airbus Defence & Space (ADS)	France
CloudSigma AG (CS)	Switzerland
BAPCO LBG (BAPCO)	United Kingdom
Center for Security Studies (KEMEA)	Greece

SECTOR / Secure common information space for the interoperability of first responders

Information

Grant Agreement N°
607821
Total Cost
€4,411,169.2
EU Contribution
€3,156,201.75
Starting Date
01/07/2014
Duration
36 months

Coordinator

E-GEOS S.P.A
Product Management and Innovation
965, via Tiburtina
00156 Roma, Italy
Contact
Maria Michela Corvino
Tel: +39 06 4079 6363
Mobile: +39 320 89 23 055
Fax: +39 06 4009 9035
E-mail:
michela.corvino@e-geos.it
Website: www.fp7-sector.eu

Project objectives

The management of crisis is one of the great challenges of the 21st century. The ever growing human, economic and environmental losses due to disasters are evidence for the need of a systematic approach to the management of crisis. Collaborative Crisis Management is usually coordinated by local authorities or civil protection organizations, supported by a variety of different national and international crisis management organizations, all acting relatively autonomously. The process is typically managed by each individual organization, supported by a range of non interoperable information management tools, depending on the level of informatisation of the local or national crisis management systems.

The projects main goals are to comprise a flexible and interoperable Collaborative Information System (CIS) for accessing integrated and up to date information and to support Crisis Collaborative Management Processing by helping different first responders organizations and police authorities to share information and resources. The challenge is to overcome the fragmentation needs in European Security Community, expressing different levels of data and system requirements as well as operational procedures and legal frameworks.

The Project is aimed at developing cooperation with other European initiatives and to build up the Common Information Systems concept and prototype starting from existing tools and learning from past crisis management experience, in order to avoid duplication of funds, and to foster standardization activities and guarantee sustainability to the proposed technological solution.

Description of the work

SECTOR project is organised in 4 phases:

Phase 1: Inventory and analyses of European CCM processes, systems and data;

Phase 2: Scenario Definition and Common information Space Concept Design;

Phase 3 (iterative) CIS development;

Phase 4: Demonstration and Validation.

The first project year focused on determining a set of analysis for the identification of diversification variances and commonalities in processes, terminology, identify data and information systems and their integration within crisis management processes. Furthermore, an iterative methodology for the collection and analysis of User requirements was performed, and the scenario on which the CIS prototype will be demonstrated was determined.

Expected results

The project will target three main innovations

1. A Collaborative Information System (CIS) concept will be designed to support crisis resolution in multiagency CCM process

2. Information sharing for joint situation awareness and cross-agency resource sharing will be enabled by a specifically developed taxonomy and by including the possibility for interfacing with Information Systems (IS) from different crisis management agencies and for sharing data by means of an Event Based Service Oriented Architecture (SOA) using a SaaS (Software as a Service) cloud computing model as a deployment architecture;

3. High level CCM Meta-Model and Collaborative Crisis Management Processes (CPs) will be defined as a basis for the SECTOR CIS concept, and hence joint cross-agency and cross-border orchestration of these processes, including the possibilities for joint resource planning and the use of joint "same purpose services (e.g. Satellite images.) offering support for managing new business models e.g. through optimizing outsourcing;

PARTNERS	COUNTRY
UNIVERSITAT POLITECNICA DE VALENCIA	Spain
ASELSAN Elektronik Sanayi ve Ticaret A.S.	Turkey
TOTALFORSVARETS FORSKNINGSINSTITUT	FOI
ITTI SP ZOO	Poland
CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA	Italy
SAADIAN TECHNOLOGIES LIMITED	Ireland
SELEX ES S.p.A	Italy
UNIVERSITAET STUTTGART	Germany
THALES SA	France
Police Service of Northern Ireland	Poland
WYZSZA SZKOLA POLICJI W SZCZYTNIE	Poland
HEALTH SERVICE EXECUTIVE HSE	Irish
Szkola Glowna Sluzby Pozarniczej	Poland
STICHTING STUDIO VEILIGHEID	The Netherlands
EBERHARD KARLS UNIVERSITAET TUEBINGEN	Germany

SIIP / Speaker Identification Integrated Project

Information

Grant Agreement N°
607784
Total Cost
€15,126,658.60
EU Contribution
€10,529,211.00
Starting Date
01/05/2014
Duration
48 months

Coordinator

VERINT SYSTEMS LTD. (VRNT)
Management
33 Maskit Street
4673333 – Herzliya - Israel
Contact
Gideon Hazzani
Tel: +972 9 962 2596
Mobile: +972 54 778 2596
E-mail:
gideon.hazzani@verint.com
Website: www.verint.com

Project objectives

SIIP's objective is to enable LEAs to overcome two main challenges they face today:

1. The "evasion" problem – i.e., the use of hidden, fake and arbitrary identities by terrorists and other criminals across telecommunications and internet media to avoid their lawful interception, identification and tracking by LEAs. Such techniques include, amongst others, the use of arbitrary nicknames in various Internet VoIP applications (e.g. Skype, Viber), the use of facemasks in social media (e.g. YouTube) and the frequent altering of SIM cards in cell phones.

2. The second challenge is the difficulty of identifying unknown participants during a lawfully intercepted call of a known speaker.

Description of the work

SSIIP will develop a break-through suspect identification solution based on a novel speaker identification (SID) engine and a global info-sharing mechanism (GISM) to identify unknown speakers captured in lawfully intercepted calls, during recorded crimes or terrorist arenas and via any other type of speech medium or channel (including social media).

SIIP's advanced SID engine will fuse multiple speech analytic algorithms regarding voice-print recognition, gender identification, age detection, language & accent identification, keyword & taxonomy spotting and voice cloning detection.

Expected results

This fusion will result in highly reliable and confident detection that keeps false positives & false negatives to a minimum while improving the judicial admissibility of the speaker identification technology.

PARTNERS	COUNTRY
Verint Systems Ltd. (VRNT)	Israel
Sail Labs Technology AG (SAIL)	Austria
Fondation de L'institut de Recherche (IDIAP)	Switzerland
Singularlogic Anonymi Etairia Pliroforiakon Sistimaton Kai Efarmogon Pliroforikis (SING)	Greece
Green Fusion Limited (DFI)	Ireland
Synthema S.R.L. (SNTMA)	Italy
OK2GO Cellular Solutions Ltd. (OK2GO)	Israel
Nuance (NUAN)	Italy
Inov Inesc Inovacao - Instituto de Novas Tecnologias (INOV)	Portugal
International Biometric Group (uk) Limited (IBG)	United Kingdom
Airbus DS SAS (ADS)	France
Rijksuniversiteit Groningen (RUG)	The Netherlands
The University of Warwick (WARWICK)	United Kingdom
Laboratorio di Scienze Della Cittadinanza (LSC)	Italy
The International Criminal Police Organization (INTERPOL)	France
Ministério da Justiça (PJ)	Portugal
Ministero della Difesa (RACIS)	Italy
Metropolitan Police Service (MPS)	United Kingdom
Bundeskriminalamt (BKA)	Germany

ADVISE / Advanced Video Surveillance archives search Engine for security applications

© AVC Group – Defence & Security

Information

Grant Agreement N°
285024
Total Cost
€4,237,304.80
EU Contribution
€2,989,761.60
Starting Date
01/03/2012
Duration
36 months

Coordinator

ENGINEERING - INGEGNERIA INFORMATICA S.P.A.
R&D Laboratory
Via Riccardo Morandi, 32
00148 – Rome - Italy
Contact
Carmela Occhipinti
Tel: +39 06 83074971
Mobile: +39 335 1328411
Fax: +39 06 83074200
(Please, write "For the attention of Carmela Occhipinti")
E-mail:
carmela.occhipinti@eng.it
Website: www.eng.it

Project objectives

ADVISE aims to design and develop a unification framework for surveillance-footage archive systems, in an effort to deal with the increasingly critical need to provide automated and smart surveillance solutions. This need arises due to the continuous growth of surveillance systems in scale, heterogeneity and utility. There are two major obstacles: the variety of the technical components of the surveillance systems, producing video repositories with different compression formats, indexing systems, data storage formats and sources, and the fact that such a system should take into careful consideration the legal, ethical and privacy rules that govern surveillance and the produced content. Towards both, ADVISE has been formed by experts on both technological and legal, ethical and privacy aspects, with valuable experiences in the security field. For this purpose, the consortium includes some major European security agencies, though it will collaborate with plenty of others through its Advisory Boards.

Description of the work

ADVISE will analyse and geo-register surveillance video archives of different agencies, and extract statistical patterns of activity and search (context-based and content-based) for specific events, people and objects through ontologies and semantic representations. In effect, the ADVISE system will enable interoperability beyond the boundaries defined by different compression formats, indexing systems, data storage formats and access systems, offering valuable insights and help during investigations of law enforcement authorities. In order to realise this aim, the following concrete goals have been identified:

» Legal and ethical exchange of data to offer secure and legally/ethically compliant inter-organisation communication;

» Video Analysis & Recognition to design, develop and validate novel, beyond SoTA, video analysis and recognition algorithms that will offer semantic search and analysis capabilities for various patterns (e.g. events, persons, cars, objects);

» Geo-registration assisted video archives analysis to support efficient time and camera indexing, thus empowering the tracing back of an object/person in time and in localisation, from surveillance system to surveillance system (and the corresponding video archives);

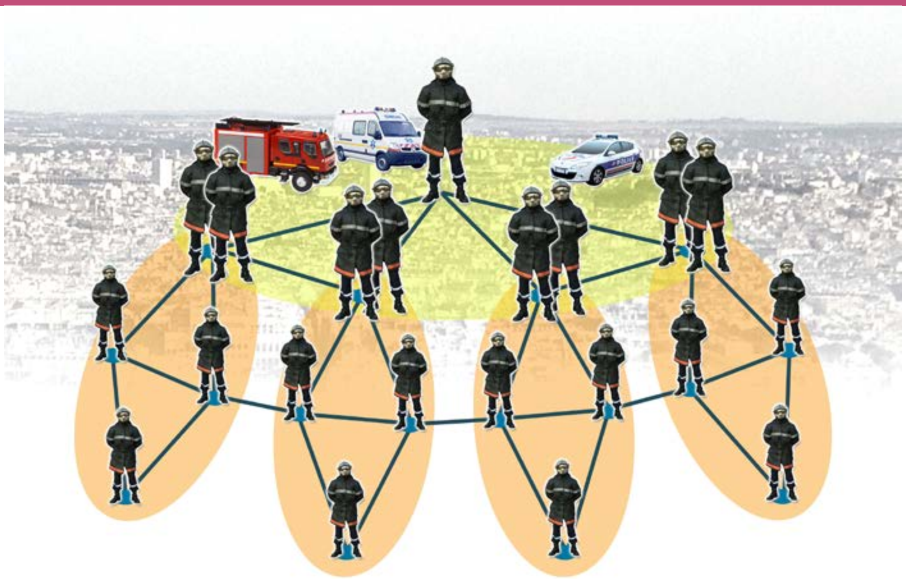
» Interoperability and Scalability to design and develop an open and extensible framework that will offer search capabilities for various patterns (e.g. objects, persons, events), into various video archives, independently from their different technological standards and ethical/privacy and legacy issues, focusing on improving the interoperability between infrastructure operators and between law enforcement agencies. The interoperability will cover the technical layer (aiming to solve the problems related to different formats of video archives and the communication format) and the semantic one (aiming to improve the search with an understanding of what happens in the footage, what is being looked for and who can access the information).

Expected results

The ADVISE system will result in two major components. The first will perform the semantically enriched, event based video analysis, offering efficient search capabilities into video archives and sophisticated result visualisation. The second will enforce the legal/ethical/privacy constraints that apply to the exchange and processing of the surveillance data. A Dedicated Engine will be developed to efficiently deal with each peer authority's technical and legal/ethical/privacy specificities.

PARTNERS	COUNTRY
ENGINEERING - INGEGNERIA INFORMATICA SPA (ENG)	Italy
SEMANTIX TECHNOLOGIES PLIROFORIKIS TILEPIKOINONION ANONYMOS ETAIREIA (SEM)	Greece
CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS/INFORMATICS & TELEMATICS INSTITUTE (CERTH/ITI)	Greece
QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)	United Kingdom
SINGULARLOGIC ANONYMOS ETAIRIA PLIROFORIAKON SYSTIMATON & EFARMOGON PLIROFORIKIS (SL)	Greece
VRIJE UNIVERSITEIT BRUSSEL (IES/VUB)	Belgium
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA-ISDEFE (ISDEFE)	Spain
ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA (Almaviva)	Italy
INNOVATION ENGINEERING SRL (INNEN)	Italy
AYUNTAMIENTO DE MADRID (ADM)	Spain

C2-SENSE / Interoperability Profiles for Command/Control Systems and Sensor Systems in Emergency Management



Information

Grant Agreement N°
607729
Total Cost
€4,363,641
EU Contribution
€2,885,416
Starting Date
31/03/2017
Duration
36 months

Coordinator

SAGEM DEFENSE SECURITE (SAGEM)
Direction R&T
Arcs de Seine, 18/20 Quai du Point du Jour
92100
Boulogne-Billancourt,
France
Contact
Banu Maria
Tel: +33 1 58 11 67 78
Mobile: +33 6 18 12 93 94
E-mail:
maria.banu@sagem.com
Website: www.c2-sense.eu

Project objectives

Effective management of emergencies depends on timely information availability, reliability and intelligibility. To achieve this, different Command and Control (C2) Systems and Sensor Systems have to cooperate, which is only possible through interoperability. However, unless standards and well-defined specifications are used, interoperability can be very complex.

C2-SENSE uses a "profiling" approach to achieve seamless interoperability by addressing all the layers of the communication stack in the security field.

The project's main objective is to develop a profile based Emergency Interoperability Framework by using existing standards and semantically enriched Web services to expose the functionalities of C2 systems, sensor systems and other emergency/crisis management systems.

C2-SENSE will develop a testing and a certification methodology allowing for the assessment of networked C2 and sensors systems for compliance with the profiles. The methodologies and framework will be made publicly available.

Description of the work

AThe work towards the definition and implementation of the profiles is organized in three steps:

» First, an "emergency domain inventory" will be created by surveying existing standards, real life use cases of sensors, devices, C2 systems and emergency management architectures for different scenarios in the security field.

» Then, based on this inventory, a common emergency domain ontology will be developed to gather all stakeholders' knowledge in a unique and flexible data model.

» Finally, by using the concepts in this ontology, and by taking into account both the functional and operational requirements, as well as different countries' cultural, linguistic and legal issues, "emergency interoperability profiles" that will constitute the framework will be developed.

In parallel with the framework definition work stream, the pilot mapped on the requirements of the Apulia Civil Protection Service will be designed and implemented to serve as a validation model and demonstration of the concepts.

The necessary standardization activities will be initiated to evolve the C2-SENSE "Emergency Interoperability Framework" into a standard specification for interoperability between sensor systems and C2 systems.

Expected results

- Increased robustness for sensors network management (sensors discovery mechanism, sensors allocation and life-cycle management).
- A trusted communication infrastructure model creating interconnectivity between different networks including TETRA, WiMAX, GSM and WiFi.
- Re-usable Web services for the emergency domain (assets and resources management, situation awareness, operations planning) based on standard data models.
- Semantic mediation mechanisms able to: harmonize information conforming to different but overlapping emergency standards; and automate many implementation processes.
- A service level agreements framework to be adopted for deployed procedures and operations.
- A definition of overall interoperability requirements and a methodology to certify compliance.

PARTNERS	COUNTRY
SAGEM DEFENSE SECURITE (SAGEM)	France
LUTECH SPA (LUTECH)	Italy
Austrian Institute of Technology GmbH (AIT)	Austria
Software Research, Development and Consultancy Limited (SRDC)	Turkey
REGIONE PUGLIA (REGIONE PUGLIA)	Italy
INNOVA PUGLIA SPA (IP)	Italy
PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW (PIAP)	Poland
Regola srl (Regola)	Italy

DISASTER / Data Interoperability Solution At Stakeholders Emergency Reaction

© PHOTOPQR - LE TELEGRAMME - Francois Destoc

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285069
Total Cost
€3,573,156
EU Contribution
€2,783,970
Starting Date
01/02/2012
End Date
31/01/2015

Coordinator

TREELOGIC TELEMÁTICA Y LÓGICA RACIONAL PARA LA EMPRESA EUROPEA S.L.
R&D
Parque Tecnológico de Asturias, parcela 30
E33428 Llanera, Asturias, Spain.
Contact
Marcos Sacristán Cepeda
Tel: +34 985 966 136
Mobile: +34 663 246 699
Fax: +34 985964190
E-mail: marcos.sacristan@treelogic.com
Website: www.treelogic.com

Project objectives

» Designing a reference architecture to solve interoperability problems in data exchange in SOA-based Emergency Management Systems (EMS), addressing interdisciplinary environments at a European level;

» Designing and developing an integrative and modular interoperable data model. This objective may be split into two sub-objectives:

- The core framework data model, common to every stakeholder involved in emergency management;
- Complementary transversal (spatial and temporal) & vertical (domain-specific) modules.

» Designing and developing mediation techniques, a set of bridges, enabling a transparent integration of the data model within already-existing SOA-based EMSs;

» Developing and executing a validation pilot phase in an actual environment, based on a representative scenario, in order to get feedback from end-users, and evaluating the project's outcomes and their benefits to the European multicultural domain related to emergency management.

Description of the work

Emergency management and information exchange become more challenging in an international crisis episode because of cultural, linguistic and legal differences between all stakeholders, especially first responders. Misunderstandings between first responders slow down decision-making and make it more difficult. The recent spread and development of networks and Emergency Management Systems (EMS) has facilitated communication and improved emergency responses, allowing them to become more coordinated and successful in overcoming distance issues, and allowing decentralized decision-making when necessary and appropriate. However, EMSs have still not solved problems related to cultural, legal and linguistic differences which are the greatest cause of slow decision-making. In addition, from a technical perspective, the consolidation of current EMSs and the limitations of their exchanged data formats offer significant problems to be solved in any solution proposing information interoperability and understanding between heterogeneous Emergency Management Systems located in different countries, and operating within different contexts.

To overcome this complicated situation, a two step solution was proposed: (i) As the main objective and foundation of the DISASTER project, the development of a common and modular ontology shared by all the stakeholders was proposed to offer the best solution to gather all stakeholders' knowledge in a unique and flexible data model, taking into account different countries' cultural, linguistic and legal issues; (ii) Then, taking advantage of the fact that most legacy Emergency Management Systems were based on Service-Oriented-Architectures (SOA), i.e. those systems compiled information from distributed and specialized systems (e.g. Geographic Information Systems). The interoperability information burden were addressed by means of transparent SOA mediation algorithms compliant with current data formats and existing solutions.

Taking into account the heterogeneity and diversity of all existing scenarios in crisis episodes, potential results of the ontology-based interoperability solution proposed have been validated through the design and development of a realistic prototype scenario, which actively involved both emergency managers and emergency first responders from organisations with significant experience in developing capability in technologies and organisational structures towards increased interoperability.

Results

Emergencies span borders. While new emergency management systems (EMSs) may improve communications and coordination, they do not address cultural, linguistic and legal differences given in an international context. Such factors may hinder emergency response.

The DISASTER project (http://www.disaster-fp7.eu/) developed a “bridge” system consisting of two components: a common and modular mapping ontology called EMERGEL that considers various cultural, semantic and linguistic issues, and a transparent service-oriented architecture providing mediation algorithms that conform to existing data formats and solutions.

Two field trials involving a fire across the German-Dutch border and a plane crash successfully tested the solutions, highlighting an effective interface of legacy EMSs between neighbouring countries, each of which updates the other side in culturally appropriate ways, allowing more coordinated crisis response.

DISASTER demonstrated the importance of data interoperability between EMSs and how new ways of information delivery and sharing can impact existing operational procedures, improving communication between first responders during major crises.

PARTNERS	COUNTRY
Treelogic Telemática y Lógica Racional para la Empresa Europea S.L. (TREE)	Spain
Fachhochschule Köln (CUAS)	Germany
Fundación CTIC Centro Tecnológico para el desarrollo en Asturias de las Tecnologías de la Información (CTIC)	Spain
Dansk Brand-Og Sikringsteknisk Institut Forening (DBI)	Denmark
Aimtech Consulting Limited (AIM)	United Kingdom
Veiligheidsregio Kennemerland (VRK)	The Netherlands
Antworting Ingenieurburo Weber Schutte Kaser partnerschaft (ANT)	Germany

ESENet / Emergency Services Europe Network

© Shutterstock

RESEARCH **COMPLETED**

Information

Grant Agreement N°
313013
Total Cost
€704,845.20
EU Contribution
€629,266.98
Starting Date
01/01/2013
End Date
31/12/2014

Coordinator

INTELLIGENCE FOR ENVIRONMENT AND SECURITY – IES SOLUTIONS (IES)
Via Monte Senario, 98
00141 Roma,
Italy
Contact
Uberto DELPRATO
Tel: +39 06 8184832
Mobile: +31 346 6367499
Fax: +39 06 87459009
E-mail: u.delprato@iessolutions.eu
Website:
www.iessolutions.eu

Project objectives

The ESENet initiative aimed at establishing a network of stakeholders in the Emergency Management domain that identified, discussed and agreed on communication needs, requirements, new technologies and best practices in responding to everyday, as well as, major emergencies.

The project aimed to achieve the following via public reports:

» The identification of gaps in the emergency service provision chain and the collection of user requirements; the results of such activity were a living document that was made available to all stakeholders;

» The selection of available and/or promising technologies for tackling the identified challenges and also identifying areas where further research is needed;

» The analysis of organisational gaps, with suggestions and best practices at EU level about procedures, framework agreements and reorganising suggested tasks; the results of such work have been reported in a public deliverable in the form of a roadmap to improve the Emergency Services throughout Europe;

» The identification of available standards, gaps in existing standards or areas where standards will be needed in the future.

Description of the work

The project planned to organise a total of 8 web-meetings and 4 workshops during the term of the project. Experts from emergency service authorities, public safety representatives and commercial organisations were invited to attend and contribute to working documents prepared by the project partners on several topics, including interoperability at all levels (from the technical level to the organisational level) and in all types of safety and security missions (daily/ordinary and/or large scale missions as well as local or cross-border missions).

The communication requirements covered by ESENet range from “Citizens to authorities”, “Authorities to authorities” and “Authorities to citizens”.

Results

Over a period of two years ESENet's network of 65 experts plus its nine webinars and four workshop identified 180 items for tackling the interoperability needs emerging from the Society.

The coverage of the communication phases during an emergency (from citizens to authorities, between authorities and from authorities to citizens) led to recommendations offered to the European Commission, the Member States and the Emergency Services about actions in the areas of legal provisions, standardisation, further research, implementation and monitoring.

The collected recommendations were organised in the following "Top Stories":

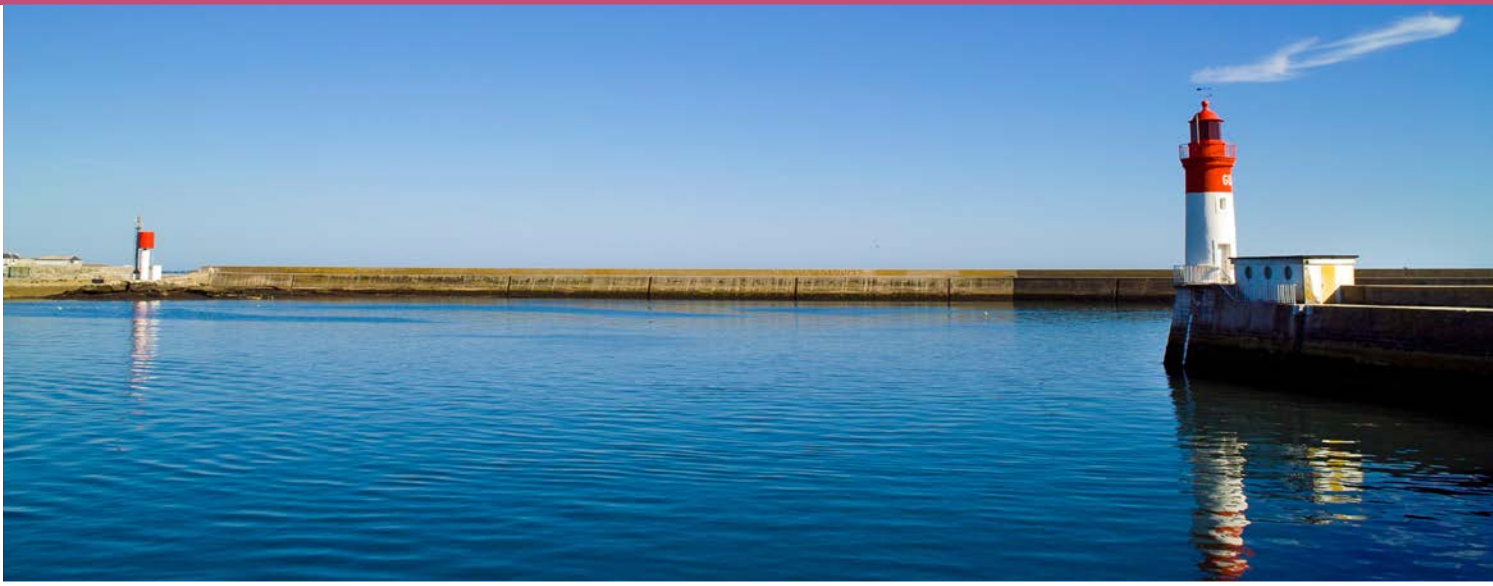
- Basic caller access and information
- Management of trans-national emergency calls
- Interaction in case of an emergency
- Mission Critical Communication
- Moving forward to NG112
- Harmonisation of public warning systems
- Data exchange between Emergency Services
- Cross-border cooperation during emergencies
- Business continuity and contingency management
- Improved call management

A final public report was produced, published and distributed.

The network of experts is continuing its work within the "Emergency services Staff Network" (ESSN), set up and supported by EENA.

PARTNERS	COUNTRY
Intelligence for Environment and Security – IES Solutions (IES)	Italy
European Emergency Number Association (EENA)	Belgium
Erupsi (ERUPSI)	Slovakia

EUCISE2020 / EUropean test bed for the maritime Common Information Sharing Environment in the 2020 perspective.



Information

Grant Agreement N°
608385
Total Cost
€17,053,927.59
EU Contribution
€13,000,000.00
Starting Date
01/12/2014
Duration
31 months

Coordinator

ITALIAN SPACE AGENCY (ASI)
Via del Politecnico snc
00133 Rome, Italy
Contact
Carolina Matarazzi
Tel: +39 06 8567941
Mobile: +39 3356764154
E-mail:
carolina.matarazzi@asi.it
Website:
www.eucise2020.eu

Project objectives

EUCISE2020 aims to establish an important milestone for implementation of CISE – the EU's Common Information Sharing Environment.

CISE supports development of the EU's "blue economy" regarding its maritime governance. It is thus an element of the union's European Digital Agenda and a pillar of its action plan, the European Maritime Security Strategy.

Description of the work

The project is based on:

» the CISE Roadmap developed by DG MARE

» results of the European pilot projects BluemassMed and MARSUNO, and of the study project "Cooperation"

» work performed by the CISE TAG-Technical Advisory Group

» previous European studies on maritime surveillance

» results of FP7 Security Research projects, in particular PERSEUS and SEABILLA

» the needs of innovation expressed by the maritime stakeholders based on their operational experience in managing maritime surveillance processes and systems at European, international and national levels

Under guidance of a stakeholder board, EUCISE2020 will manage in parallel the elaboration of the action plan for the operational validation of new elements of R&D needed to develop CISE such as concepts of architecture, concepts of operation, standards of data and services, and new services and processes. It will develop an open European testbed for incremental advancement of CISE in the medium-long term. It will carry out independent verification and validation of new R&D elements, and assess organisational instruments needed to sustain CISE's governance structure while stimulating public-private cooperation.

The EUCISE2020 consortium will define the requirements of the CISE testbed and launch a European tender to develop and demonstrate it.

EUCISE2020 will create significant opportunities for national and European maritime institutions to collaboratively innovate their processes and systems, and for European enterprises to develop a new range of competitive solutions and services in the international market.

Expected results

EUCISE2020 aims to achieve pre-operational information sharing between the maritime authorities of the involved European nations.

PARTNERS	COUNTRY
Italian Space Agency (ASI)	Italy
Ministero della Difesa (MMI)	Italy
Ministero dell'economia e delle finanze (MEF GDF)	Italy
Italian Ministry of Infrastructures and Transports (MIT GC)	Italy
Ministerio de defensa de Espana (MDE ES)	Spain
Ministerio del Interior (GUCI)	Spain
Ministerio de Fomento (SASEMAR)	Spain
European Union Satellite Centre (EUSC)	Spain
Swedish Coast Guard (SwedCG)	Sweden
Ministry of the Interior (MIN INT FBG)	Finland
Liikennevirasto (FTA)	Finland
Liikenteen Turvallisuusvirasto (TRAFI)	Finland
Ministry of Transport, Information Technologies and Communications (BGPORT)	Bulgaria
Samferdselsdepartementet – Ministry of Transport and Communications (MTC)	Norway
Laurea – Ammattikorkeakouli Oy (LAUREA)	Finland
University of Cyprus (OC-UCY)	Cyprus
Agenzia per la Promozione della Ricerca Europea (APRE)	Italy
Istituto Nazionale di Geofisica e Vulcanologia (INGV)	Italy
Centro Euro-Mediterraneo sui Cambiamenti Climatici (CMCC)	Italy
Danmarks Meteorologiske Institut (DMI DK)	Denmark
Stiftelsen Nansen Senter For Miljoog Fjernmaling (NERSC)	Norway
Agencia Estatal de Administracion Tributaria (AEAT ES)	Spain
Cork Institute of technology (CIT)	Ireland
Direcao-Geral de Politica do Mar (DGPM)	Portugal
Executive Agency Maritime Administration (MARAD)	Bulgaria
National Center for Scientific Research (DEMOKRITOS)	Greece
Ispectoratul General al Politiei de Frontera (RBP)	Romania
Finnish Navy (FINNAVY)	Finland
Bundesministerium fur Verkehr, Bau und Stadtentwicklung (FGMSSC)	Germany
Ministry of National Defence (HMOD)	Greece
Ministry of Citizens Protection (EL-HCG)	Greece
Mercator Ocean (MERCATOR)	France
Ministero dello Sviluppo Economico (MISE)	Italy
Studio Legale Tosato (GLT)	Italy
Department for Transport (DFT)	United Kingdom
Link Campus University (LCU)	Italy
Wise Pens International Limited (WPI)	United Kingdom

ISITEP / Inter System Interoperability for Tetra-TetraPol Networks

ISITEP
INTER SYSTEM INTEROPERABILITY FOR TETRA-TETRAPOL NETWORKS
Achieving a full Interoperability through the integration of all TETRA and TETRAPOL networks,with new mission procedures and enhanced terminals.

Information

Grant Agreement N°
312484
Total Cost
€15,985,650.87
EU Contribution
€10,292,495.07
Starting Date
01/09/2013
Duration
36 months

Coordinator

SELEX ES (SES)
Institutional Financing EU,
NATO and United Nations
Via Tiburtina km 12,400
00131 - Roma - Italy
Contact
Paolo DI MICHELE
Tel: +39 06 4150 4850
Mobile: +39 335 7570 556
Fax: +39 06 4458 3088
E-mail: paolo.dimichele@selex-es.com
Website: www.selex-es.com

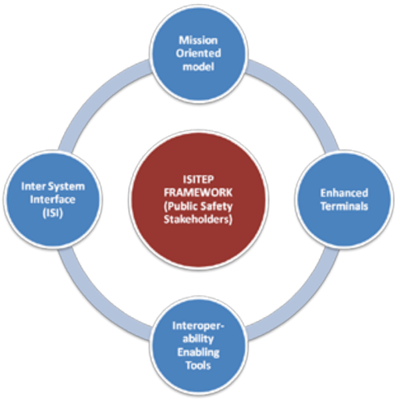
Project objectives

» Develop a future-proof pan-European framework for the integration of different Public Protection & Disaster Relief (PPDR) national organizations, merging communications technology, operational procedures and the legal framework

» Test the provided framework using a number of multiagency cooperation scenarios, such as cross-border Police hot pursuit, Joint police patrol surveillance operation, joint forces airplane disaster management, and VIP protection through cooperation of national police forces

Description of the work

ISITEP will develop procedures, technology and legal agreements to achieve a cost effective solution for PPDR interoperability.


Mission Oriented model
Inter System Interface (ISI)
ISITEP FRAMEWORK (Public Safety Stakeholders)
Enhanced Terminals
Interoper-ability Enabling Tools

ISITEP will demonstrate full radio interface capabilities for PPDR resources. ISITEP end users will drive requirements to guarantee legal, operational and technical coherence. In addition, a legal agreement template will be proposed for approval between Norway and Sweden within the project timeframe. Through ISITEP, European end users will utilize enhanced terminals in operations abroad within an agreed framework of procedures. This will improve cooperation among European PPDR resources for the benefit of all citizens. European stakeholders will have an economically sustainable solution for sharing national PPDR services. ISITEP's results will be disseminated by a proper plan utilizing the resources of the Consortium, which includes all the manufacturers of national European networks and the main PPDR stakeholders. Furthermore, through ISITEP technology, the European security industry will have new market opportunities.

Expected results

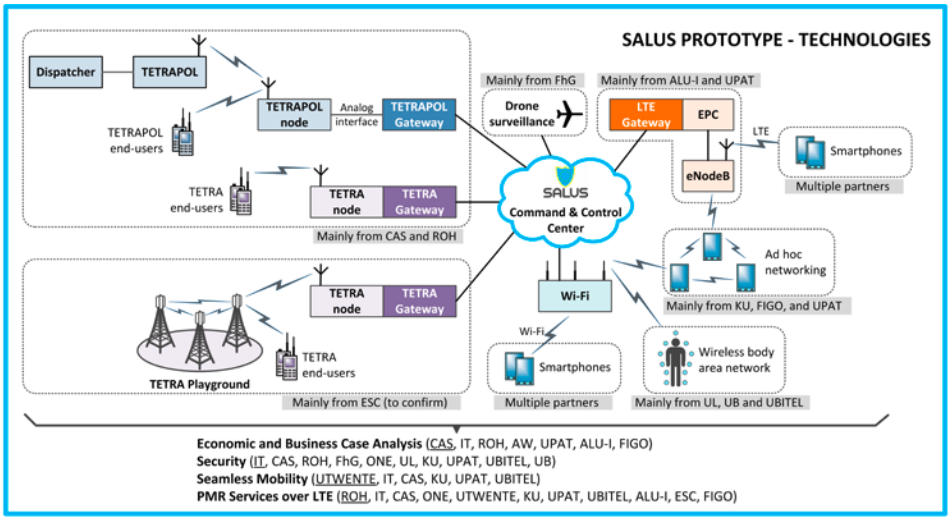
The project goals will be obtained through the delivery of the ISITEP framework, which will be based on:

- » Mission oriented procedures, functional models and legal agreements
- » An European network solution integrating all types of European national PPDR networks through a novel InterSystem Interface (ISI) over IP protocol, encompassing:
  - ETSI standardized ISI among TETRA national networks
  - ISI over IP Gateways among national TETRAPOL networks
  - ISI over IP gateways among TETRAPOL - TETRA networks
- » Bi-technology terminals based on smartphones/tablets with PPDR applications
- » Supporting tools to assess business sustainability, technology needs and improve training

Thanks to increased cooperation achieved through the proposed framework, a better management of migration at European national borders is expected with a reduction of cross border crime activities and a more effective protection of EU citizens. Similar significant improvements are expected in joint disaster relief operations.

PARTNERS	COUNTRY
Selex ES (SES)	Italy
Service Public Federal Interieur (BFP)	Belgium
Norwegian Ministry of Justice and Public Safety (DNK)	Norway
Myndigheten for Samhallsskydd och Beredskap (MSB)	Sweden
Ministerie van Binnenlandse Zaken en Koninkrjksrelaties (V&J)	The Netherlands
Amper Sistemas S.A. (AMP)	Spain
Cassidian Finland OY (CAS FI)	Finland
Cassidian SAS (CAS FR)	France
Motorola Solutions Danmark AS	Denmark
Istituto Superiore delle Telecomunicazioni e delle Tecnologie dell'Informazione (ISCOM)	Italy
Net Technologies Etaireia Periorismenis Efthynis (NETTECH)	Greece
Università degli Studi Roma Tre (RM3)	Italy
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Universitat Politecnica de Catalunya (UPC)	Spain
Devoteam Fringes (DVT)	Spain

SALUS / Security And InteroperabiLity in Next Generation PPDR CommUnication InfrastructureS



Economic and Business Case Analysis (CAS, IT, ROH, AW, UPAT, ALU-I, FIGO)
Security (IT, CAS, ROH, FhG, ONE, UL, KU, UPAT, UBITEL, UB)
Seamless Mobility (UTWENTE, IT, CAS, KU, UPAT, UBITEL)
PMR Services over LTE (ROH, IT, CAS, ONE, UTWENTE, KU, UPAT, UBITEL, ALU-I, ESC, FIGO)

IT-Instituto de Telecommunicacoes (PT)| CAS – Cassidian (FR)| ROH – Rohill (NL) | AW – Airwave (UK) | FhG – Fraunhofer IOSB (DE) | ONE – OneSource (PT) | UL – Univ. Ljubljana (SI)| UTWENTE – Univ. Twente (NL) | KU - Kingston University London (UK) | UPAT - Uni Patras (GR)| UBITEL – Ubitel (RUS)| UB – Univ. Belgrade (SRB) | PSCE – Public Safety Communications Europe (BE)| ALU-I – Alcatel Lucent International (FR)| FIGO – FIGO BV (NL)

Information

Grant Agreement N°
313296
Total Cost
€4,768,125.28
EU Contribution
€3,499,829.00
Starting Date
01/09/2013
Duration
36 months

Coordinator

INSTITUTO DE TELECOMUNICAÇÕES (IT)
Aveiro
Campus Universitário de Santiago
3810-193
Portugal
Contact
Hugo Marques
Tel: +351 234 377 900
Mobile: +351 917 866 391
Fax: +351 234 377 901
E-mail:
hugo.marques@av.it.pt
Website: www.sec-salus.eu

Project objectives

» Design, develop and validate the next generation PPDR network concept;

» Support TETRA and TETRAPOL functionalities on the next generation PPDR network;

» Provide guidelines towards the medium/long term evolution of the PPDR network;

» Set out economic implications and possible migration paths for the PPDR network and service evolution;

» Collect statistical data related to police forces and first responders across Europe;

» Foresee business cases associated with the evolution of the PPDR network;

» Contribute towards the standardisation efforts on the next generation PPDR network (including architectural design and spectrum requirements).

Description of the work

SALUS Project aims to develop and prototype the next generation PPDR network and services for public protection and disaster relief. The network will be backward compatible with legacy communication technologies, fully converged with the 4G evolutionary wireless paradigm and supporting robust and reliable transmission of broadband data. This task is supported by network operators and industry, which will provide security, privacy, seamless mobility, Quality of Service (QoS) and reliability support for mission-critical PMR voice and broadband data services.

Expected results

To enable robust, reliable, and secure mobile broadband communication for a wide variety of PPDR applications, including the ability of inter-system, inter-agency and cross-border interoperability.

PARTNERS	COUNTRY
European Commission (EC)	Belgium
Instituto de Telecomunicacoes (IT)	Portugal
Cassidian SAS (CAS)	France
Rohill Technologies BV (ROH)	Netherlands
Airwave Solutions Ltd (AW)	United Kingdom
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V (FhG)	Germany
One Source Consultoria Informatica Lda (ONE)	Portugal
Univerza v Ljubljani (UL)	Slovenia
Universiteit Twente (UTWENTE)	The Netherlands
Kingston University Higher Education Corporation (KU)	United Kingdom
University of Patras (UPAT)	Greece
Ubitel CO Ltd (UBITEL)	Russian Federation
Elektrotehnicki Fakultet Univerzitet u Beogradu (UB)	Serbia
Public Safety Communication Europe Forum AISBL (PSCE)	Belgium
Alcatel-Lucent International SAS (ALU-I)	France
Pelastusopisto, Emergency Services College (ESC)	Finland

SAVASA / Standards Based Approach to Video Archive Search and Analysis

© Mike Zakharov - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285621
Total Cost
€4,061,085
EU Contribution
€3,166,266.58
Starting Date
01/12/2011
End Date
31/12/2014

Coordinator

ANGEL IGLESIAS S.A. - IKUSI
R&D
Paseo Miramon
20009, San Sebastian
Contact
Gorka Peréz
Tel: +34 943 44 88 00
Mobile: +34 650 15 69 56
Fax: +34 943 44 88 20
E-mail:
gorka.perez@ikusi.com
Website: http://www.ikusi.com/

Project objectives

The SAVASA project proposes the creation of a video archive search platform that allows authorised users to perform semantic queries over different, remote and non-interoperable video archives. This project will exploit the current trends in computer vision, video retrieval and semantic video analysis. It is also a goal of the project to ensure that its results are capable of deployment in distributed systems and as software services.

However, technology for technology's sake is of little value. Therefore the involvement of ethicist, legal experts and, those users who must operate Video Archive installations and services to meet the needs of law enforcement agencies and judicial authorities, as well as those of civil protection and day-to-day organisational needs, is required. The SAVASA consortium covers each of these roles.

At its core, SAVASA will use existing reference technologies from the ICT field that have overcome the barrier of system interoperability/compatibility, i.e. between container and compression formats. The project will implement a prototype platform capable of demonstrating unified archive integration and an approach to common search and indexing. The project will also provide a set of tailored video analytics and semantic analysis tools that will provide added value to end-users, but which can also function within a legal and ethical framework. The project will provide an analysis of existing technical barriers/requirements in the standardisation of technologies and procedures, via the validation testing of a prototype platform with end users.

Description of the work

The SAVASA project plan will focus on the following objectives:

Interoperability:

» Application of semantic technologies to enhance the analysis of video archive content;

» Compliance with national and European regulations applicable to video surveillance.

Open standards:

» Definition of a migration path from proprietary technologies to open standards;

» Propose best practices and procedural approaches in the absence of defined standards;

» Participation in standards bodies relevant to the results of the project;

» Leverage existing Open and International Standards, and open source initiatives.

User focused applied research:

» Focus on the real user needs, such as operators and law enforcement agencies that make intensive use of video archives;

» The introduction of high level and rich information to video sources to boost data mining from video archives, as well as keeping protected privacy data through the application.

Ethical and privacy protection:

» Address issues that video surveillance inevitably implies; ethically sensitive issues related to personal data beyond what is established by law;

» Operational restrictions controlled by rules on conducting situational assessments to ensure that required control levels are reached.

Video analytics:

» Application of the latest trends in object detection and tracking, based on probabilistic inference and models, to enhance robustness and accuracy of elements of interest descriptions within videos;

» Use of signal encryption and cryptographic methods to protect private elements of the video;

» Exploitation of visual features to identify object properties in order to enrich the metadata descriptions;

» Development of video analysis tools to automatically annotate video with semantic concepts and scenarios.

Contribution to Standards:

» Contribution to standards related to video surveillance, storage, secure communications and metadata indexing;

» Development of a set of operational best practices derived from the results of end-user validation tests.

Multiple Archive Integration:

» Integration of multiple video archive systems (remote or local), under a single technology that presents these archives as a homogenous logical system vis-à-vis an indexing and search system;

- Multi-modal search across multiple video archives tailored to the requirements of end users of surveillance video archives;
- Implementation of the core technological deliverables as a set of distributed applications suitable for deployment as software services.

Results

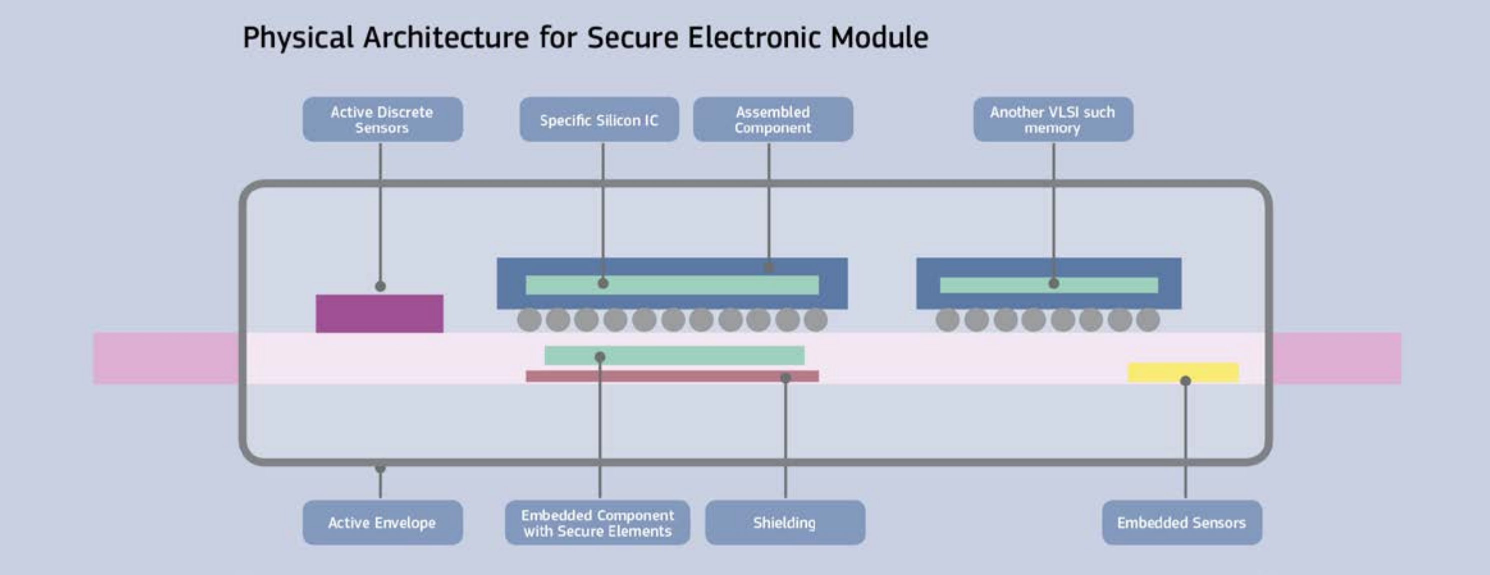
At the end of the project, the SAVASA platform has been implemented and has provided a step forward for video surveillance archive exploitation comprising a unified archive integration layer that is capable of making multiple remote or local video archiving systems available to end-users as a logically unified archive. It also provides a common video search and indexing application that builds upon the integration layer which supports multi-modal video search over multiple archives in a distributed manner.

The application of open standards has been a design requirement for moving from a legacy set of proprietary compression, encoding and container formats into an integrated set of open source and open standards tools. A set of enhanced video analytics applications have been deployed that can leverage the common archive integration and search applications to provide operators with tools that are lacking in current systems.

The whole framework provides an absolute guarantee that neither legal nor ethical norms are compromised. The integration of video semantic analysis and annotation permits operators to perform searches across multiple archives based on a generalised hypothesis rather than concrete syntactic concepts. In a few words, the SAVASA project has reached its S&T objectives by focusing on interoperability, open standards, ethical and privacy protection, semantic video analytics and multiple archive integration.

PARTNERS	COUNTRY
Angel Iglesias S.A.- IKUSI (IKUSI)	Spain
Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones Vicomtech (VICOM)	Spain
Studio Professionale Associato a Baker & McKenzie (BAK)	Italy
HI-Iberia Ingeniería y Proyectos S.L. (HIB)	Spain
Dublin City University (DCU)	Ireland
University of Ulster (UU)	United Kingdom
INECO (INECO)	Spain
Demokritos (NCSRD)	Greece
Sintel Italia (SINTEL)	Italy
Dirección General de Tráfico – Ministerio del Interior (DGT)	Spain
RENFE Operadora (RENFE)	Spain

UNSETH / Embedded protection of security systems and anti-tampering technologies



Information

Grant Agreement N°
312701
Total Cost
€6,615,904
EU Contribution
€3,874,033
Starting Date
01/01/2014
Duration
36 months

Coordinator

THALES COMMUNICATIONS & SECURITY SAS (TCS)
HTE - Hardware Technology Tools & Engineering Competence Center
4 Avenue des Louvresses
92622 GENNEVILLIERS - FRANCE
Contact
Bernard Candaele
Tel: +33 1 46 13 27 66
Mobile: +33 6 08 65 07 96
Fax: +33 1 46 13 25 55
E-mail: bernard.candaele@thalesgroup.com
Website:
www.thalesgroup.com

Project objectives

UNSETH aims to complement the solutions already available at chip level by adding new technologies (like tamper detection features and higher tamper resistance) for electronic assembly and packaging and to propose a generic protection profile to the highest possible assurance level, while meeting the need to protect against high levels of attack.

Security has become a vital part of European electronic products and equipment as they handle sensitive data in uncontrolled environments and as they face more and more content protection questions and counterfeiting. New applications combine a challenging set of requirements, including low-cost, security, and tamper-resistance.

UNSETH explores and derives the advantages which can be obtained by introducing new nanomaterial printed envelopes, 3-D embedded devices, and System-in-Packages with active anti-tamper sensors that focus on both the electronic modules and the manufacturing process.

The aim is to set up and qualify European technologies and capabilities and to maintain Europe as a worldwide player in the field of secure and safe architectures. Major achievements expected are protections against tampering, higher security compatible with mass production costs, and robust secure protection needed for high end products.

Description of the work

The project analyses constraints for mobile, network or security resources, coupling their requirements with nanomaterial printed envelopes, embedded dye protection, and tamper resistant SiP into hardware architectural building blocks. Test vehicles are defined for prototyping and also as references to measure their resistance to potential attacks and to propose related countermeasures. The project proposes to develop state of the art and advanced technologies, i.e. nanoparticle inks by aerosol-jet from Fraunhofer ENAS, Embedded Components packaging in PCB from AT&S, and eWLP and SiP System-in-Package assembly from Nanium. Thales brings applications for security with its entity TCS and checks manufacturability of the technologies with TGS. While Epoche & Espri is the security evaluation center which proposes a related Protection Profile

UNSETH integrates the results from ongoing embedded dye technology work in FP7's HERMES scheme. PCB module containing embedded dyes are used and integrated to build UNSETH technology prototype to be assessed with security evaluation.

The project realises several test vehicles to validate the building blocks for the different technologies, to perform security evaluation of the integrated solution, as well functional verifications and solution manufacturing within the timeframe.

Expected results

The project will validate two complementary technologies as tool boxes for security:

- embedding secure microcontroller in printed circuit boards to form a highly integrated part of the electronic system which can be protected to form a first level of anti-tampering protection
- secure sensor printed in a casing above the electronic module to form a second level of anti-tamper envelopes.

The project performs, tests and evaluates the reliability of the assembled boards equipped with the smart envelopes.

The project will draw on conclusions from the security testing and evaluation to provide guidance to users and integrators of the UNSETH technology: the security testing and evaluation protocol will be formalised in a standard form to be shared with the European community.

PARTNERS	COUNTRY
Austria Technologie & SystemTechnik Aktiengesellschaft (AT&S)	Austria
Nanium S.A (NAN)	Portugal
Fraunhofer-Gesellschaft for Foerderung der Angewandten Forschung E.V. (FhG ENAS)	Germany
Thales Global Services SAS (EPM)	France
Epoche and Espri S.L. (EPO)	Spain

EULER / European software defined radio for wireless joint security operations

© RCP Photo- Fotolia.com

RESEARCH COMPLETED

Information

Grant Agreement N°
218133
Total Cost
€15,468,483
EU Contribution
€8,720,692
Starting Date
01/03/2009
End Date
30/04/2012

Coordinator

THALES COMMUNICATIONS S.A.
Boulevard de Valmy 160
FR-92700 Colombes
France
Contact
Bruno Calvet
Tel: +33 (0) 1 41 302 084
Fax: +33 (0) 1 46 132 555
E-mail: bruno.calvet@fr.thalesgroup.com

Project objectives

EULER collaborative research project gathers main European actors to demonstrate how the benefits of Software Defined Radio can be leveraged in order to enhance interoperability and fast deployment in case of crisis needed to be jointly resolved.

Communication systems used on field by security organisations constitute major elements enabling restoring security and safety after crisis in an efficient manner. Large scale events necessitate the cooperation between security organisations of different nature and different nations. In connection with a strong group of end-users in Europe, EULER will contribute in proposing a more agile, interoperable, robust communication system supporting a new range of services to its users. In order to achieve these goals, three main components will be combined: a reference high-data-rate radio technique, a communication system architecture allowing integration of heterogeneous radio standards and Software Defined Radio (SDR) as a key enabler for this.

Description of the work

Enable enhanced deployment of protection organisations on a crisis location: groups gathered to operate need their radio systems to coexist and to be inter-connected, with short configuration time. EULER will provide a reference system architecture enabling on-the-field integration of such radio techniques.

Enhance the capabilities of wireless communication systems to enable high-speed communication backbone and also allow emerging types of services (such as on-field video, telemedicine, on-field sensors' values transmission) but also usual PMR ones. To this end, a new reference high-speed radio waveform will be proposed in line with functional, security and operational conditions (e.g urban, rural areas, …).

Provide fully programmable radios via a standardised software interface (Software Defined Radio), allowing to realise the system architecture and reference wireless communication waveform in a software-portable fashion, hence guaranteeing reusability of these elements across platforms from different organisations and suppliers.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

© wayne ruston – Fotolia.com

PARTNERS	COUNTRY
Thales Communications S.A	France
Cassidian S.A.S. (EADS DS)	France
Astrium Ltd. (EADS-Astrium)	United Kingdom
Budapest University of Technology and Economics	Hungary
Elsag Datamat s.p.a.	Italy
Selex Communications S.P.A.	Italy
Telespazio S.P.A.	Italy
Universita di Pisa.	Italy
Saab Communications	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Indra Sistemas S.A.	Spain
Rohde & Schwarz gmbh.	Germany
Center for Wireless Communications, University of Oulu	Finland
Prismtech Limited	United Kingdom
Interuniversitair Micro-Electronica Centrum VZW (IMEC)	Belgium
European Commission – Joint Research Centre (JRC)	Belgium
Ecole Superieure d'Electricite	France
Elektrobit Wireless Communications	Finland
SELEX Sistemi Integrati S.p.A. (SELEX)	Italy

FREESIC / Free Secure Interoperable Communications

© UL û Aurel Machalek

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285205
Total Cost
€4,338,320
EU Contribution
€3,284,040
Starting Date
01/02/2012
End Date
31/07/2014

Coordinator

ARDACO, A.S.
Polianky 5
84101 – Bratislava
Slovakia
Contact
Miroslav Konecny
Tel: +421 232 212 311
Mobile: +421 910 889 650
Fax: +421 232 212 312
E-mail: miroslav.konecny@ardaco.com
Website: www.freesic.eu

Project objectives

The main objective of FREESIC was to validate an innovative interoperability ICT concept for better cooperation of various emergency responders (both public services and private grid services).

FREESIC investigated barriers to interoperability of emergency services, proposed a communication solution supporting information exchange through heterogeneous communication systems, deployed the interoperability platform into three countries and evaluated its operation.

Security aspects and user requirements were both essential and shaped the delivery of the project.

Description of the work

The FREESIC project created a solution that allowed highly secure and cost effective interoperability between communication infrastructures right across Europe. The project has been inspired by legal, organizational and operational barriers the consortium has encountered during its previous activities (i.e. the project Secricom).

Approach

Existing interoperability solutions such as gateways are the right approach and simplified FREESIC's adoption and in return FREESIC opened broader possibilities for them. It was operated free-of-charge and offered an open source gateway, documentation and operational guidelines for others to use. It was the project's ambition to continue the free-of-charge operation after the project's end as well. The operational costs were covered by the new business opportunities.

Operation

The system should motivate end users outside the consortium to request the integration from their system vendors or integrators. The architecture took into account ongoing standardization research (e.g.: NCOIC Interoperability Framework) to reduce the integration time and costs. The integration process was simple; the system integrator took the gateway and modified it as needed. The gateway remained the property of the integrator. The integrators did not have to worry about disclosing any know-how or information. The communication between gateways was end-to-end encrypted and the gateway was under full control of end users to avoid security concerns.

Workpackage structure:

» *WP1* - Project management;
» *WP2* - Requirements and limiting factors analysis;
» *WP3* - Definition of technical and non-technical solutions;
» *WP4* - Implementation of the interoperability platform;
» *WP5* - Integration of end user systems;
» *WP6* - Acceptance and scenario testing by users;
» *WP7* - Dissemination and exploitation.

Results

FREESIC's goal was to "allow highly secure and cost effective interoperability between communication infrastructures over the entire Europe". The approach chosen was to leverage existing interoperability solutions such as gateways, simplifying FREESIC's adoption by agencies, and, in return, opening broader possibilities for them. The services operated free of charge and offered open source gateway code, documentation and operational guidelines for others to use.

Provisions were made to continue the free-of-charge operation after the project's end. The architecture took into account ongoing standardisation research (e.g., the NCOIC Interoperability Framework) to reduce integration time and costs.

The integration process was simple: the system integrator took the gateway equipment and modified it as needed. While the gateway remained the property of the integrator, the integrator did not have to worry about disclosing any know-how or information. Communication between gateways was end-to-end encrypted and each gateway was under the full control of the end user, so as to avoid security concerns. The project was successful in showing initial concept of open source communication gateway together with socio-networking cooperation.

- The FREESIC Interoperable communication platform was developed with its validity proven during a final demonstration.
- An open-source gateway was developed and its source code was published and made available to end users and for future development.
- The project's outputs have obtained wide recognition in Europe, thanks to participation in two major events: Security Essen and Milipol Paris.
- The FREESIC project provided the basis for a subsequent project researching interoperability, REDIRNET – Emergency Responder Data Interoperability Network.
- The Czech Republic has showed interest in the FREESIC concept and implementation. Huge FREESIC deployment is planned during modernization of Pegas network; common radio communication technology platform for all members of Czech Republic IRS.
- Ongoing standardisation activities

PARTNERS	COUNTRY
Ardaco, a.s. (ADO)	Slovakia
National Security Authority of the Slovak Republic (NSA)	SlovakiaUniver-
sité du Luxembourg (UL)	Luxembourg
British Association of Public Safety Communication Officers (BAPCO)	United Kingdom
ITTI Ltd. (ITTI)	Poland
NEXTEL S.A. (NEX)	Spain
Centre de Communications du Gouvernement (CCG)	Luxembourg
World Consult, a.s. (WCT)	Slovakia
Pramacom Prague (PCM)	Czech Republic

GERYON / Next generation technology independent interoperability of emergency services

© GERYON

RESEARCH COMPLETED

Information

Grant Agreement N°
284863
Total Cost
€3,590,730.20
EU Contribution
€2,512,308.65
Starting Date
01/12/2011
End date
31/05/2014

Coordinator

UNIVERSIDAD DEL PAIS VASCO EHU UPV
Faculty of Engineering
of Bilbao
Alameda Urquijo s/n
48013 Bilbao, Spain
Contact
Fidel Liberal
Tel: +34 946014129
Fax: +34 946014259
E-mail: fidel.liberal@ehu.es
Website: www.sec-geryon.eu

Project objectives

GERYON proposed seizing the existing window of opportunity due to the convergence of commercial LTE networks, IMS as a predominant enabler for multimedia networks, and uncertainty about the future of classic emergency networks due to spectrum scarcity, digital dividend issues and economic crisis.

The project aims at unifying technical and operational logic of first responder communications by providing an IMS based technology independent system. GERYON ensured seamless operation regardless of the access technology and took advantage of the coverage and responsiveness of existing PMRs and broadband data services of 4G networks.

Intermediate objectives included the design and development of:

- A fully operational IMS-driven emergency services management platform;
- An emergency services central management system and associated transcoding and security gateways.
- Advanced decision support logic for multimedia emergency communications;
- A technology agnostic TETRA-IMS interconnection gateway;
- A software client that allowed for using a subset of GERYON services through non-GERYON access networks;
- A transnational TETRA and 4G based testbed.

Description of the work

GERYON proposed an innovative emergency internetworking system capable of connecting existing first responder communication systems and enabling the integration of next generation mobile networks by defining technology independent standardized interfaces and autonomic configuration and adaptation techniques under the umbrella of IMS.

GERYON demonstrated both classic (i.e. PTT, MTP and preemptive calls) and enhanced emergency services (i.e. multimedia streaming and data services) over an across-frontier testbed. Furthermore, its capability for including general purpose IMS terminals and GERYON enhanced ones allowed an easy access to first responder networks to general purpose devices.

The project was divided into 5 technical Work Packages (WPs):

Specifications and system design.
The initial stage was dedicated to the definition of the overall system architecture and the specifications of the GERYON interfaces between different modules and systems, including internal ones and those related to IMS signalling. The trial plan and tests to be conducted were also specified. End users took an active role in the requirements gathering stage of this WP.

GERYON management system design and development.
This WP dealt with the design and implementation of the hardware and software modules of the central management system, as well as the considered emergency services and transcoding and security gateways.

Interconnection gateway design and development.
A technology independent reference interconnection gateway was designed in this WP. Later, a working prototype considering TETRA, LTE and IMS was developed according to a GERYON specific testbed.

GERYON-enabled LTE emergency communications.
The GERYON testbed demanded basic technology dependent interfaces to be developed for the LTE scenario.

Integration, Field Trials and Evaluation.
The final WP was dedicated to the integration of all the

systems, components, hardware and software modules that have been developed in previous WPs into a complete system, in order to demonstrate the whole GERYON ecosystem. Again, end users took part significantly in trial and evaluation tasks.

Results

GERYON developed and demonstrated a complex ecosystem of next generation public safety services using standarsized interfaces. The resulting platform ensured seamless operation regardless of the access technology, by using technology-independent interfaces and autonomous configuration and adaptation techniques through Internet Multimedia Sub-system (IMS) suite of standards. Specifically, the system was capable of connecting existing first-responder communication systems and integrating these systems into next-generation mobile networks.

The successful outcomes of the project were presented in the "Jornadas de Redes de Emergencias" (Emergency Network Days, May 2014) event organized in Bilbao and attracted remarkable interest by many public stakeholders.

The activity of the consortium in the Next Generation Public Safety Communications area has continued since the official end of the project. From the expertise gained in the project, some of the partners have joined and actively contributed to different standardisation organisations (ITU-T, ETSI and 3GPP) and emergency and public safety bodies associations (EENA112 and PSCE).

Furthermore, some of the problems and solutions envisioned by the project in 2011-2014 are currently under ongoing discussions as part of standardisation efforts (particularly in MCPTT -3GPP R13- and NG112).

PARTNERS	COUNTRY
Universidad del Pais Vasco EHU UPV (UPV/EHU)	Spain
Itelazpi SA (ITEL)	Spain
Grupo Comunicaciones y Sonido SL (CYS)	Spain
University of Plymouth (UoP)	United Kingdom
Viotech Communications SARL (VIO)	France
National Center for Scientific Research "DEMOKRITOS" (NCSRD)	Greece
Cosmote Kinites Tilepikoinonies AE (COS)	Greece

HIT-GATE / Heterogeneous Interoperable Transportable GATEway for First-Responders

© HIT-GATE

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284940
Total Cost
€5,052,636.30
EU Contribution
€3,451,257.72
Starting Date
01/02/2012
End Date
31/07/2014

Coordinator

THALES COMMUNICATIONS & SECURITY
Direction Technique
4 avenue des Louvresses
92230 Gennevilliers,
France
Contact
Vania Conan
Tel: +33 1 46 13 35 30
Fax: +33 1 46 13 26 86
E-mail:
Vania.conan@thalesgroup.com

Project objectives

The goal of HIT-GATE was to develop a generic gateway that allows communications across networks currently used by first responders in Europe. Present networks use a large number of different and incompatible technologies therefore compromising efficient coordination of combined operations (such as cross-border or crisis management). Addressing specifically this issue to answer First Responder needs, HIT-GATE supported a mix of technologies used today by organizations involved in Public-Safety, ranging from legacy-PMR, TETRA to next-generation networks. In this way, organizations may keep their existing systems and/or adopt novel technologies, since the proposed HIT-GATE solution is future proof and ensured communications interoperability between the networks (limited, of course, to the limitations in capabilities of each network). HIT-GATE also enabled communications across heterogeneous networks between first responders during operations. By connecting HIT-GATE to their networks, first responders may continue to use their current receiver equipment, communications base-stations and communications infrastructures.

Description of the work

The overall strategy adopted to successfully achieve HIT-GATE objectives and goals was as follows:

1. Implement a coherent management group capable to provide continuous oversight over several of the project areas, including, project coordination (e.g., budget, calendar, scope and risk), quality, scientific accomplishments, end-users participation and exploitation activities. Project Management activities were aligned with principles and best practices from PMBOK and CMMI.

2. Actively involve of end-users throughout the project phases, with a strong participation in initial phases (definition of user requirements and operational scenarios) and demonstration activities. Active participation of end-users ensured that HIT-GATE was a valid product and that meets their needs.

3. Adopt known and proven development processes and sub-disciplines (ISO 12207) with enough flexibility to incorporate new know-how and corrections as a result of new discoveries and/or verification activities.

4. Achieve capabilities at early stages of the project. For that, a two-iteration process was implemented:

» a. Iteration 1: stand-alone HIT-GATE capabilities and subset of IP-adaptors (covering TETRA, TETRAPOL and analog-PMR).

» b. Iteration 2: networking HIT-GATE capabilities and complete set of IP-adaptors (covering GSM/Cellular and Broadband).

5. Demonstrate actual HIT-GATE capabilities to end-users in a field-simulated scenario. A demonstration, involving FRs and their technology, will be conducted close to the end of the project.

Results

The HIT-GATE project designed, implemented, and validated through laboratory and field tests a set of solutions allowing seamless interoperability between various first responder networks (PMR radios, TETRA/TETRAPOL, GSM, 3G, LTE, and WiFi).

The developed solution enhances first responder operations in national and cross border situations by providing a transportable, deployable and autonomous gateway offering cross network services (Private/emergency/Group calls, Push-To-Talk, and enhanced messaging/location/presence services).

A HIT-GATE network was deployed at the Madrid-based Technological Institute "La Marañosa" (ITM) and at its involved European first responders' access networks to showcase the interoperability between end–users (Guardia Civil(ES), National Police(ES, PT and GR), Fire Brigade(ES)), and to exhibit the capabilities of the HIT-GATE system.

Dissemination of the project's results was conducted through our attendance at various European conferences (organised for the scientific community and end-users). A particular focus was put on targeting decision makers and PPDR end-users for dissemination.

The official website of the HIT-GATE project is maintained at: www.hit-gate.eu

PARTNERS	COUNTRY
Thales Communications & Security SAS (TCS)	France
National Center for Scientific Research "Demokritos" (DEM)	Greece
Center For Security Studies (KEMEA)	Greece
Teletel S.A. – Telecommunications and Information Technology (TELETEL)	Greece
Amper Sistemas, S.A. (AMPER)	Spain
Cluster de Seguridad y Confianza de la Comunidad de Madrid (Cluster Seguridad)	Spain
Edisoft Emresa de serviços z desenvolvimento de software (EDISOFT)	Portugal
Rohill Technologies BV (ROHILL)	The Netherlands
ITTI Sp.zo.o. (ITTI)	Poland
Thyia Tehnologije d.o.o (THYIA)	Slovenia
Rinicom Limited (RINICOM)	The United Kingdom

PPDR-TC / Public Protection Disaster Relief – Transformation Center

© PPDR-TC

RESEARCH **COMPLETED**

Information

Grant Agreement N°
313015
Total Cost
€3,962,239.68
EU Contribution
€2,890,684.20
Starting Date
01/04/2013
End Date
30/09/2015

Coordinator

EXODUS S.A. (EXO)
Business Development and Delivery
73-75 Mesogeion Av & Estias Str 1
115 26 – Athens
Greece
Contact
Dimitris Vassiliadis
Tel: +30 210 7450321
Mobile: +30 6 947566676
Fax: +30 210 7450399
E-mail: dvas@exus.co.uk
Website : www.exus.co.uk

Project objectives

Public protection disaster relief (PPDR) systems should include capabilities such as voice, real-time video and localization of responders, as well as high speed data transfer for dealing with natural and man-provoked disasters.

PPDR-TC's main objective was to provide a strategic roadmap for the evolution of future PPDR systems over the next 10-15 years. Its modular study approach included:

» Extensive data gathering from European PPDR organisations to define reference scenarios, classify current and future services, and identify candidate PPDR technologies and architectures.

» Derive technical recommendations on uniform communication for public safety agencies (broadband, TETRA, TETRAPOL networks, etc.) and secure communication over dedicated and commercial networks, plus links to other networks (LTE, 3G, WiMAX, etc.).

» Provide economic recommendations and a cost/benefit analysis to the decision makers.

Description of the work

PPDR-TC's tasks were to:

» define future PPDR reference usage scenarios

» identify services and applications that met the PPDR specific requirements

» elaborate roadmap guidelines based on selected parameters impacting PPDR market/technologies

» validate/assess the viability of options for future PPDR systems, architecture and services

» frame a 10-15 years "evolutionary" roadmap based on analysis of the technical and economical/costs reports

» promote the roadmap to standardisation bodies to build compliant business models in accordance with the existing standards

Results

The project's main outcomes are:

1. Public documents on reporting PPDR communication requirements, scenarios, and services, together with a compliance matrix that maps them to technology gaps.

2. Various software tools to assist the PPDR and the research communities:

» a. an on-line database to provide PPDR-related facts and figures within the EU, actively populated by the PPDR community itself.

» b. a software toolbox to help PPDR decision-makers determine the most suitable business model for acquiring, deploying, and upgrading a PPDR network.

» c. various network test beds, as well as updated modules for the ns-3 network simulator, all released with free software licenses to assist the technical community.

3. Techno-economical recommendations, supported by a comprehensive set of simulations and field trials

to prepare a transition roadmap from current voice-centered PPDR networks to broadband-capable communication systems.

4. Organisation of various scientific and end-user workshops to both ensure wider diffusion of project's outcome and higher impact on the PPDR community.

5. Scientific publications in international journals and conference proceedings

6. A standardisation proposal to 3GPP LTE Public-Safety Work Groups.

PARTNERS	**COUNTRY**
EXODUS S.A. (EXO)	Greece
Institute of Communication and Computer Systems (ICCS)	Greece
Thales Communications & Security SAS (TCS)	France
Rinicom Limited (RINI)	United Kingdom
TELETEL S.A. – Telecommunications and Information Technology (TELE)	Greece
AEGIS Systems Limited (AEGI)	United Kingdom
ITTI Sp.zo.o. (ITTI)	Poland
TEKEVER – Tecnologias De Informacao, S.A. (TEK)	Portugal
Universita Degli Studi Di Modena e Reggio Emilia (UNIMORE)	Italy
SC Lithuanian radio & TV centre (LRTC)	Lithuania

SECRICOM / Seamless communication for crisis

© L_ PackShot - Fotolia com

RESEARCH
COMPLETED

Information

Grant Agreement N°
218123
Total Cost
€12,424,827.51
EU Contribution
€8,606,568.20
Starting Date
01/09/2008
End Date
30/04/2012

Coordinator

QINETIQ LTD
Buckingham Gate 85
UK-SW1E 6PD London
United Kingdom
Contact
David Traynor
Tel: +44 (0) 2392 31 2750
Fax: +44 (0) 2392 31 2768
Mobile: +44 (0) 7881846076 / (0) 7590551967
E-mail: dtraynor@qinetiq.com
Website:
http://www.secricom.eu

Project objectives

In September 2006 the European Security Research Advisory Board (ESRAB) published a report setting the European security research agenda and the requirements on new communication infrastructures.

These requirements included security, dependability, enhanced connectivity, transmission of multiple formats and advanced search functions.

In response to these ESRAB requirements, the collaborative research project SECRICOM will create and demonstrate a secure communication platform for crisis management in Europe.

Solve problems of contemporary crisis communication infrastructures:

» Seamless and secure interoperability of the several hundred thousand mobile devices already deployed;

» Smooth, simple, converging interface from systems currently deployed to systems of the new SDR generation;

» Creation of pervasive and trusted communication infrastructure, bringing interconnectivity between different networks;

» Provide true collaboration and inter-working of emergency responders; and

» Seamlessly support different user traffic over different communication bearers.

Add new smart functions using distributed IT systems based on an SDR secure agents' infrastructure:

Easier instant information gathering and processing focusing on emergency responders' main task – saving lives.

Description of the work

The project work is divided into nine RTD work-packages supported by two work-packages for management and dissemination. Top innovations deal with:

» Creation of a secure wireless fault tolerant communication system for mobile devices based on a push-to-talk system;

» Secure distributed system; and

» Secure docking module – system on chip design.

These innovations will be extended by:

» IPV6 based secure communication;

» Internetwork interfaces, an interoperable, recoverable and extendable network;

» Communication infrastructure monitoring and control centre equipped with localization of actors.

Working infrastructure – the objective of the SECRICOM project will be ensured by:

» Integration of research results; and

» Demonstrator creation and presentation.

Results

The project developed its "Silentel' client application that communicate only with the server and was designed to support the operation of public safety agencies and other responders on a daily basis and in crisis situations. The system enables flexible management of groups by facilitating phone calls and instant messaging between actors using different devices and located in different countries.

SECRICOM's results manifested themselves in the system's security, quality and ability to work across multiple platforms. The system allows for resilient connectivity through a multi-bearer-router and an extendable, on-site deployable network.

In terms of security, it exploited:

» state-of-the-art encryption and user authentication software
» trusted docking station concepts
» chip-level security and a secure docking module
» threat and intrusion detectors and monitors

SECRICOM's technology is capable of functioning across multiple platforms through communication servers and gateways that are applicable for a range of modern devices and interoperable with legacy systems. The research team also worked to improve the quality of service by developing a user-friendly system with a monitoring and control system that was ready for Internet Protocol Version 6.

Three core agent types were identified and implemented:

1. information delivery agents (IDA) to send information from/to data sources

2. user communication agents (UCA) to communicate information with to human users through guided dialog, with most of these done via Silentel's "push-to-talk" devices

3. IP agents (IPA) to monitor and configure network routing devices

The project provided a proof-of-concept solution for crisis management communications and was effectively demonstrated via four live demonstrations.

PARTNERS	COUNTRY
QinetiQ Ltd	United Kingdom
Ardaco, as. (ADO)	Slovakia
Bumar sp. z o.o. (BUM)	Poland
NEXTEL S.A. (NEX)	Spain
Infineon Technologies AG (IFX)	Germany
Université du Luxembourg (Uni Lu)	Luxembourg
Ustav Informatiky, Slovenska Akademia Vied (UI SAV)	Slovakia
Technische Universität Graz (TUG)	Austria
Geothermal Anywhere, s.r.o. (SMT)	Slovakia
ITTI Sp. z o.o. (ITTI)	Poland
British Association of Public Safety Communication Officers (BAPCO)	United Kingdom
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Hitachi Europe SAS (HIT)	France
University of Patras (UOP)	Greece

CRISP / Evaluation and certification schemes for security products

Information

Grant Agreement N°
607941
Total Cost
€2,634,214.38
EU Contribution
€2,213,041.26
Starting Date
01/04/2014
Duration
36 months

Coordinator

STICHTING NEDERLANDS NORMALISATIE-INSTITUUT (NEN)
NEN Environment and Society
Vlinderweg 6
PO Box 5059
2600 GB – Delft - The Netherlands
Contact
Ronald Boon
Tel: + 31 15 269 04 12
E-mail: crisp@nen.nl
Website:
www.crispproject.eu

Project objectives

CRISP (Evaluation and Certification Schemes for Security Products) is a three-year project that aims to promote a harmonised playing field for the European security industry by developing a robust and innovative evaluation and certification methodology for security products, systems and services (PSS).

Its main objective is to enhance existing security evaluation and certification schemes by offering an evaluation methodology that integrates the security, trust, efficiency and freedom infringement assessment dimensions. The proposed scheme will be based on a new taxonomy, developed by the CRISP consortium, which encompasses a diversity of security products and services across application areas. The project will take into account the varying roles of Europe's security stakeholder community – manufacturers, regulatory and certification bodies, data protection authorities and end users – to gather their insights to help overcome the problems of acceptance that challenge current schemes. This will be achieved via dissemination, promotion, and a range of stakeholder-focused events such as workshops and a final conference.

Description of the work

Work Package 1 (WP1) will create a taxonomy of security products and systems, concepts of operations, application areas and performance levels and set out the criteria for comparing security products and systems.

WP2 will provide a historical perspective on security standards and certification in Europe and analyse the state of the art regarding security standards, certification and accreditation at Member State, regional and international levels. WP3 will identify and determine the role of different stakeholders, gauge their views on the challenges affecting security certification, and determine the requirements for a harmonised EU-wide approach.

WP4 will examine the core dimensions (security, trust, efficiency, freedom infringement) of security product certification and then define the requirements for enhancing today's evaluation and certification schemes. WP5 will present a certification methodology, policy and procedures for security products, and then test-drive, evaluate and refine the methodology, while WP6 will propose a roadmap for adopting the proposed certification scheme.

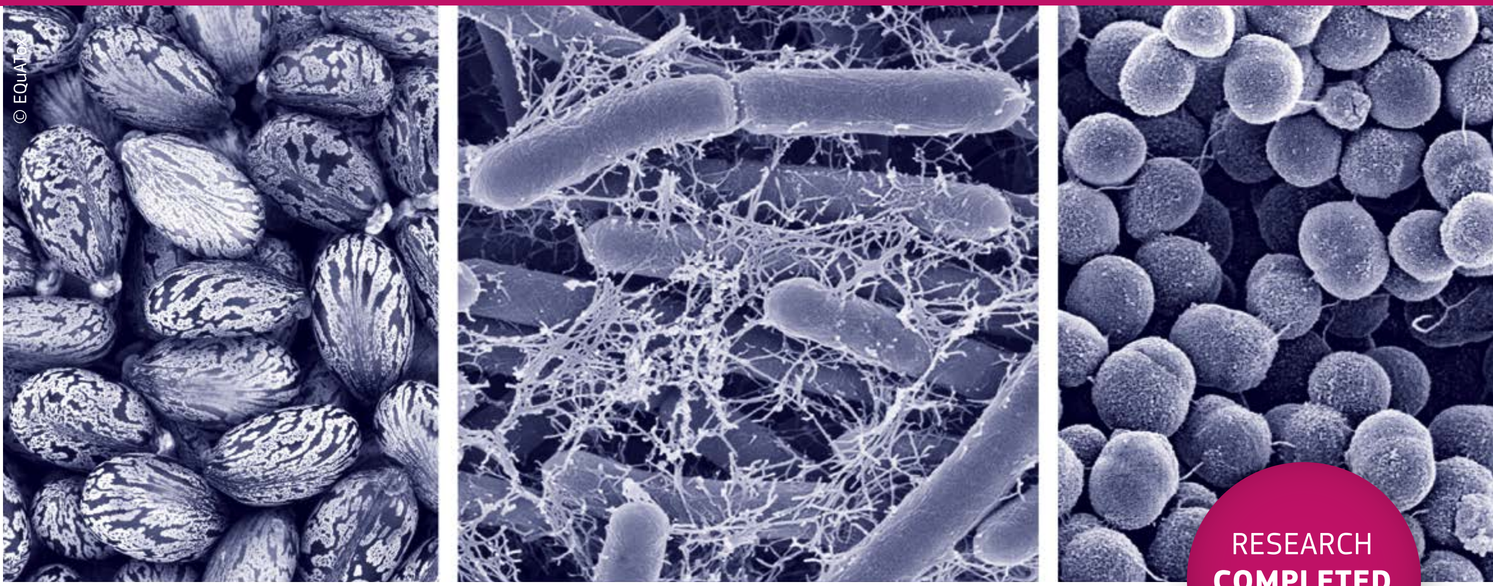
Finally, WP7 will focus on activities to enhance acceptance of the new certification measures, leaving WP8 to focus on stakeholder engagement and dissemination.

Expected results

CRISP's key deliverables will be an innovative methodology for evaluation and certification, based on the aforementioned STEFi assessment dimensions, a certification manual and a clear roadmap offering the vision and steps for implementation the CRISP scheme across Europe.

PARTNERS	COUNTRY
Stichting Nederlands Normalisatie-Instituut (NEN)	The Netherlands
Trilateral Research & Consulting LLP (TRI)	United Kingdom
Technische Universität Berlin (TUB)	Germany
IRKS Research GmbH (IRKS)	Austria
Vrije Universiteit Brussel (VUB)	Belgium
Universitat Jaume i de Castellon (UJI)	Spain
Informacijski Pooblaščenec – Information Commissioner (IP-RS)	Slovenia

EQUATOX / Establishment of Quality Assurances for the Detection of Biological Toxins of Potential Bioterrorism Risk



© EQuATox

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285120
Total Cost
€1,591,305.10
EU Contribution
€1,338,634
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

ROBERT KOCH-INSTITUT
Center for Biological Security, Microbial Toxins (ZBS3)
Nordufer 20
13353 Berlin, Germany
Contact
Dr. Brigitte G. Dorner
Tel: +49 30 18754 2500
Fax: +49 30 18754 2501
E-mail: DornerB@rki.de
Website: www.rki.de

Project objectives

The features of biological toxins like ricin, botulinum toxins, staphylococcal enterotoxins and saxitoxin place them at the interface of biological and chemical agents. They could be used for terrorist attacks on the basis of their availability, ease of preparation, their toxicity or the lack of countermeasures. Some toxins are considered among the most relevant agents in the field of bioterrorism, for which the current level of preparedness within the EU should be further improved to limit casualties in the case of an intentional release. While different technologies for toxin detection have been established, hardly any universally agreed "gold standards" are available, and reference materials, as well as proficiency tests, are generally lacking.

To address these issues EQuATox created a network of experts among the EU 28 and associated countries, focused on biological toxins and integrating experts from the security, verification, and health and food sector.

Description of the work

The main objectives of EQuATox were the following:

1. Establishment of an EU-wide network focused on the detection and identification of biological toxins which are at the interface of classical B- and C-agents, and are highly relevant in terms of a potential bio-threat attack.

2. Screening for information within Europe: who is responsible for the detection of biological toxins of potential bioterrorism risk in each Member State? 35 laboratories from 20 countries took part in the EQuATox project.

3. Generation and characterization of toxin reference materials, in case they are not readily accessible from certified sources. Four independent proficiency tests to compare diagnostic results attained by different analytical approaches (one proficiency test each on ricin, saxitoxin, staphylococcal enterotoxin B and botulinum toxins) were carried out.

4. Identification of "best practices" for the analysis of the different biological toxins based on the results obtained in the proficiency tests. Recommendations were given on how to close any gaps identified in order to minimise potential health and security risks for European citizens.

5. Exchange of information and know-how between all network partners, including information on protocols, reagents etc. in order to optimize analytical procedures within the network's laboratories.

Results

By creating a network of experts the project helped to minimize the security and health threats posed by biological toxins. Based on the status quo of toxin detection described in EQuATox, good practices and critical gaps in detection technology were identified as a foundation to harmonize and standardize detection capabilities across the EU.

PARTNERS	COUNTRY
Robert Koch-Institut (RKI)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
Institut Scientifique de Santé Publique (WIV-ISP)	Belgium
University of Helsinki, Finnish Institute for Verification of the Chemical Weapons Convention, VERIFIN (UH/VERIFIN)	Finland
French agency for food, environmental and occupational health safety (Anses)	France
Toxogen GmbH (Toxo)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Federal Department of Defence, Civil Protection and Sport - SPIEZ LABORATORY (VBS-LS)	Switzerland
ChemStat (CHS)	Switzerland

HECTOS / Harmonized Evaluation, Certification and Testing of Security Products

Information

Grant Agreement N°
606861
Total Cost
€4,690,924
EU Contribution
€3,489,016
Starting Date
01/09/2014
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)
Defence and Security, Systems and Technology
Grindsjön Research Center
147 25 Tumba, Sweden
Contact
Anneli Ehlerding
Tel: +46-855504007
Mobile: +46-709277383
E-mail:
anneli.ehlerding@foi.se
Website: www.hectos-fp7.eu

Project objectives

HECTOS objective is to support the harmonization of the European market for security products by producing a roadmap for the development of harmonized evaluation and certification of physical security products.

Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance, and similar security products are difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality. Currently, there are very few test, evaluation and certification procedures in Europe that are mutually recognized by different Member States.

Description of the work

The HECTOS project focuses on work towards harmonization of evaluation and certification schemes for physical security products.

The project studies how existing certification systems and schemes used in this and other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure. While doing so, stakeholder input and requirements are an important part, and this input is used together with the review of the current systems and schemes to develop framework for evaluation and certification schemes.

This approach is then validated by using the framework to develop schemes for two different product groups as case studies; explosives detection systems (outside of aviation security) and biometric recognition. The feedback from these studies to the development of the evaluation and certification system is an important part of the project.

The HECTOS project will also learn from and work with other initiatives working in broader areas such as security systems and cybersecurity, as well as with other standardization and certification initiatives.

Expected results

HECTOS will point out steps and actions needed for a harmonized evaluation and certification process, and evaluate elements in the certification system with respect to physical security products. The project will result in elements to a roadmap for the development of harmonized European certification systems for physical security products.

PARTNERS	COUNTRY
Totalforsvarets Forskningsinstitut (FOI)	Sweden
Morpho (MPH)	France
Iconal Technology Ltd (ICO)	United Kingdom
Frauhofer Gesellschaft zur Foerderung der Angewandten Forschungen (FhG)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
University of Warwick (UW)	United Kingdom
NPL Management Ltd (NPL)	United Kingdom
DIN Deutsches Institut fuer Normung e.v. (DIN)	Germany

SLAM / Standardisation of Laboratory analytical methods

© SLAM

Information

Grant Agreement N°
285410
Total Cost
€1,237,261.33
EU Contribution
€1,117,608.41
Starting Date
01/04/2012
Duration
24 months

Coordinator

UMEÅ UNIVERSITY
European CBRNE Center
Umeå University campus
90187 Umeå, Sweden
Contact
Dr Agneta H. Plamboeck
Tel: +46 (0) 90 10 67 34
Mobile: +46 (0) 73 211 10 00
E-mail: Agneta.plamboeck@cbrne.umu.se

Project objectives

The purpose of the present project is to propose a system view on the need for quality control (i.e. standards) on the European capability for CBRN analysis. Discussing the needs at different levels and for different purposes the SLAM project will invite representatives from relevant laboratories of the EU Member States in order to achieve a widespread understanding and approval of the differentiated needs of the CBRN analytical capability. Tutorial tabletop inter-calibration laboratory exercises will become a useful instrument in this process. The final outcome of the project is a road-map for the development of European CBRN laboratory standards.

The objectives are:

» To suggest and seek agreement between the EU 27 on differential needs for CBRN laboratory standards;

» To motivate and initiate a discussion on different CBRN networks depending on the role and requirement of laboratories;

» To engage and educate relevant laboratories in the EU 27 on inter-calibration exercises for CBRN analytical laboratories as requested in the call;

» To produce a road-map for correct and efficient standardisation of the European CBRN laboratory capability as requested in the call.

Description of the work

The SLAM project is a two-year project that is broken down into six work packages (WP). WP0 contains the management and coordination efforts of this project, which also includes arranging a kick-off meeting and a workshop for WP1-WP3 to facilitate the harmonisation process between those work packages.

WP1, WP2 and WP3 cover Chemical Analysis, Biological Analysis and Radio Nuclear Analysis, respectively and will together, in coordination, generate an overview of European laboratories analysing CBRN substances and background materials like CBRN threat agents, existing procedures and protocols relevant for the threat agents. This also involves an overview and comparison of different standard regimes for the full analytical cycle, i.e. from sampling to the interpretation of data. Transportation regulations, guidelines and systems in place among European laboratories are also part of the background material needed for the final road-map.

WP4 will illustrate relevant cases of mixed or unknown samples. An inventory will be made of different methods that have been developed and applied for unknown samples suspected to contain highly toxic and/or highly infectious and/or dangerous radioactive material. WP4 will depend on input from WP1–WP3 and thereafter similarly to these WPs perform a full cycle analysis, from sampling to interpretation of data.

WP5 will collate inventories of existing initiatives (regimes), and their protocols and methods from WP1-4 and develop a workshop programme based on that information. WP5 will promote the interaction with neighbouring Member States and will, through a workshop with co-beneficiaries and stakeholders, analyse the outputs of WP1 to 4 and discuss and propose the most suitable standard operating procedures for Member States reference laboratories to follow for CBRN incidents. This involves agreeing on the best practices as well as issues relevant to surveillance, alert and response at local and national level. The outputs of the workshop will in turn be tested through a Round Robin inter-calibration exercise.

Finally, WP6 will use all available inputs, internal (WP1 to WP4), external and WP5, to suggest a road-map for needs and means to achieve systematic standardisation of European CBRN analytical capability.

Expected results

Enhancing the competence in Member States in the development of common methods, procedures and protocols for the detection, analysis and identification of CBRN substances allowing for a significant comparison of results from different laboratories and operators within Europe.

A road-map suggesting methods of choice and processes and means to implement necessary standards to CBRN analysis will be presented and reported. A functional standardisation of CBRN analysis at the necessary level of stringency will become an important component of a Europe more resilient to CBRN incidents.

PARTNERS	COUNTRY
Umeå University (UmU)	Sweden
Commissariat à l’énergie atomique et aux énergies alternatives (CEA)	France
Forsvarets forskningsinstitutt (FFI)	Norway
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Health Protection Agency (HPA)	United Kingdom
Robert Koch-Institut (RKI)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands

ANVIL / Analysis of Civil Security Systems in Europe

© Larissa Belova - iStock

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284678
Total Cost
€2,202,702.60
EU Contribution
€2,009,228
Starting Date
01/03/2012
End Date
28/02/2014

Coordinator

RESEARCH MANAGEMENT AS
Fortunalia 14
7057 Jonsvatnet, Norway
Contact
James P. Rydock
Tel: +47 7391 9307
Mobile: +47 9590 7562
Fax: +47 7391 8200
E-mail:
jrydock@researchmgt.com
Website:
www.anvil-project.net

Project objectives

The ANVIL project has six main objectives:

» To pinpoint essential similarities and differences between civil security systems across Europe, through mapping and comparing, especially with regard to relevant cultural phenomena and legal determinations;

» To study a representative number of security regional architectures in a comparative analysis regarding the sharing of responsibilities between public and private bodies and the role that citizens play in regional security architectures;

» To determine whether these systems are efficient and effective in protecting their citizens (i.e. to determine what works and what doesn't work in existing civil security systems);

» To provide advice about what changes or modifications could result in improvements to the security situation in regions or countries where this is desired by EU policymakers;

» To ensure that the project gives EU-added value to policy stakeholders;

» To link to future research needs where possible.

Description of the work

To reach these objectives, ANVIL has formulated three sub-strategies (encompassing the first five of in all seven work packages) for each project pillar: design, mapping and analysis, each of which is informed by policy stakeholders. Each pillar is essential to the outcome of the project.

» *WP1: Clever design*

The strategy is to organize a focused and intense design phase at the start. Existing literature will be used to formulate a framework for design, which will be translated into a "mapping manual". This will involve experts with different backgrounds (civil security, public administration, crisis management) to make sure the proposed mapping method is feasible in all selected regions;

» *WPs 2 and 3: Accurate and efficient mapping*

The strategy will be to identify what the best sources of existing data are and how we can access these. ANVIL will make use of our extended network (of both practitioners and academics) to identify these data sources. In addition, it is important that all partners collect data in the same way to ensure comparability (which is necessary for the analytical phase). Part of this strategy is to organize several meetings (in person and using video networking) to discuss and compare data collection processes, and jointly devise solutions for emerging data-related problems;

» *WPs 4 and 5: EU-focused analysis, dissemination and impact*

ANVIL will draw on previous research into the growing role of the EU and the existing constraints on developing EU crisis and disaster management capacities. This will provide a clear overview of the needs at the EU level. In addition, ANVIL will create a policy stakeholder group in WP5 to inform and provide feedback to our work, and who can ultimately validate our findings and function as an additional avenue for dissemination of ANVIL results;

» *Finally, WP6 is for overall dissemination, both during and after the project, and WP7 is for project management.*

Results

Current European civil security systems are heavily localised, with complex institutional arrangements and varying degrees of centralization. There is a strong use of voluntary organizations in most countries, however, the role of the private sector is limited, with outsourcing of core tasks in crisis management not a major trend. Civil security systems are generally perceived as effective. In terms of efficiency, costs are often dispersed and therefore total national civil security budgets are largely unknown. Despite this uncertainty, a majority of citizens appear to have a positive attitude towards civil security and feel generally safe, though levels of support differ somewhat geographically. There is a well-developed framework for external and cross-border assistance, but it is used only reluctantly by countries needing help during domestic crises. Looking at national civil security in the EU context, there is a basic acceptance, but low visibility of the EU as a coordinator and facilitator of joint responses to disasters occurring inside or outside Europe. Finally, there is a limited role for regional organizations, which are seen to be weakly institutionalised, have limited competences in crisis and emergency management and depend on often reluctant member states for financial resources and operational capacities. Results from the ANVIL project are appearing in international peer reviewed publications such as the Journal of Risk Research, as well as in a forthcoming book title 'EU civil security governance: Diversity and cooperation in crisis and disaster management' to be published by Pelgrave Macmillan.

PARTNERS	COUNTRY
Research Management AS (Resman)	Norway
Universiteit Utrecht (Utrecht)	The Netherlands
Ideella Foreningar Utrikespolitiskainstitutet, Informationsavd (UI)	Sweden
University of Essex (UEssex)	United Kingdom
Institut za Medunarodne Odnose (IMO)	Croatia
Hellenberg Oy (HI)	Finland
Istituto Affari Internazionali (I.A.I.)	Italy
Institut fur Friedenforschung und Sicherhetspolitik an der Universitat Hamburg (IFSH)	Germany
Försvarshögskolan, Swedish National Defence College (SNDC)	Sweden
Univeristet u Beogradu, Fakultet Bezbednosti (FB)	Serbia
Fondation pour la Recherche Strategique (FRS)	France
Uniwersytet im. Adama Mickiewicza w Poznaniu (AMU)	Poland

ATHENA

Information

Grant Agreement N°
613220
Total Cost
€5,436,445.04
EU Contribution
€2,631,592.00
Starting Date
01/12/2013
Duration
36 months

Coordinator

POLICE AND CRIME COMMISSIONER FOR WEST YORKSHIRE (WYP)
West Yorkshire for Innovation (WyFi)
Laburnum Road
PO Box 9
WF1 3QP – Wakefield
United Kingdom
Contact
Jessica Gibson
Tel: +44 (0) 1924 292207
Mobile:
+44 (0) 7515 573789
E-mail: jessica.gibson@westyorkshire.pnn.police.uk
Website:
http://www.westyorkshire.police.uk/athena

Project objectives

The public are under-utilised as crisis responders; often first on the scene, and vastly outnumbering emergency responders, they are creative and resourceful.

In a crisis, the public self-organise into groups, adapt quickly, emerge as leaders and experts, and perform countless life-saving actions. Though to do this they are increasingly reliant upon the use of new media. Therefore ATHENA will:

» help by joining their conversations and adding an enabling voice.

» give them the information they need, in a way they can understand.

» assist them in targeting their actions; directing them to the places they need to be and away from danger.

» identify emergent behaviour that is beneficial, and then provide support with law enforcement agency (LEA) resources to develop that behaviour.

Description of the work

The goal of the ATHENA project is to deliver two major outputs that will enable and encourage users of new media to contribute to the safety of citizens in crisis situations, and in search and rescue actions.

The ATHENA project places considerable importance on the involvement of end-users, and the project will be developed through an iterative process involving close working between technical and end-user partners.

Expected results

- A set of best practice guidelines for LEAs, first responders and citizens for the use of new media, supporting tools and technologies in crisis situations
- A suite of prototype software tools to enhance the ability of LEAs, first responders an00d citizens in their use of new media in crisis situations

ATHENA will provide the emergency services with new real-time intelligence from crowd-sourced information, assisting in decision making and making search and rescue more efficient.

ATHENA will create a fundamental and permanent shift in the way crisis situations are managed; helping the public become a part of the crisis team.

It will use social media and smart mobile devices as part of a shared and interoperable two-way communication platform. By developing an orchestrated cycle of data, information and knowledge, ATHENA will empower both the public and emergency services with the intelligence they need in dealing with a crisis.

PARTNERS	COUNTRY
Police and Crime Commissioner for West Yorkshire (WYP)	United Kingdom
International Organization for Migration (IOM)	Begium
Sheffield Hallam University (SHU)	United Kingdom
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FKIE)	Germany
SAS Software Limited (SAS)	United Kingdom
Municipality of Ljubljana (MOL)	Slovenia
Thales Nederland BV (Thales-NL)	The Netherlands
University Of Virginia (UVA)	United States
Försvarshögskolan, Swedish National Defence College (SNDC)	Sweden
EPAM Systems (Nordic) AB (EPAM)	Sweden
Izmir Buyuksehir Belediyesi (IBB)	Turkey
Research In Motion Limited (RIM)	Canada
Epidemico Ltd (EMCO)	Ireland

COSMIC / The Contribution of Social Media in Crisis Management

© COSMIC

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312737
Total Cost
€1,228,896
EU Contribution
€997,040.20
Starting Date
01/04/2013
End Date
31/03/2015

Coordinator

EUROPEAN DYNAMICS ADVANCED SYSTEMS OF TELECOMMUNICATIONS INFORMATICS AND TELEMATICS SA (ED)
Department of Research and Development
Kifissias 209
15124, Marousi, Greece
Contact
Ioannis Kotsiopoulos
Tel: +30 210 8094500
Fax: +30 210 8094508
E-mail: ioannis.kotsiopoulos@eurodyn.com
Website: www.eurodyn.com

Project objectives

The major premise of the COSMIC project was that the experience from recent emergency situations was indicative of a need to instigate collaboration efforts and exchange of ideas and know-how across national borders and among different stakeholders. Extant research on information technology design for emergency purposes indicated that the conventional command and control approach to emergency response, which favoured a hierarchical approach to communication structures, should have been replaced by one which relied on decentralised structures and prioritized social interactions among different stakeholders. A suitable information technology design should be able to enhance informal interactions in dispersed networks (and localities), while being flexible enough to accommodate situational and locational variation (and make sense of such variation) so as to enhance information sharing. This could result in adding visibility, permanence and sensibility to ephemeral information shared over those dispersed networks.

The project bridged the gap between different stakeholders with various and sometimes conflicting needs, and complemented existing EC and other international projects by integrating the know-how derived from them and disseminating it to a wide network of interested parties. In particular, the project aspired to:

- explore new and emerging communication technologies and applications and provide insight into the most effective ways to utilise this media for the safety and security of citizens in crisis situations
- assist better communication and better information gathering for authorities and first responders
- examine the potential roles and ethics for citizen participation in emergency response
- produce guidelines to assist authorities and first responders in deploying new and emerging communication technologies and applications for protecting citizens in crisis situations

Description of the work

COSMIC achieved its objectives via these lines of action:

- Studies on crises, the main stakeholders (including the public) and the communication technologies they currently use. Emerging technologies were investigated and stakeholders informed about available innovative forms of communication.
- Strategic support: COSMIC analysed the stakeholders in crises and offered ways to achieve sustainable collaboration.
- Awareness raising and dissemination: COSMIC communicated progress made and promoted its vision for crisis management.

Results

COSMIC highlighted the use of citizen-generated data via social media as an indicator of where specific emergency resources or search and rescue operations are necessary. This can assist decision makers, law enforcement officers and first responders in using new technology for communication and information gathering. It can also positively influence citizens' preparedness by showing how trusted information can be communicated to the public and, in reverse, how citizens can assist the authorities and one another via own-produced relevant supplementary information.

To this end, the project offered expert-validated advice and guidelines on how new media technologies and applications can best be used for rapid response to crises. A series of workshops and a final conference helped validate those guidelines and verified their usefulness and relevance to the needs of a variety of stakeholders. On a wider perspective, the findings of COSMIC offer value to other EU projects, governments, and researchers regarding possible new areas in policy studies and research in relation to social media and emergency response.

PARTNERS	COUNTRY
European Dynamics, Advanced Systems of Telecommunications Informatics and Telematics SA (ED)	Greece
Trilateral Research & Consulting LLP (TRI)	United Kingdom
Radboud University Nijmegen – Crisislab (RUN)	The Netherlands
KOC University (KU)	Turkey
Elliniki Omada Diasosis Somateio (HRT)	Greece
Public Safety Communication Europe Forum AISBL (PSCE)	Belgium
Veiligheidsregio Zuid-Holland Zuid (VZHZ)	The Netherlands

CPSI / Changing perceptions of security and interventions

© Zoe - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217881
Total Cost
€2,712,487
EU Contribution
€2,165,637
Starting Date
01/04/2008
End Date
31/03/2010

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK
Defence, Security and Safety
Kampweg 5
P.O. Box 23
3769 ZG Soesterberg
The Netherlands
Contact
Dr. Heather J. Griffioen-Young
Tel: +31 346 356 378
Mobile: +31 6 2246 1065
Fax: +31 346 353 977
E-mail:
heather.griffioen@tno.nl
Website: www.cpsi-fp7.eu

Project objectives

CPSI – Changing Perceptions on Security and Interventions –aims to create a methodology to collect, quantify, organize, query, analyse, interpret and monitor data on actual and perceived security, determinants and mediators.

The four main objectives of the project were to:

» Develop a conceptual model of actual and perceived security and their determinants,

» Design a methodology to register and process security-related data,

» Develop a data warehouse to store amassed data and

» Carry out an empirical proof-of-principle study to test the model, methodology and data warehouse.

In CPSI we focus on security related to "everyday" crime, such as theft, assault and vandalism. The CPSI methodology, however, can be applied to other areas of security as well, such as terrorism or financial security.

The main deliverables include a detailed description of the methodology, data warehouse, and empirical study. In addition, we will develop an "instruction manual" describing how an end-user can implement the CPSI methodology.

Description of the work

The core of CPSI is psychological in nature. The conceptual model is based on factors related to each individual which determine perceived security, such as demographic characteristics, personality traits and lifestyle, and history of victimization. The model was developed using literature review and morphological analysis, a structured group-discussion technique used to give concrete form to multidimensional non-quantifiable problem spaces.

Overall, however, CPSI takes an explicitly multidisciplinary approach. Aside from psychological aspects, we believe that security also has strong links with sociological factors and national culture. Specifically we will examine the relationship between public opinion and the media, in addition to an analysis of national security cultures across Europe.

In this project we will test if it is possible to answer relevant security-related questions from the field using the CPSI methodology. Example questions include:

» How does actual security relate to the subjective perception of security?

» What are the levels of perceived and actual security in specific locations?

» Which interventions work where?

» How does security change over time?

In an empirical study taking place in Amsterdam, The Netherlands, we are filling a data warehouse with data on registered crimes, results from a survey on perceived security, and analyses of media expressions concerning crimes and security in general. From this information, we can test the validity of the conceptual model and the applicability of the methodology.

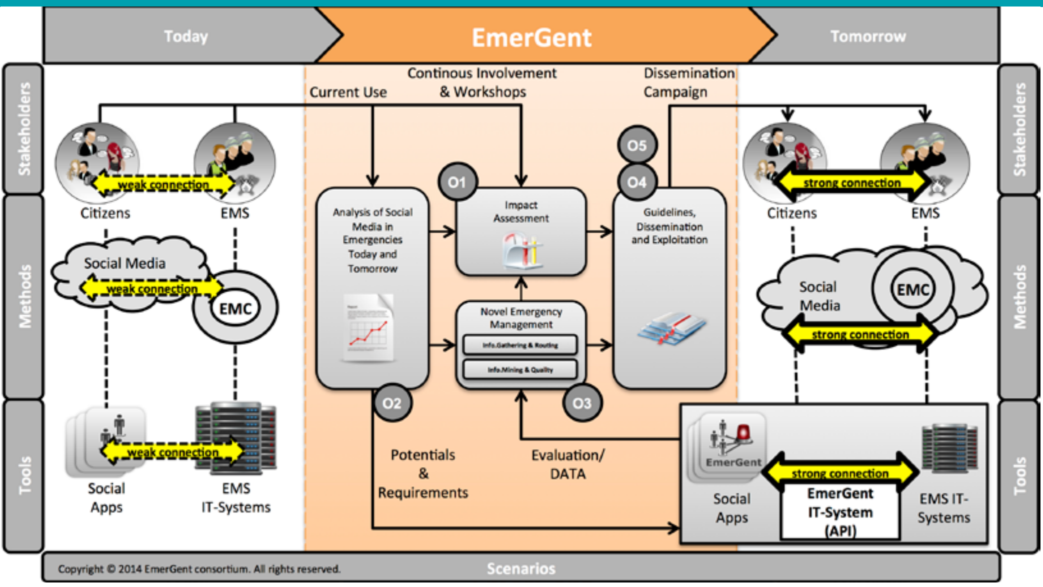
The widespread implementation of monitoring tools such as the CPSI methodology brings with it ethical and legal risks related to – among other things – citizens' privacy and the use of data. In CPSI we take these issues seriously and are employing a technique known as ethical parallel research in which ethical and legal issues are addressed as they arise during the execution of the project.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Totalförsvarets Forskningsinstitut (FOI)	Sweden
University of Kent (UniKent)	United Kingdom
Sogeti Nederland B.V. (Sogeti)	The Netherlands
Temis S.A. (Temis)	France
European Commission - Joint Research Centre (JRC)	Belgium
WWEDU World Wide Education GmbH (CESS)	Austria
Ministerie van Volksgezondheid, Welzijn en Sport (SCP)	The Netherlands
VLC Projects B.V. (VLC)	The Netherlands
Sigmund Freud Privatuniversitat Wien GmbH (SFPUW)	Austria

EmerGent / Emergency Management in Social Media Generation



Information

Grant Agreement N°
608352
Total Cost
€4,153,322
EU Contribution
€3,331,184
Starting Date
01/04/2014
Duration
36 months

Coordinator

UNIVERSITY OF PADERBORN (UPB)
COMPUTER APPLICATION AND INTEGRATION IN DESIGN AND PLANNING (C.I.K.)
Pohlweg 47-49
33098 Paderborn, Germany
Contact
Therese Friberg
Tel: +49 (0)5251 60 5474
Mobile:
+49 (0)174 3427984
Fax: +49 (0)5251 60 3206
E-mail: friberg@cik.upb.de
Website:
http://www.fp7-emergent.eu

Project objectives

Social media is a serious and fast growing phenomenon for creating and maintaining social links. The convergence of social networking and mobile media technology is changing the way people communicate, and access or share information, especially during emergency or crisis situations. Wherever emergencies or crises occur, ad-hoc communities are built through existing social media channels. But these communities are often unconnected or weakly connected to the emergency management services (EMS) and the corresponding emergency management processes.

The overall objective of EmerGent is to understand the positive and negative impacts of social media in emergencies to:

1. enhance objective and perceived safety and security of citizens before, during and after emergencies,

2. strengthen the role of European companies that supply services and products related to EmerGent's results.

Description of the work

Today the "emergency management cycle" (EMC) with its phases does not capture social media with its highly valuable information. Although existing social apps (e. g. for mobile devices) are sometimes used by citizens to share their observations and feelings, these are only weakly connected to existing EMS systems. To achieve the goal of EmerGent the consortium has developed a strong research oriented methodology.

Within the "Analysis of Social Media in Emergencies Today and Tomorrow", EmerGent investigates the current use of social media during emergencies, and the future potential for citizens and EMS involvement within all phases when using social media. It also performs an analysis of the methods and tools for citizens and EMS to integrate on a technical level.

The results of the analysis are used to assess the impact of social media in emergencies for citizens and EMS through continuous citizen and EMS involvement via social media and workshops. This includes users who will participate over the long-term as well as development of basic infrastructures to maintain and support relationship via social media. The methodology of the impact assessment consists of case studies, analyses of past emergencies where social media played a crucial role, workshops with experts and deep-content analysis of feelings and reactions on both sides.

To handle the vast amount of valuable and distributed information, methods for information mining and information quality are developed to classify and rate the available and provided data from users. Information gathering and information routing, including the development of new social apps, will be done as part of the "Novel Emergency Management". The development of new social apps will obtain and provide visualisations of the most relevant information (as assessed by EmerGent) integrated with several social network providers.

Expected results

All analysis and impact assessment results lead to the creation of guidelines. These guidelines enable EMS and all other involved stakeholders to understand

» the benefits of social media and

» its integration into their process on different levels (conceptual & technical).

The insights and results from the studies are incorporated into these guidelines via

» the collection and presentation of Information,

» the analysis of social media in emergencies and

» the development of Information Mining and Information Quality methods,

An IT-system for the "Novel Emergency Management in Social Media Generation" will be developed.

PARTNERS	COUNTRY
University of Paderborn (UPB)	Germany
Intelligence for Environment and Security - IES Solutions (IES)	Italy
Oxford Computer Consultants (OCC)	United Kingdom
University of Siegen (USI)	Germany
The Tavistock Institute of Human Relations (TIHR)	United Kingdom
Western Norway Research Institute (WNRI)	Norway
Federation of the European Union Fire Officer Associations (FEU)	Luxembourg
European Emergency Number Association (EENA)	Belgium
City of Dortmund, Fire Department, Institute of Fire Service and Rescue Technology (FDDO)	Germany
Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej im. Jozefa Tuliszkowskiego Panstwowy Instytut Badawczy (CNBOP-PIB)	Poland

IMPACT Europe / Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe

Information

Grant Agreement N°
312235
Total Cost
€3,534,308.74
EU Contribution
€2,801,537.10
Starting Date
01/2014
Duration
42 months

Coordinator

RAND EUROPE (RAND)
Westbrook Centre, Milton Road
Cambridge, UK CB4 1YG
Contact
Ines von Behr
Tel: +32 2669 2408
E-mail: ivonbehr@rand.org
Website:
http://impacteurope.eu/

Project objectives

The key motivation behind IMPACT Europe is to develop an evaluation toolkit to enable evaluators, policy-makers, frontline workers and academics working in the field of violent radicalisation to answer the three questions that limit the effectiveness of their work:

» How effective are various programmes at tackling violent radicalisation?

» What are the best practices in tackling violent radicalisation?

» How does this inform our knowledge and understanding of violent radicalisation?

Description of the work

IMPACT Europe will develop a toolkit to help professionals in the public and voluntary sectors design, implement and evaluate how their programmes (whether policies and interventions) tackle violent radicalisation. The toolkit will also help professionals go beyond the evaluation of a single project by integrating best practices into the design and implementation of future programmes.

Expected results

The IMPACT Europe evaluation toolkit will be composed of four elements:

1. A standardised methodology to provide professionals with a tool to conduct robust evaluations;

2. An evaluation results database to allow professionals to analyse these results over time, identify best practices and develop a more informed understanding of violent radicalisation;

3. A training course (including a train-the-trainer component), to build professionals' capacity to design, carry out and learn from appropriate evaluations;

4. A training manual to provide easy reference for professionals using the toolkit.

PARTNERS	COUNTRY
RAND Europe (RAND)	United Kingdom
Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)	The Netherlands
Fondation pour la Recherche Stratégique (FRS)	France
Studio CEVAS (CEVAS)	Italy
ITTI (ITTI)	Poland
University of Milan Bicocca (UNIMIB)	Italy
Hogeschool Utrecht (HU)	The Netherlands
Verwey-Jonker Instituut (VJI)	The Netherlands
Intelligence in Science (ISC)	Belgium
International Security and Counter-terrorism Academy (ISCA)	Israel
Nationale Politie (DNP)	The Netherlands
Radical Middle Way (RMW)	United Kingdom

iSAR+ / Online and Mobile Communications for Crisis Response and Search and Rescue

© ISAR+

RESEARCH
COMPLETED

Information

Grant Agreement N°
312850
Total Cost
€5,225,062
EU Contribution
€3,987,991.65
Starting Date
01/01/2013
End Date
30/06/2015

Coordinator

TEKEVER - TECNOLOGIAS DE INFORMACAO, S.A. (TEKEVER)
Rua das Musas 3.30
1990-113 Lisboa
Portugal
Contact
Pedro Sinogas
Tel: +351 213 304 300
Mobile: +351 213 304 300
Fax: +351 213 304 301
E-mail: pedro.sinogas@tekever.com
Website: isar.i112.eu

Project objectives

Citizens can function as the “in-situ first sensors” now that they are empowered by new communication media such as mobile phones with cameras and internet-based applications that connect to social media platforms. However their added-value involvement in crisis response efforts is often disregarded by PPDRs when they are developing situational awareness during emergencies.

The iSAR+ project aimed to research and develop guidelines and an associated platform that, in emergencies or crises, enabled citizens using new mobile and online technologies to actively participate in the response effort. This could be done through bi-directional provision, dissemination, or sharing and retrieval of information essential for critical PPDR intervention, in disaster relief scenarios.

In particular, iSAR+ aimed to achieve the following objectives:

» Develop effective guidelines to enable the new media users to contribute to crisis response efforts and search and rescue actions;
» Recommend the most effective and efficient ways for citizens to contribute to crisis response and search and rescue actions;
» Design iSAR+ to suit PPDR organisations;
» Design iSAR+ to suit citizens;
» Design iSAR+ accordingly to the EU ethical and legal framework;
» Design an innovative iSAR+ technological platform for experimentation and validation purposes, which gets the most out of mobile technology and social media;
» Define a stepwise process for the adoption of online social media and mobile technologies in PPDR organisations;
» Integrate iSAR+ in the existing PPDR toolkit for crises;
» Establish a wide European community of end-users, interested in researching the challenges of using social media for supporting disaster relief operations.

Description of the work

In order to address the project objectives iSAR+ reached the conclusion that the answer is not solely technological. Useful technology is already available; the real problem is mostly related to the question of how to use existing technology so that PPDRs and citizens may mutually trust the channels of bi-directional social media communication.

Therefore the iSAR+ approach, code named the THEO approach, was based on a multi-dimensional analysis that encompasses the technological, human, ethical, legal, and the organisational perspectives of the problem. In iSAR+ each THEO dimension was assigned a work package to thoroughly study the project’s challenges under its respective perspective.

The THEO work packages were executed concurrently and the results are merged to form one unified vision. This process was repeated through several iterations. At the end of each iteration, the iSAR+ end user community met at showcases and workshops, to review the achieved results. The end-user feedback was then incorporated into the next iteration of the project, thus promoting the establishment of an end-user driven solution by the time the final project iteration has been achieved.

Results

iSAR+ successfully achieved its goals of developing a technological platform for use of mobile technology and social media tools by PPDR organisations and citizens, proposing guidelines, and developing a roadmap for the adoption of said tools.

iSAR+ developed organisational (33), technological (30), ethical (22), and human factors (20) recommendations for the adoption and use of social media and mobile technologies in crisis management. These were aggregated into 28 integrated recommendations. These included: development of a human-centred CONOPS to be implemented in crisis mode and non-crisis mode; the use of iSAR+ as a means of inter-team, inter-agency communication and coordination; creation of clear ethical guidelines for use of the system; and the development of a citizen education plan.

Furthermore, iSAR+ developed a platform integrating the following modules:

- the iSAR+ Portal Software (IPS);
- myPublicAlerts (mPA);
- optional 3rd party modules;
- SMM Crawler (Social Media Monitoring Crawler);
- Information Mining and Synthesis (IMS);
- Text Analysis Tweet Locator (TAT2);
- Multi-Language Text Analytics (MTA).

The iSAR+ tools and modules underwent two iterations and were validated by real end-users during showcases in France and Finland.

PARTNERS	COUNTRY
Tekever - Tecnologias de Informacão, S.A. (TEKEVER)	Portugal
Bridge 129 Spa - Safety and Security (BRIDGE129)	Italy
Centre for Science, Society and Citizenship (CSSC)	Italy
Deveryware (DEV)	France
Pelastusopisto, Emergency Services College (ESC)	Finland
Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)	Germany
ITTI Sp.zo.o. (ITTI)	Poland
Helse Bergen Hf*Haukeland University Hospital (HUS)	Norway
Kuopion Kaupunki (PSPELA)	Finland
Police and Crime Commissioner for North Yorkshire (PCCNY)	United Kingdom
Pole Pilote De Securite Locale (PSSL)	France
Poliisiammattikorkeakoulu (POLAMK)	Finland
The Provost, Fellows, Foundation Scholars & The Other Members Of Board Of The College Of The Holy & Undivided Trinity Of Queen Elizabeth Near Dublin (TCD)	Ireland
Thales Communications & Security SAS (THALES)	France
Itä-Suomen Yliopisto (UEF)	Finland
Zanasi Alessandro Srl (ZANASI)	Italy

PARIS / PrivAcy pReserving Infrastructure for Surveillance

© PARIS

Information

Grant Agreement N°
312504
Total Cost
€4,771,052
EU Contribution
€3,490,491
Starting Date
01/01/2013
Duration
36 months

Coordinator

TRIALOG
25 rue du Général Foy
75008 Paris, France
Contact
Antonio Kung
Tel: +33 1 44 70 61 00
Fax: +33 1 44 70 05 91
E-mail:
antonio.kung@trialog.com
Website:
http://www.paris-project.org

Project objectives

PARIS will define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens to privacy, justice, and freedom. It will take into account the evolving nature of such rights such as aspects that are acceptable today but might not be in the future, as well as the social and ethical nature of those rights, e.g. the variation of the perception of rights in different countries.

Description of the work

The methodological approach will be based on two pillars: 1) a theoretical framework for balancing surveillance with the protection of privacy and data which fully integrates the concept of accountability, and 2) an associated process for the design of surveillance systems which takes into account privacy and accountability from the start, i.e. privacy-by-design and accountability-by-design.

Expected results

First a generic framework will be defined for SALT: Socio-ethicAl Legal Technological aspects. Based on the SALT framework, guidelines will be provided to define specialized conceptual frameworks, e.g. for a given country. Examples of SALT frameworks will be provided. The interplay of SALT frameworks and the exchange of surveillance data will be analysed.

A framework management tool will be developed in order to 1) allow for the creation and editing of a conceptual framework, and 2) subsequently act as a reference for surveillance system designers. A SALT compliant design process will be defined so that the balance of surveillance and privacy according to the specialised framework will be ensured throughout the process.

Two use cases will be demonstrated, one based on video search technology which focuses on archived data, and the other based on biometrics technology which focuses on embedded systems sensor data. The two use cases will use different SALT frameworks. The resulting methodology will be promoted through associations and standardisation bodies.

PARTNERS	COUNTRY
Trialog	France
Austrian Institute of Technology GmbH (AIT)	Austria
Institut National de Recherche en Informatique et en Automatique (INRIA)	France
Katholieke Universiteit Leuven (KUL)	Belgium
Universidad de Malaga (UMA)	Spain
Université de Namur	Belgium
Thales Communications & Security SA	France
Visual Tools SA	Spain

PRIME / Preventing, Interdicting and Mitigating Extremist events: Defending against lone actor extremism

Information

Grant Agreement N°
608354
Total Cost
€3,590,953.80
EU Contribution
€2,842,878.45
Starting Date
01/05/2014
Duration
36 months

Coordinator

UNIVERSITY COLLEGE LONDON (UCL)
UCL DEPARTMENT OF SECURITY AND CRIME SCIENCE
35 TAVISTOCK SQUARE
WC1H 9EZ, LONDON,
ENGLAND
Contact
DR NOEMIE BOUHANA
Tel: +44 2031 083022
Mobile: +44 7914 663166
Fax: +44 2031 083088
E-mail: n.bouhana@ucl.ac.uk
Website: www.fp7-prime.eu

Project objectives

The PRIME project will deliver a knowledge-base to inform the design of measures to defend against lone actor extremism, by achieving the following objectives:

1. Characterising the risk posed by lone actor extremists, and the context in which measures to defend against lone actor extremist events (LAEEs) may be implemented;
2. Producing a cross-level risk analysis framework within which to articulate the key factors and processes implicated in LAEEs, across all stages of the event (radicalisation, attack preparation, attack).
3. Translating the risk analysis framework into a meta-script of lone actor extremist events.
4. Producing an integrated, cross-level script of LAEEs, and identifying categories of intervention points or 'pinch points'.
5. Delivering a portfolio of requirements for the design of measures for the prevention, interdiction and mitigation of lone actor extremist events across levels of intervention. 6): Delivering a portfolio of requirements for communication measures directed at a diverse audience at each stage of the script, in coordination with the portfolio of counter-measures.

Description of the work

The PRIME work plan is organised in four phases.

Phase 1: "Framework": we will carry out the necessary analysis to identify the contextual factors which may impact the selection, design, adoption and/or implementation of counter-measures to defend against lone actor extremism, establish the data requirements necessary to produce a cross-level model of these events, and develop the formal scripting approach. Work carried out in the first phase ensures that the empirical work taking place in the next phase proceeds from a systematic, formalised, and clear conceptual and methodological basis.

Phase 2: "Modelling": we will create cross-level subscripts for each event stage (radicalisation, attack preparation, attack) from collected data, integrate the subscripts into a single event model, and identify categories of intervention points or 'pinch points', where intervention has the potential to disrupt lone actor extremist events. This will lead to a robust, empirically-supported, valid event model and a set of transparently-derived intervention points.

Phase 3: "Response": review existing counter- and communication measures against lone actor extremism, formulate requirements for new or refined measures based on the categories of 'pinch points' previously identified, and validate the requirements portfolios. The work carried out in the third phase is necessary to ensure the project delivers a clear set of measure requirements, formulated in such a way as to be easily conveyed to end-users.

Phase 4: "Dissemination": we will disseminate the project's scientific outputs to interested parties and promote the adoption of the script-based methodology and counter-measure requirements among stakeholders. The work carried out in the last phase will be done in a manner which supports and encourages understanding and adoption. The project makes specific provision to provide end-users with training in the operation of key deliverables.

Expected results

Through the production of counter-measure portfolios and communication measure requirements, PRIME will inform the selection, design and implementation of technologies for the prevention, interdiction and mitigation of lone actor extremist events. It intends to deliver a decision-support tool for a range of end-users – national and local, from law enforcement agencies to civilian organisations – whose remit includes the prevention, interdiction or mitigation of lone actor extremism, and who are responsible for choosing what measures to implement in their particular context.

PARTNERS	COUNTRY
European Commission (EC)	Belgium
University College London (UCL)	United Kingdom
King’s College London (KCL)	United Kingdom
Uniwersytet Warszawski (UoW)	Poland
Aarhus Universitet (AaU)	Denmark
The Hebrew University of Jerusalem (HUJ)	Israel
Universiteit Leiden (UoL)	The Netherlands

RECOBIA / Reduction of Cognitive BIAses in Intelligence Analysis

© Yury Kuzmin - istockphoto

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285010
Total Cost
€4,445,420.60
EU Contribution
€3,215,454.00
Starting Date
01/02/2012
End Date
31/01/2015

Coordinator

COMPAGNIE EUROPÉENNE D’INTELLIGENCE STRATÉGIQUE (CEIS)
Boulevard Charlemagne, 42
1000 Brussels
Contact
Axel Dyèvre
Tel: +32 2 646 70 43
E-mail: adyevre@ceis.eu
Website: www.recobia.eu

Project objectives

The goal of RECOBIA (Reduction of Cognitive Biases in Intelligence Analysis) is to improve the work of intelligence officers by reducing the negative effect of cognitive biases through the application of mitigation strategies that have been developed in the framework of the project. After three years, RECOBIA ended in January of 2015.

Description of the work

Cognitive biases are mental short-cuts deriving from our instinctive desire to simplify decision making by reducing the amount of information and uncertainty we have to deal with. These biases typically operate on the unconscious level and result in cognitive simplifications based on memory, experience, education, cultural background, political or ideological beliefs.

How can an intelligence officer deliver a reliable report to the political decision-maker when he or she is not aware of the confirmation bias, an effect that makes the analyst disregard all information that contradicts one’s pre-existing opinion on the subject? The answer is that the intelligence analyst cannot.

The objective of the project was to improve the quality of intelligence by reducing the impact of cognitive biases through the development of mitigation strategies. Therefore, the partners developed the following research plan:

» Examination of the activities of intelligence officers

» Assessment of cognitive biases

» Identification of the intelligence activities that are susceptible to cognitive biases

» Development of mitigation strategies

Since all humans are subjected to cognitive biases, the RECOBIA project focused not only on intelligence analysts, but on intelligence officers in general. Thus the findings of RECOBIA do not apply only to intelligence analysts but also to all employees of intelligence services.

One of the key successes of the RECOBIA project was to raise awareness of these aspects. The research conducted during the three years of the project always kept this principle in mind.

Results

RECOBIA delivered results in intelligence and the mitigation of cognitive biases that constitute a break-through in the field. The project team deconstructed the activities of intelligence officers and clustered them into key intelligence tasks (KITs). Those KITs described, for the first time, what intelligence officers actually do – both from an intelligence as well as a psychological perspective.

The KITs were used to identify the situation and activities in which cognitive biases are likely to impact intelligence officers. Finally, the project team developed mitigation methodologies and strategies, which are easy to implement and will boost the quality of intelligence.

All the results were validated by representatives from Europe's intelligence community via six workshops. These attracted more than 100 participants from 21 national intelligence agencies and five European Institutions. The workshops aimed at identifying the needs and requirements of professionals and to validate the developed solutions so as to ensure the results are applicable.

The intelligence field is not the only domain that could benefit from the findings of RECOBIA, however. Since all humans are affected by cognitive biases, the solutions have a wide range of applications in several other areas of analysis, particularly in the sectors of journalism, banking, finance, health and consulting. A training programme could be derived from the project's findings.

PARTNERS	COUNTRY
Compagnie Européenne d'Intelligence Stratégique (CEIS)	Belgium
Hawk Associates Limited	United Kingdom
THALES SA (Thales)	France
ATOS SPAIN SA	Spain
Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	France
ISEA PSY SAS	France
EUROSINT FORUM ASBL	Belgium
Zanasi Alessandro SRL	Italy
Universitat Konstanz	Germany
Technische Universitaet Graz	Austria

RESPECT / Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285582
Total Cost
€4,271,165
EU Contribution
€3,492,687
Starting Date
01/02/2012
End Date
31/05/2015

Coordinator

RIJKSUNIVERSITEIT GRONINGEN (RUG)
Faculty of Law
Oude Kijk in 't Jatstraat 26
PO Box 716
9712 EK Groningen,
The Netherlands
Contact
Joseph Cannataci
Tel: +31 50 363 5689
Mobile: +356 9942 6133
Fax: +31 50 363 5603
E-mail: j.a.cannataci@rug.nl
Website:
www.respectproject.eu

Project objectives

Convenience and cost-effectiveness are the two key considerations for citizens and security forces when deciding which technologies to adopt or avoid. States and private corporations adopt information communication technologies (ICTs) because they are cost-effective. ICTs are then capable of being bridged in multiple ways to permit police/security forces to go beyond the data they directly collect by tapping into data gathered and stored by private corporations. These ICTs are deemed to be "in balance" if they are implemented in a way which respects individuals privacy while still maximising convenience, profitability, public safety and security.

RESPECT sought to investigate if current and future implementation of ICTs in surveillance is indeed "in balance" and, where a lack of balance may exist or is perceived by citizens not to exist. The project explored options for redressing the balance through tools developed in the project thereby enabling policy makers to understand the socio-cultural as well as the operational and economic impact of surveillance systems.

Description of the work

The RESPECT project reviewed the effectiveness of surveillance systems and procedures used in Europe in preventing/reducing crime; and in tracking evidence for improved prosecutions of crimes and acts of terrorism. Five key sectors - CCTV, data mining and interconnection, social network analysis, RFID & geo-location/sensor devices, financial tracking – were investigated. RESPECT identified and examined the social and economic costs involved in the adoption and implementation of these systems and procedures.

RESPECT's work determined the legal basis adopted for these systems and procedures, identifying best practices that have evolved from the legal basis, and gaps that exist. RESPECT also explored (through qualitative and quantitative analysis) European citizens' awareness/acceptance of surveillance systems and procedures based on attitudes to efficiency, economic and social costs.

Results

RESPECT produced tools that enable policy makers to understand the socio-cultural as well as the operational and economic impact of surveillance systems. The project has three sets of outcomes:

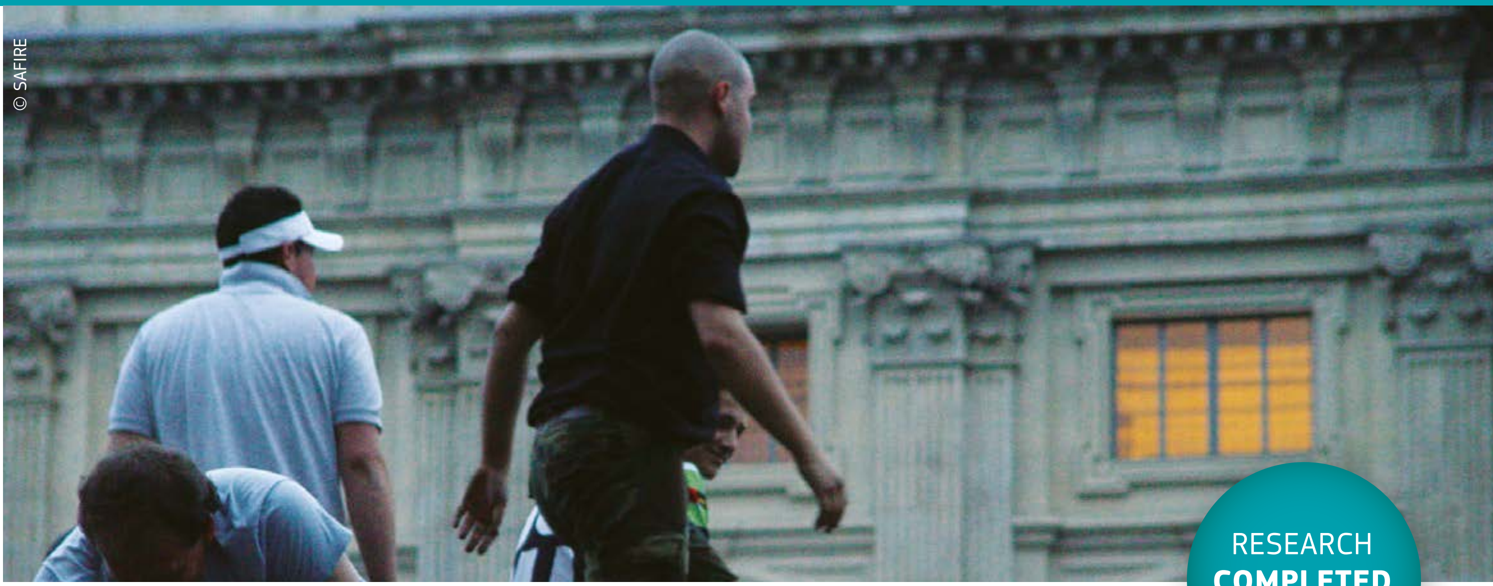
a. a draft model law laying down safeguards to protect the fundamental rights and freedoms of individuals when surveillance systems are deployed, as well as when non-surveillance data are used for the purpose of surveillance.

b. a decision-support tool aimed policy makers about the introduction and/or retention of a surveillance system. The tool's innovation is that it brings together operational, legal, economic and social implications in the decision-making process.

c. a brief identifying policy recommendations for action based on key findings of the RESPECT. Seven sets of action are identified: i. Introducing and/or strengthening of legislation; ii. Strategic planning and development; iii. Oversight & enforcement; iv. Cooperation; v. Capacity building & training; vi. Technical matters; vii. Citizens' awareness.

PARTNERS	COUNTRY
Rijksuniversiteit Groningen (RuG)	The Netherlands
University of Central Lancashire (UCLan)	United Kingdom
University of Ljubljana (UL)	Slovenia
Laboratorio di Scienze della Cittadinanza (LSC)	Italy
Babeș-Bolyai University of Cluj-Napoca (BBU)	Romania
Universitetet i Oslo (UiO)	Norway
Universidad de Leon (ULE)	Spain
Law and Internet Foundation (LiF)	Bulgaria
Uppsala University (UU)	Sweden
Georg-August-Universitaet Goettingen Stiftung Oeffentlichen Rechts (UGOE)	Germany
Sheffield University (SHEFU)	United Kingdom
Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Germany
Consiglio Nazionale delle Ricerch (CNR)	Italy
Universzita Komenskeho v Bratislave (FMUNIBA)	Slovakia
University of Malta (UoM)	Malta
University of Vienna (UNIVIE)	Austria
Masarykova univerzita (MU)	Czech Republic
Edith Cowan University (ECU)	Australia
International Criminal Police Organisation (INTERPOL)	France (Headquarters)
University of Westminster (UoW)	United Kingdom
Universitat de Barcelona (UB)	Spain

SAFIRE / Scientific Approach to Finding Indicators for & Responses to Radicalisation


© SAFIRE

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241744
Total Cost
€3,681,260
EU Contribution
€2,906,600.95
Starting Date
01/06/2010
End Date
30/11/2013

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
The Netherlands
Contact
Dr. Heather Griffioen-Young
Tel: +31 346356378
Fax: +31 346353977
E-mail: heather.griffioen@tno.nl
Website: http://www.safire-project.eu

Project objectives

The key in democratic societies is to ensure citizens' rights to free thought – even radical thought – while protecting society from the fallout of illegal actions from violent radicalised groups and individuals. Successfully achieving this goal depends on understanding the phenomenon of radicalisation, from its roots in thought and discourse to the stage where individuals go beyond it and engage in violent and illegal behaviour in the name of their cause.

SAFIRE is an EU project started in June 2010 to explore this interesting and sensitive topic. The scope of SAFIRE primarily involves groups and individuals on the extreme and violent end of the radicalisation spectrum. However, in order to understand them and their motives, we also need to step back and understand what happened before they turned to a more violent version of their philosophy.

Description of the work

In this project, we focus on two innovations in this field of research:

» Developing a non-linear model of the radicalisation process based on typologies of radical groups, cultural aspects of radicalisation, observable indicators of radicalisation, interventions designed to reverse, halt or prevent the radicalisation process.

» The collection of qualitative and quantitative empirical data to test hypotheses about radicalisation and principles of effective interventions.

Results

We developed and carried out the SAFIRE research with the explicit application to policy and field in mind. Some relevant practical results are:

» Intervening in the pre-violent stage of radicalisation is not supported by all EU Member States

» Various cultural factors seem to make a society more or less susceptible to radicalisation

» Part of the challenge of dealing with violent radicalisation is separating the wheat from the chaff

» Different types of radicalised groups have different characteristics and, as such, require a different approach to deal effectively with the threat of violence they pose to society

» The Internet is an increasingly important environment for individuals on the way towards radicalisation

» Indicators of radicalisation cannot be sought in unchanging behaviour or in any one individual behaviour

» Most successful interventions designed to prevent violent radicalisation tend to focus on psychological factors, such as self-esteem, dealing with negative emotions, and reducing feelings of injustice

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Stichting Forum, Instituut voor Multiculturele Ontwikkeling (FORUM)	The Netherlands
International Security and Counter-Terrorism Academy (ISCA)	Israel
Rand Europe Cambridge Ltd (RAND)	United Kingdom
Stichting Hogeschool Utrecht (Hogeschool Utrecht)	The Netherlands
Bridge 129 Spa Safety and Security (Bridge)	Italy
Compagnie europeenne d’intelligence stratégique SA (CEIS)	France
Universidade de Coimbra (UC)	Portugal
Fondation pour la recherche stratégique (FRS)	France
Universiteit van Amsterdam (UvA)	The Netherlands

SLANDAIL / Security System for language and image analysis

Information

Grant Agreement N°
607691
Total Cost
€3,844,488.80
EU Contribution
€2,942,445.00
Starting Date
01/04/2014
Duration
36 months

Coordinator

THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN (TCD)
Department of Computer Science
O'Reilly Institute, Trinity College
Dublin 2- Ireland
Contact
Prof. Khurshid Ahmad
Tel: +353 (0)1 896 8429
Mobile:
+353 (0)87 9757669
Fax: +353 (0)1 677 2204
E-mail: kahmad@scss.tcd.ie
Website: www.cs.tcd.ie/khurshid.ahmad

Project objectives

SLANDAIL has three key objectives:

- Collate and review the sharing and dissemination of disaster zone information amongst experts tasked with improving the security of citizens and property;
- Create protocols to protect the rights of the citizens and to manage the confidentiality of the collected data and processed information relating to individual citizens;
- Build and test a prototype system for collecting, processing, aggregating and disseminating information for disaster emergency management.

Description of the work

The project will begin with a comprehensive specification and analysis of end-user needs. Relevant disaster case studies will be identified, the existing use of social media in disaster management will be evaluated, the technology systems used by civil protection agencies will be reviewed and the compliance protocols for data protection used by such agencies will be examined.

The ethical and factual provenance of data and information will be ensured through examining the societal impact of social media in security contexts.

The project will then develop methods and ontologies for extraction and analysis of multilingual textual and speech data and images from social media. Software systems for text and image analytics will subsequently be evaluated and integrated to produce a final demonstrator. The performance and communicability of this system will be tested and evaluated.

Expected results

The main research output of SLANDAIL will be the specification and a prototype of an emergency management system that takes its feeds from emergency operatives, social media feeds and formal media feeds. The system will be multi-modal (encompassing text, speech and image analytics), multi-lingual and capable of aggregation. It will moreover have a novel self-learning component that will update the emergency management systems knowledge base through the life cycle of a disaster.

PARTNERS	COUNTRY
The Provost, Fellow, Foundation Scholars and the Other Members of Board of the College of the Holy & Undivided Trinity of Queen Elizabeth near Dublin (TCD)	Ireland
Institut for Angewandte Informatik e.V. (INFAI)	Germany
University of Ulster (Ulster)	United Kingdom
Universita Degli Studi di Padova (UNIPD)	Italy
CID GmBH (CID)	Germany
Stillwater Communications Limited(Stillwater)	Ireland
Centre for Irish and European Security Limited (CIES)	Ireland
Police Service of Northern Ireland (PSNI)	United Kingdom
Datapiano SRL (DataPiano)	Italy
Bundesministerium der Verteidigung (BLS)	Germany
Pintail Ltd (PT)	Ireland
An Garda Siochana	Ireland

SOTERIA / Online and Mobile Communications for Emergencies

Information

Grant Agreement N°
606796
Total Cost
€5,128,589.60
EU Contribution
€3,971,177.60
Starting Date
01/09/2014
Duration
30 months

Coordinator

TEKEVER + (TEK)
Rua das Musas 3.30
1990-113 – Lisboa
Portugal
Contact
Pedro Sinogas
Tel: +351 213 304 300
Mobile: +351 938 358 560
Fax: +351 213 304 301
E-mail:
Soteria.coordination@
tekever.com
Website: www.soteria.i112.eu

Project objectives

SOTERIA will develop recommendations and a toolbox to increase the impact that social media can play in emergencies, enabling public safety organizations (PSOs) and citizens to communicate before, during and after an emergency event. Empowered by mobile phones with cameras, text messaging and internet-based applications that connect to social media, citizens expect PSOs to use the same technologies.

Description of the work

The project will research the impact of social media in emergencies and develop a SOTERIA prototype, comprising:

» SOTERIA recommendations on guidelines and courses of action for PSOs and citizens;

» A SOTERIA toolbox that integrates emergency-related ICT tools and functionality (e.g., social media tools and mobile applications) to offer additional communication channels between PSOs and citizens and enhance high-quality situational awareness for PSOs and citizens in emergencies.

SOTERIA will innovate by allowing the (i) understanding of the impact of social media in emergency management systems; (ii) use of all communication channels in emergency situations, including social media, (iii) exploitation of the ubiquity of mobile platforms to locate and effectively communicate with citizens in distress; and (iv) leverage the levels of shared awareness and performance of PSOs that benefit from social media information.

Expected results

The main results from SOTERIA are threefold:

- A set of recommendations for the use of social media technologies and tools in emergencies;
- A professional SOTERIA toolbox for emergency response;
- A set of tools based on social media for use by citizens.

The professional and citizen toolboxes will be designed to take into account the organizational culture of emergency services and the EU's legislation and concerns on privacy, as well as related human and technological dimensions. These will enable PSOs to understand the benefits of social media in emergencies and to gradually adopt these technologies to their daily activities, thus helping safeguard citizens in emergency and crisis situations.

PARTNERS	COUNTRY
TEKEVER (TEK)	Portugal
Ambulance and Emergency Physicians Association (AAHD)	Turkey
Area7 srl (AREA7)	Italy
Ministério da Administração Interna (GNR)	Portugal
Deveryware (DEVERYWARE)	France
Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)	Germany
Pelastusopisto, Emergency Services College (ESC)	Finland
Helse Bergen HF*Haukeland University Hospital (HUS)	Norway
ITTI Sp Zoo (ITTI)	Poland
Police and Crime Commissioner for North Yorkshire (PCCNY)	United Kingdom
Poliisiammattikorkeakoulu (POLAMK)	Finland
Pole Pilote de Securite Locale (PPSL)	France
Kuopion Kaupunki (PSPELA)	Finland
The Provost, Fellows, Foundation Scholars & the Other Members of Board of the College of the Holy & Undivided Trinity of Queen Elizabeth near Dublin (TCD)	Ireland
Thales SA (THALES)	France
Ita-Suomen Yliopisto (UEF)	Finland
Zanasi Alessandro SRL (ZANASI)	Italy

SUPER / Social sensors for secUrity Assessments and Proactive EmeRgencies management

real time social network mapping
behavioral analysis
strategic planning and emergency management

Information

Grant Agreement N°
606853
Total Cost
€4,252,770.40
EU Contribution
€3,117,318.00
Starting Date
01/04/2014
Duration
36 months

Coordinator

VITROCISET S.P.A. (VITRO)
Business Unit Homeland Security
Via Tiburtina
1020
00156 – Rome - Italy
Contact
Marco Cosentino
Tel: +39 06 8820 4316
Fax: +39 06 8820 6189
E-mail:
m.cosentino@vitrociset.it
Website: www.vitrociset.it

Project objectives

The main goal of the SUPER project is to research and implement a holistic integrated approach to using social media in emergencies and security incidents. This will operate at multiple time-scales while providing several security and emergency management functionalities. The SUPER approach will exploit social media information to assess citizens' behaviours and attitude before, during and after security or emergency incidents. This information will be integrated into tools serving both the strategic and the tactical level of security/emergency management, thus facilitating security operators and civil protection officers in a variety of tasks. These include: intelligence gathering and strategic planning, real-time management of security operations, generation of a common operational picture (COP) and other tasks. SUPER's technologies will be validated in two distinct scenarios, one dealing with emergency management during (natural or man-made) disasters and the other with police services.

Description of the work

The SUPER consortium has devised a 36-month work plan for its objectives. This is organized into nine major work areas. The work areas can be clustered into three categories:

1. Horizontal work packages spanning the whole duration of the project which are pertinent to all activities of SUPER.

2. Technological development work packages, dealing with the project's core of research and technology development (RTD) areas such as algorithms and techniques for social media analysis and development of a modular plug-n'-play architecture for SUPER's framework.

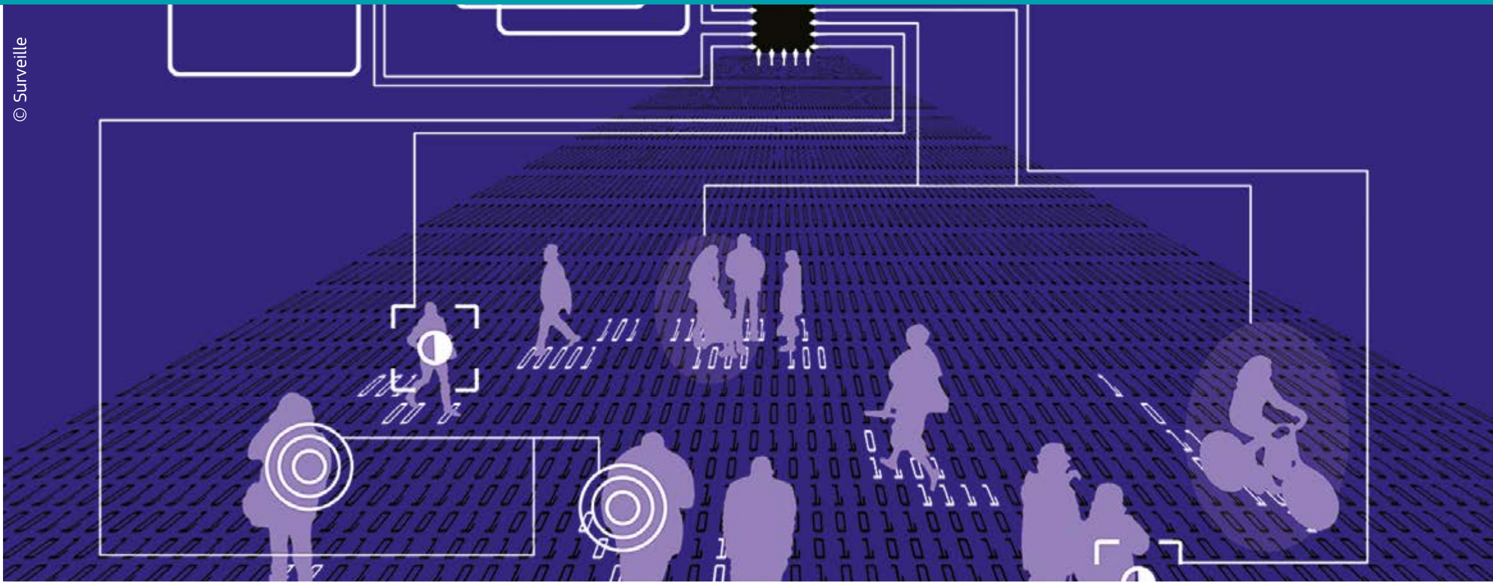
3. Integration, validation, testing and evaluation activities whose main goal is to enable an early launch of the project's integration and applications developments by remedying potential problems.

Expected results

The main outcome of the SUPER research (i.e. behavioural analysis algorithms) will be integrated into security and emergency management applications. Itsresearch will be used to drive implementation of the next-generation emergency management and crisis management tools.

PARTNERS	COUNTRY
Vitrociset S.p.A. (VITRO)	Italy
University of Glasgow (GLA)	United Kingdom
Institute of Communication and Computer Systems/National Technical University of Athens (ICCS/NTUA)	Greece
Sensing & Control Systems S.L. (S&C)	Spain
Civil Protection Service of Campania Region (Regione Campania)	Italy
Fundació Barcelona Media -Yahoo! Research (BM-Yahoo!)	Spain
SENSAP Swiss AG (SENSAP)	Switzerland
IN2 Search interfaces development ltd (IN2)	United Kingdom
Inspectoratul General al Politiei Romane (IGPR)	Romania

SURVEILLE / Surveillance: Ethical Issues, Legal Limitations, and Efficiency



© Surveille

Information

Grant Agreement N°
284725
Total Cost
€4,382,719.80
EU Contribution
€3,382,354
Starting Date
01/02/2012
Duration
39 months

Coordinator

EUROPEAN UNIVERSITY INSTITUTE
Research Administration
Via dei Roccettini 9, San Domenico Di Fiesole
50014 Firenze, Italy
Contact
Ms. Serena Scarselli
Tel: +39 055 4685 204
Fax: +39 055 4685 293
E-mail: serena.scarselli@eui.eu
Website: www.surveille.eu

Project objectives

SURVEILLE systematically reviews the impacts of different surveillance systems, and also helps manufacturers and end-users better develop and deploy these systems. It is a multidisciplinary project combining law, ethics, sociology and technology analysis. SURVEILLE assesses surveillance technology for its effectiveness in fighting crime and terrorism and its social and economic costs; it will assess perceptions of surveillance in the general public and certain identified target groups. SURVEILLE addresses legal limitations on the use of surveillance technologies as well as ethical constraints. SURVEILLE analyses the potential of 'privacy by design' and privacy-enhancing technologies in the context of surveillance systems and interacts with technology developers and manufacturers through a systematically delivered advisory service. SURVEILLE engages with law enforcement officials to seek their feedback as results emerge from the research. The project aims at wide dissemination, including amongst European and national decision-makers and will contribute to the field of training of judges, prosecutors and the police.

Description of the work

SURVEILLE is an interdisciplinary programme of research that will help decision makers to make better choices concerning the development, deployment and use of surveillance technologies. SURVEILLE conducts a comprehensive survey of surveillance systems and technologies that are currently used in Europe or that are likely to be introduced and addresses the legal limits on surveillance and the ethical issues it raises. It will also assess the effectiveness of surveillance technologies in improving security. SURVEILLE examines perceptions of surveillance and surveillance technologies amongst the general public and specific target groups, and informs decision-makers and other relevant stakeholders about the public acceptability of these technologies. Interactions between SURVEIILLE and developers and end-users will help manufacturers to adapt their systems to public concerns, and will help users to deploy systems more effectively. SURVEILLE builds upon the work of DETECTER – an FP7 Security funded project involving some of the members of this consortium that successfully experimented with the use of closed meetings between law enforcement officials, technology developers and human rights lawyers and ethicists to discuss how products could be developed in line with human rights and ethical standards. SURVEILLE further innovates by piloting an advisory service for technology developers using teleconferencing for virtual meetings and a telephone help-line as a potential advance in best practice. The concerns of technology developers will also serve as an input to research on ethical and legal constraints; here SURVEILLE also adds value to other projects funded under FP7 Security calls. SURVEILLE's interaction with technology developers, end-users and the data gained on perceptions of surveillance will be combined with the theoretical research to produce the best possible academic input for policy makers. SURVEILLE includes cutting edge expertise in ethics and human rights law.

Expected results

SURVEILLE provides a comprehensive survey of surveillance technology deployed in Europe and appraises security concerns, economic cost, public perceptions, and infringement of fundamental rights, and examines the legal and ethical issues of surveillance technology in the prevention, investigation and prosecution of terrorism and other serious crimes. SURVEILLE will continuously communicate results with stakeholders – European decision-makers, law enforcement, local authorities and technology developers – and receive feedback to inform ongoing research.

PARTNERS	COUNTRY
EUROPEAN UNIVERSITY INSTITUTE (EUI)	Italy
UNIVERSITY OF BIRMINGHAM (UOB)	United Kingdom
RAOUL WALLENBERG INSTITUTE OF HUMAN RIGHTS AND HUMANITARIAN LAW (RWI)	Sweden
TECHNISCHE UNIVERSITEIT DELFT (TU DELFT)	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IOSB)	Germany
UNIVERSITE LIBRE DE BRUXELLES (ULB)	Belgium
FORUM EUROPEEN POUR LA SECURITE URBAINE (EFUS)	France
MERSEYSIDE POLICE AUTHORITY (MERPOL)	United Kingdom
ALBERT-LUDWIGS-UNIVERSITAET FREIBURG (ALU-FR)	Germany

TRACE / TRafficking as A Criminal Enterprise

Information

Grant Agreement N°
607669
Total Cost
€1,126,383.65
EU Contribution
€1,006,492.37
Starting Date
01/05/2014
Duration
24 months

Coordinator

TRILATERAL RESEARCH LTD (TRI)
Kush Wadhwa
Crown House, 72 Hammersmith Road
W14 8TH, London, UK
Contact
Kush Wadhwa
Tel: +44 (0) 207 559 3550
Mobile:
+44 (0)7765 820366
Fax: +44 (0) 207 559 3551
E-mail: Kush.wadhwa@trilateralresearch.com
Website:
www.trilateralresearch.com

Project objectives

TRACE aimedto help stakeholders disrupt the trafficking of human beings (THB). It has developed a state-of-the-art understanding of criminal, social, economic, psychological and political processes that make the trafficking industry what it is. Key objectives include:

1. Develop a theory-driven understanding of trafficking as a criminal enterprise;
2. Acquire a part-theory, part-evidence-based understanding of the specific characteristics of the traffickers: who are they? why do they become traffickers? and why do some victims become traffickers? Lastly, to understand the nature of the interaction amongst, traffickers, victims and third parties who facilitate THB;
3. Develop a framework of factors influencing the current and future trends in trafficking of human beings; and
4. Develop a theory-driven understanding of current policies and provide a framework of policy actions available for stakeholders.

Description of the work

TRACE will use case studies from European countries to investigate the trafficking industry in detail. It creates a conceptual map of the THB industry to develop a preliminary understanding of the way in which THB has been defined and framed in Europe (WP1). It seeks to understand the relationship between the THB business and the broader organized crime trade (WP1). It looks at the geographical and modus operandi trends within the industry (WP 2). TRACE examines the specific characteristics of individuals involved in the trafficking industry and the relationships between them (WP3). An examination of factors that have influenced the operation of the trafficking industry (WP4 & WP5), including: the role of technology, economic and political factors. Based on this analysis TRACE will identify future trends in THB. The findings will be used to develop policy recommendations for stakeholders and to develop a handbook for those working towards combatting THB (WP6).

Expected results

TRACE will provide stakeholders with more detailed information on the criminal enterprise behind THB to assist them in combatting this ever-growing form of organized crime. Key outputs from TRACE include:

- Identification of future trends in THB in Europe.
- Policy recommendations and briefing papers for stakeholders.
- TRACE Handbook – "Trafficking in Human Beings: analysis of criminal networks for more effective counter-trafficking handbook".
- Final conference to showcase the project's findings and deliver its policy recommendations and handbook.

The findings will be widely disseminated through different means, including our website: http://trace-project.eu and Twitter account: @TRACE_EU

PARTNERS	COUNTRY
Trilateral Research Ltd (TRI)	United Kingdom
Vrije Universiteit Brussel (VUB)	Belgium
Stichting Katholieke Universiteit Brabant Universiteit Van Tilburg (TiU)	The Netherlands
The Council of the Baltic Sea States Secretariat (CBSS TF-THB)	Sweden
Agentia Nationala Impotriva Traficului de Persoane (ANITP)	Romania
Cyprus Police (CY POL – THB)	Cyprus
The International La Strada Association (LSI)	The Netherlands
Animus Association Foundation (AAF)	Bulgaria

ADDPRIV / Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance

© Andrey Maslennikov - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261653
Total Cost
€4,077,720.40
EU Contribution
€2,818,338
Starting Date
01/02/2011
End Date
31/03/2014

Coordinator

ANOVA IT CONSULTING, SL
Avda. Punto Mobi, 4 -
Parque Científico Tecnológico de la Universidad de Alcalá
28805 – Alcalá de Henares
Spain
Contact
Paolo D'Arminio
Tel: +34 918 305 977
Mobile: +34 634 933 543
Fax: +34 918 305 928
E-mail: paolo.darminio@anovagroup.es
Website: www.addpriv.eu

Project objectives

The ADDPRIV project proposed novel knowledge and developments to better comply with citizens' privacy rights through limiting the storage of unnecessary data throughout existing multicamera networks.

It addressed the challenge of determining in a precise and reliable manner private data captured by video surveillance systems that are not relevant from a security perspective.

ADDPRIV proposed solutions for automatic discrimination of relevant data recorded on a multicamera network, related to an individual whose suspicious behaviour triggered an alert. Relevant data not only corresponds to video scenes capturing individuals' suspicious behaviour (smart video surveillance), but also automatically extracting images of these individuals recorded before and after the suspicious event and across the surveillance network.

Description of the work

The project was divided into 8 work packages, 6 devoted to R&D and 2 devoted to Management Activities:

» **Requirements for better compliance with privacy rights:** precise definition of all legal and ethical specifications that the solution has to fulfil; preliminary definition of the system compliance with citizens' privacy evaluating criteria;

» **Definition of technical specifications:** detailed definition of the ADDPRIV solution's technical specifications; definition of the standards to be used in order to ensure interoperability; precise definition of the real life scenarios for testing;

» **Data relevancy discrimination algorithms:** generation of new algorithms for Automatic Data Relevancy Discrimination capable of reconstructing the route followed by a suspicious person throughout a camera network, automatically triggered by smart surveillance algorithms and capable of adapting to different scenarios;

» **Intelligent storage and secure deletion technologies:** development of intelligent storage algorithms and methodologies for the automatic browsing and retrieval of all the relevant data related to a suspicious event (automatic processes that avoid a manual handling of the recorded images that lead to privacy infringements); development of secure erase technologies specific for SSDs to be applied on images that are not relevant from a security perspective;

» **Implementation and validation of developed solutions in a real life scenario:** design and implementation of the developed solution in a real application context along with the already existing video surveillance systems;

» **Analysis of the impact of the proposed solutions on human rights and organizational processes:** analysis of ADDPRIV's impact on the organizations involved in surveillance and security in order to look for possible amendments to the technological solution; development of a strong and detailed understanding of the current public concerns with privacy, security and surveillance in order to address them;

» **Project Coordination and Quality Management;**

» **Dissemination, Exploitation and Ethical Management.**

Results

ADDPRIV offers an innovative approach to security through the implementation of technologies for privacy-sensitive video surveillance in public places, with automatic data relevancy discrimination, and intelligent storage according to an image's relevancy.

Images considered by the system as irrelevant (not associated with security sensitive events) are deleted according to the highest security standards, in order to ensure that citizens' privacy rights are preserved during. Moreover, by strongly limiting the intervention of CCTV operators, consequences such as having ethnical subgroups be the focus of attention of surveillance operations are eliminated, thus contributing to the respect of values of human dignity, freedom, and equality for minorities.

ADDPRIV has strong potential for improving the social acceptability of video surveillance technologies due to its inclusion of the value and importance of privacy alongside enhanced security. At the same time, organisations and system operators can be more efficient and increase customer satisfaction by meeting the expectations of maintaining security without an intrusive instrument in their private life sphere.

PARTNERS	COUNTRY
ANOVA IT CONSULTING, SL	Spain
KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION	United Kingdom
POLITECHNIKA GDANSKA	Poland
LANCASTER UNIVERSITY	United Kingdom
AVANZIT TECNOLOGIA, S.L.	Spain
HEWLETT PACKARD ITALIANA SRL	Italy
SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA	Italy
Renfe Operadora	Spain
THE PROVOST FELLOWS & SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN	Ireland

ALTERNATIVE / Developing alternative understandings of security and justice through restorative justice approaches in intercultural settings within democratic societies

© eva serrabassa - istockphoto.com

Information

Grant Agreement N°
285368
Total Cost
€4,354,777.60
EU Contribution
€3,423,262
Starting Date
01/02/2012
Duration
48 months

Coordinator

KATHOLIEKE UNIVERSITEIT LEUVEN (KU LEUVEN)
Leuven Institute of Criminology (LINC)
Hooverplein 10
3000 Leuven, Belgium
Contact
Inge Vanfraechem
Tel: +32 16 32 5277
Fax: +32 16 32 5463
E-mail: inge.vanfraechem@law.kuleuven.be
Website:
www.law.kuleuven.be/linc

Project objectives

The overall objective of this project is to provide an alternative and deepened understanding based on empirical evidence of how to handle conflicts within intercultural contexts in democratic societies in order to set up security solutions for citizens and communities. From this general objective several specific objectives are derived :

» To develop a coherent theoretical framework for an alternative understanding of security and justice,

» To develop empirically applicable knowledge on conflict and conflict transformation in intercultural settings,

» To design, apply and evaluate concrete action models in four different intercultural conflict settings, based on an alternative understanding of justice and security and on existing restorative justice (RJ) models, and

» To analyse the findings from the four pilot settings in a comparative way and to advance knowledge by integrating the empirical results into theoretical insights and by adapting the latter where appropriate.

Description of the work

The project is set up in different work-packages (WP). Three work-packages focus on the theoretical development of the concepts: WP1 will: critically analyse the existing epistemologies of thinking, talking about, and doing justice in current democratic societies, especially in relation to the discourse on human security; offer a new theoretical understanding based on alternative epistemologies on how to tackle conflict, especially in intercultural settings in a constructive and transformative way; and analyse RJ as an alternative academic and policy oriented discourse to the current dominant discourses on justice and human security. WP2 will: undertake an analysis of 'conflict' in intercultural contexts, conflict transformation mechanisms and security perceptions; study the role of dialogical processes and possible contributions from civil society in conflict transformation at individual and societal level; study the role of gender and age in conflict resolution approaches; and investigate conflict transformative processes in an intercultural context at three different levels (micro-meso-macro) in four different settings. WP3 will study the existing RJ models and their potential application and relevance to conflicts in an intercultural context and possible implications for European policies.

Four more practice-oriented WPs will apply action research in different settings. WP4: Dealing with everyday conflicts at the micro-level between local residents and residents with migrant backgrounds in public/social housing (Vienna); WP5: Dealing with meso-level conflicts in a small town with tensions between Roma and non-Roma inhabitants (Hungary); WP6: Dealing with interethnic conflicts at meso- and macro-level (Serbia); and WP7: Dealing with civil conflicts at meso- and macro-level (Northern Ireland).

WP 8, 9 and 10 deal respectively with comparative research, dissemination of the results, and the management of the whole project.

Expected results

At the end of the project, innovative and exemplary RJ based models and procedures of conflict resolution will be available to statutory and non-statutory agencies which are confronted daily with problems of intercultural/ interethnic conflicts throughout Europe. The project will demonstrate in a very concrete and visible way how alternative understandings of security and justice issues in democratic societies can be constructed through participatory processes with citizens.

PARTNERS	COUNTRY
Katholieke Universiteit Leuven (KU Leuven)	Belgium
Institute for the Sociology of Law and Criminology (IRKS)	Austria
European Forum for Restorative Justice (EFRJ)	Belgium
Foresee Research Group (Foresee)	Hungary
Norwegian Social Research (NOVA)	Norway
Victimology Society of Serbia (VDS)	Serbia
University of Ulster (UU)	Northern Ireland

COREPOL / Conflict Resolution, Mediation and Restorative Justice and the Policing of Ethnic Minorities in Germany, Austria, and Hungary

© Merijn van der Vliet - iStockphoto

Information

Grant Agreement N°
285166
Total Cost
€1,775,192
EU Contribution
€1,429,681
Starting Date
01/01/2012
Duration
36 months

Coordinator

GERMAN POLICE UNIVERSITY
Police Science Department
Zum Roten Berge 18-24
D-48165 Münster, Germany
Contact
Professor Joachim Kersten
Tel: +49 2501 806295
Mobile: +49 172 260 3860
Fax: +49 2501 806 226
E-mail:
Joachim.Kersten@dhpol.de
Website: www.corepol.eu

Project objectives

The proposed research will use a comparative design (Germany, Austria, Hungary) to establish whether better police - minority relations can be achieved through means of a Restorative Justice (RJ) approach.

The main objective of the COREPOL project will be:

» To provide a basis for coordinated research activities in the area of police-minority relations using a comparative method of data analysis; the findings will further police science research in this crucial area of peace building as part of a democratic process within European societies;

» To address the practical issue of effective dissemination of research findings to improve police-minority interaction making use of the realm of police tertiary education and in-service staff training but also involving other agencies including NGOs;

» To serve as a principal network for a practice oriented dissemination of RJ strategies and peace building in the conflict zone of police and minorities. In the area of police education, this concerns CEPOL course curricula (e.g. TOPSCOP) and course material and curricula for similar influential target groups, and also civil and public sector agencies.

Description of the work

The extent and cultural particularities of RJ programs and their affiliation to the criminal justice system will be ascertained. Then, specific minority populations (Turks in Germany, Roma in Hungary, Africans in Austria) will be examined in regard to the country's security context. The involvement of police in RJ programs for minority populations will be explored. Finally, the proposed research will exemplify the scope of RJ approaches for the improvement of police-minority communication and interaction. Based on the legality principle and on an inquisitorial civil law tradition of policing and criminal justice, the partner countries' legal and policing systems differ substantially from the Anglo-American-Australian hemisphere of restorative justice.

Expected results

It is one of the objectives of the proposed research to spread basic knowledge about the concept of RJ, its practical implementation, its varieties across the legal cultures, and its impact on different security contexts, the policing in general, and the policing of minorities in particular: RJ's potential for handling conflicts and peace building within democratic societies. The findings will have a wider impact on the Central and Eastern EU situation. The research will include open questions of gender, age and cultural compatibility of RJ.

PARTNERS	COUNTRY
German Police University (DHPOL)	Germany
Rendőrtiszti Főiskola (RTF)	Hungary
Bundesministerium für Inneres (SIAK)	Austria
Verein für Rechts- und Kriminalsoziologie (IRKS)	Austria
European Research Services GmbH (ERS)	Germany

DETECTER / Detection technologies, ethics, human rights and terrorism

© V. Yakobchuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217862
Total Cost
€2,424,419
EU Contribution
€1,869,684
Starting Date
01/12/2008
End Date
31/01/2012

Coordinator

UNIVERSITY OF BIRMINGHAM
Dept. of Philosophy, School of Social Sciences
Edgbaston
B15 2TT BIRMINGHAM
United Kingdom
Contact
Tom Sorell
Tel: +44 121 414 8443
Fax: +44 121 414 8453
E-mail: t.sorell@bham.ac.uk
Website:
www.detecter.bham.ac.uk

Project objectives

The overall objective of DETECTER was to identify appropriate human rights, legal and moral standards for detection technologies in counter-terrorism. This assessment took into account the effectiveness of these technologies as judged by law enforcement bodies responsible for counter-terrorism, and other relevant authorities.

DETECTER aimed to do this in three ways:

» by surveying current and foreseeable applications of detection technologies in counter-terrorism;

» by conducting legal and philosophical research into the implications of human rights and ethics for counter-terrorism, and the use in counter-terrorism of technologies for the surveillance, identification or tracking of people and places; and

» by engaging directly and continuously with developers and users of detection technologies.

Results

DETECTER conducted a comprehensive review of the latest developments in detection technologies, resulting in five technology review reports, a series of day-long meetings with technology developers and users, and focus-groups with counter-terrorism professionals. The feedback and analysis of these groups will be released in academic publications.

A further series of research papers examined the ethical norms of counter-terrorism, including the extent of intrusion that can be justified for investigating terrorist threats and the moral hazards of profiling as a counter-terrorism tool. One paper on the ethics of special investigative techniques has already been published and one proposing a novel theory of privacy is in the process of being published, both in academic journals. Another study, focused on border security ethics and the rights of refugees, will also be released via academic publication.

Yet another of DETECTER's studies examined permissible limitations to the human right of privacy and recommended six universal safeguards that should be adopted to avoid abuses of power when undertaking surveillance. These include categories of offence liable for surveillance investigation, limitations on data dissemination and storage, and guarantees of due process.

Other work packages focused on data mining and electronic surveillance of internet activity. New insights were gained by assessing relevant practices in EU Member States and comparing them against US case studies. The findings fed into a series of research meetings on the judicial implications of such technology in counter-terrorism activities, including the need for a regular review of practices by national courts and the UN Human Rights Committee.

Many of these reports, including multi-media presentations and digestible summaries of key research findings, are available for public review and discussion on the DETECTER project website - http://www.detecter.bham.ac.uk/index.html

PARTNERS	**COUNTRY**
University of Birmingham	United Kingdom
Åbo Akademi University	Finland
University of Nottingham	United Kingdom
University of Zurich	Switzerland
University of Oslo, Centre for Human Rights	Norway
Raoul Wallenberg Institute of Human Rights and Humanitarian Law	Sweden
Danish Institute for Human Rights	Denmark
European University Institute	Italy

INEX / Converging and conflicting ethical values in the internal/external security continuum in Europe

© quayside- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218265
Total Cost
€2,422,082
EU Contribution
€1,890,248
Starting Date
01/04/2008
End Date
31/03/2011

Coordinator

INTERNATIONAL PEACE RESEARCH INSTITUTE
Hausmannsgate 7
NO-0186 Oslo
Norway
Contact
J. Peter Burgess
Tel: +47 22 54 77 00
Fax: +47 22 54 77 01
E-mail: peter@prio.no
Website:
http://www.inexproject.eu

Project objectives

This project set out to analyse the value assumptions and ethical consequences of the internal/external security continuum in Europe of trans-border security initiatives. Its goal was to better understanding the role of values in security measures and to frame recommendations for strengthening the coherence, effectiveness and justice of security policy in the EU.

The work of INEX project was designed around thematic and geopolitical research axes. The thematic axes explored four fields of knowledge relating to value-laden tensions that arise from internal/external security continuum:

- ethical consequences of the proliferation of security technologies;
- legal dilemmas linked to transnational security arrangements;
- ethical and value questions stemming from the shifting role of security professionals;
- consequences of the changing role of foreign security policy in an era when the distinction between external and internal borders grows less distinct.

Along the geopolitical axis, the project studied the aims and outcomes of the EU's Eastern European and Mediterranean neighbourhood policies.

Results

INEX's research concluded that ethical concerns and the value assumptions should play a central role in the formation of European security policy.

The study of internal and external security measures suggests the need for careful consideration of the ethical assumptions behind security technological, for new interpretations of conventional legal documents, for attention to the values informing the work of security professionals and the shifting forces of the foreign policy arena.

The project's results indicate that these new needs have consequences for the external policing policies of the EU in an age of rapid security sector reform. The ambitions of the EU's European Neighbourhood Policy and Mediterranean policies have been challenged by inadequate attention to the geopolitical, cultural, religious and economic dimensions of rapidly changing events.

The project's results suggest that security cannot be reduced to a single political approach, institutional orientation or sole dependence on scientific means. They indicate that reliance on security technologies as the default approach to security challenges is not only an inadequate solution to the threats European society faces, but can, at times, stand in the way of suitable solutions.

PARTNERS	COUNTRY
International Peace Research Institute	Norway
Ericsson Security Systems	Norway
Centre d'études sur les conflits	France
Vrije Universiteit Brussel	Belgium
Vrije Universiteit Amsterdam	The Netherlands
Centre for Security Studies, Collegium Civitas	Poland
Centro de Investigación de Relaciones Internacionales y Desarrollo	Spain
Bilkent University	Turkey
Centre for European Policy Studies	Belgium

PACT / Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action

© PACT

Information

Grant Agreement N°
285635
Total Cost
€3,237,736.40
EU Contribution
€2,675,107.85
Starting Date
01/02/2012
Duration
36 months

Coordinator

VITAMIB SAS
Rue Colonel Dumont 26
38000 Grenoble, France
Contact
Xavier Fabre
Tel: + 33 4861 10185
Mobile: + 33 6768 42877
Fax: + 33 4765 18491
E-mail: xfabre@vitamib.com
Website: www.vitamib.com

Project objectives

PACT is a collaborative project, which aims:

» to assess existing knowledge about public perception of the tension between security and privacy and the role played by social trust and concern,

» to collect empirical evidence about the way in which European citizens perceive and assess in real life novel surveillance technologies,

» to analyze the main factors that affect public assessment of the security and privacy implications of given security technology.

On the basis of such an investigation, the project will develop and validate a prototype Decision Support System (DSS), which may help end users to evaluate pros and cons of specific security investments also on the basis of the societal perception of privacy and liberty.

Description of the work

The first year of the project is devoted to creating the baseline knowledge and designing a pan European survey on privacy and security; the second year is entirely devoted to carrying out and analysing the survey; the third year is devoted to developing a new Privacy Reference Framework for security technologies and the DSS.

WP1 explores the existing gaps in current approaches, available evidence, and modeling of public perception of privacy and security through a literature review from a number of domains, also taking into account deliverables of previous and current EC funded projects.

In *WP2*, the consortium designs and pilots the survey consisting of three real life scenarios - in which security technologies might affect privacy and fundamental rights - and background questions such as socio economic characteristics, perceptions of security and privacy as well as attitudinal and life style indicators.

In *WP3*, the consortium carries out the fieldwork by interviewing twenty-seven thousand individuals in the 27 EU countries. The fieldwork will be conducted via a self administered methodology using a combination of online methodologies and face to face approaches.

WP4 will focus on the analysis of the collected data using both descriptive and advanced quantitative techniques.

WP5 will exploit results from the previous WPs to develop a new conceptual Privacy Reference Framework for Security Technology (PRFST) covering levels of respect for privacy and liberty in different aspects of its descriptive scheme with illustrative descriptors scale.

WP6 will develop the PACT DSS, through a series of sessions among partners, with direct involvement of stakeholders.

WP7 is devoted to dissemination and the involvement of stakeholders.

Finally, *WP8* deals with project management and quality control.

Expected results

The PACT project is expected to provide a Decision Support System to decision makers giving them insight into the pros and cons of specific security investments taking into account a wider societal context. Furthermore, a Pan-European survey carried out in PACT will allow citizens, policy makers, scholars and other stakeholders to better grasp democratic questions of privacy, surveillance, and security and better understand the relationship between privacy and security.

PARTNERS	COUNTRY
VITAMIB SAS (VITAMIB)	France
ATOS SPAIN SA (ATOS)	Spain
CENTRE FOR IRISH AND EUROPEAN SECURITY LIMITED (CIES)	Ireland
MARKET & OPINION RESEARCH INTERNATIONAL LIMITED (IPSOS MORI)	United Kingdom
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
MINISTRY OF PUBLIC SECURITY (MOPS/IP)	Israel
NATIONAL CENTER FOR SCIENTIFIC RESEARCH “DEMOKRITOS” (NCSR Demokritos)	Greece
RAND EUROPE CAMBRIDGE LTD (RAND)	United Kingdom
INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)	Norway
UPPSALA UNIVERSITET (UU)	Sweden
CENTRE FOR SCIENCE, SOCIETY AND CITIZENSHIP (CSSC)	Italy

PRISMS / The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making

© kyoshino - istockphoto.com

Information

Grant Agreement N°
285399
Total Cost
€3,561,935
EU Contribution
€2,985,744
Starting Date
01/02/2012
Duration
42 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48
76139 Karlsruhe, Germany
Contact
Dr. Michael Friedewald
Tel: +49 (0) 721 6809 146
Fax: +49 (0) 721 6809 315
E-mail: michael.friedewald@isi.fraunhofer.de
Website:
http://www.prismsproject.eu

Project objectives

The PRISMS project will analyse the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It will examine how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance. PRISMS will determine the factors that affect public assessment of the security and privacy implications of a given security technology. The project will use these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Description of the work

The first phase of PRISMS begins with a multidimensional analysis of the relation between privacy and security from the different perspectives of technology, policy, media, criminology and law. These diverse perspectives offer an analytical background against which perceptions and attitudes of citizens can be studied. The consortium will determine the factors that affect public assessment of the security and privacy implications of a given security technology. Having analysed the conceptualisations of and interrelations between privacy and security, the consortium will test and validate its analysis in interviews, focus groups and workshops which will bring together various stakeholder groups (citizens, policy advisors, security people, societal organisations, criminologists, scientists).

The main outcome of the first project phase will be hypotheses about the relationship between privacy and security, trust and concern. These hypotheses will form the basis of a pan-European survey in the project's second phase. The survey will investigate the opinions, attitudes and behaviour of a representative sample of citizens on privacy and security. It will include 1,000 telephone interviews in each of the 27 Member States of the Union. This survey will allow us to identify the main driving factors that influence the forming of citizens' opinions on privacy and security and to make consistent comparisons between countries or regions in the EU.

In its third phase PRISMS will use these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives, taking into account a wide societal context. The decision support system will need to reconcile the various dimensions such that the results can be understood in terms of discriminating between options for security investments.

Expected results

- A better understanding of the iridescent terms "security" and "privacy" and their interrelationship;
- A model of how privacy and security attitudes of citizens are formed;
- A proposal for a participatory decision support process for an early assessment of emerging security technologies based on reconciling security, privacy and trust;
- Improving decision makers awareness of critical aspects of security technologies;
- Policy recommendations for ensuring human rights by design.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI)	Germany
Trilateral Research and Consulting LLP (Trilateral)	United Kingdom
Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (VUB-LSTS)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
The University of Edinburgh (UEdin)	United Kingdom
Eötvös Károly Public Policy Institute (EKINT)	Hungary
Zuyd University of Applied Sciences (Zuyd)	The Netherlands
Market & Opinion Research International Ltd. (Ipsos MORI)	United Kingdom

SAPIENT / Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies

© Sapient

RESEARCH
COMPLETED

Information

Grant Agreement N°
261698
Total Cost
€1,539,687
EU Contribution
€1,248,577
Starting Date
01/02/2011
End Date
31/07/2014

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Systems and Innovation Research
Breslauer Straße 48
76139 Karlsruhe,
Germany
Contact
Michael Friedewald
Tel: +49 (0) 721 6809 146
Fax: +49 (0) 721 6809 315
E-mail: michael.friedewald@isi.fraunhofer.de
Website:
www.sapientproject.eu

Project objectives

SAPIENT aimed to specify how and when smart surveillance should be used (or not) and the characteristics needed to be effective and scalable in order to rapidly adapt to changing situations. It aimed to provide stakeholders with a set of criteria for data protection and integrity that could be used to verify that surveillance systems and the sharing of information respect the privacy of citizens. The project developed a privacy impact assessment methodology tailored for surveillance projects and technology developments. Thisprovides the means for limiting the collection and storage of unnecessary data. The project focused on the necessity and proportionality of data collection needs to avoid undue threats to data protection and privacy. SAPIENT has paved the way towards an approach to surveillance where respect of the privacy of the citizen will be central.

Description of the work

The SAPIENT project defined and characterised smart surveillance within technological, social, political, legal, and ethical contexts. It analysed current studies of state-of-the-art of surveillance, and emerging technologies and related applications expected over the next decade.

The second step started the process of active stakeholder engagement through focus groups with participants having various views and interests on different applications of smart surveillance.

The SAPIENT team has also examined existing privacy impact assessment (PIA) methodologies and proposed a methodology suitable for the assessment of state-of-the-art and emerging surveillance technologies and related applications.

The suggested PIA was validated by a number of real-life test cases. These cases included smart CCTV, number plate recognition, situation awareness, and cloud computing. Based on lessons learned from these cases SAPIENT produced a Surveillance Privacy Impact Assessment Manual.

Moreover, a series of policy meetings and a final conference were held during the project to present its research results.

Results

The best way to limit the collection and storage of data and to fine-tune data collection needs and data protection requirements is to adhere to the principles of the EU's General Data Protection Regulation and to engage and consult with all relevant stakeholders by means of a privacy impact assessment methodology tailored to smart surveillance (i.e., a surveillance impact assessment).

SAPIENT tried to pave the way towards an approach to surveillance where respect of the privacy and of other values important to citizens are central by means of a surveillance impact assessment methodology. The lattercan be used by any organization in advance of developing and deploying a surveillance project. In this way, SAPIENT contributes to establishing surveillance impact assessments as a tool that governments and industry can use in security investment decisions to make sure that fundamental citizens' rights are well balanced with the need for security. Finally, companies may view surveillance impact assessments as akin to insurance or as a good investment – i.e., by identifying any problems early on, they will avoid potentially huge costs later on.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FhG)	Germany
Trilateral Research & Consulting LLP (Trilateral)	United Kingdom
Centre for Science, Society and Citizenship (CSSC)	Italy
Vrije Universiteit Brussel, Research Group on Law Science Technology & Society (VUB-LSTS)	Belgium
University of Lugano, Faculty of Informatics (USI)	Switzerland
King's College London, Department of War Studies (KCL)	United Kingdom
Centre for European Policy Studies (CEPS)	Belgium

SMART / Scalable Measures for Automated Recognition Technologies

© kalafoto - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261727
Total Cost
€4,202,156
EU Contribution
€3,456,017
Starting Date
01/06/2011
End Date
01/06/2014

Coordinator

UNIVERSITY OF MALTA (UOM)
Department of Information Policy and Governance
Msida
MSD 2080
Contact
Professor Joseph Cannataci
Tel: +356 2340 2782
E-mail: jcannataci@sec.research.um.edu.mt
Website: www.smartsurveillance.eu

Project objectives

The project's objectives were to :

» Determine the state of the art and likely future trends of smart surveillance, its proportionality and its impact on privacy;

» Identify the dependency and vulnerability of smart surveillance on underlying technology infrastructures and explore system integrity and privacy issues;

» Identify and explore smart surveillance and privacy issues in cyberspace;

» Map out characteristics of laws governing surveillance and identify lacunae as well as best practices;

» Explore the attitudes and beliefs of citizens towards smart surveillance;

» Establish best-practice criteria developed on the basis of operational efficiency, established legal principles and citizen perceptions;

» Develop a toolkit for policy-makers, police and security forces to implement and promote the best practice approach.

Description of the work

Four pillars of work were carried out:

» **Status quo analysis :** The project identified the current status of smart surveillance technologies already in use or about to be used in four key areas : border control, counter-terrorism and law-enforcement, consumer sector multi-purpose mobile devices and e-Government. The status quo analysis also mapped out characteristics of laws governing surveillance and identified lacunae/ new safeguards and gave special attention to mapping out characteristics of laws governing interoperability and data exchange.

» **Infrastructure analysis :** The project carried out risk analysis of the technologies utilised in underlying telecommunications network technology infrastructures as well as cyberspace.

» **Citizen attitudes :** Part of the project carried out qualitative research on the attitudes of citizens to smart surveillance and privacy. In addition, analytical bibliographies as well as a literature review was carried out on the sociology of surveillance in order to inform the overall analysis of citizen attitudes as well as the impact assessments produced in other streams in an effort to identify criteria for best practices.

» **Best practice and development of the toolkit for policy makers :** The SMART project developed a toolkit for policy-makers, and decision-makers to implement and promote best practices.

Results

SMART identified a great diversity in application of smart surveillance technologies. There appears to be a trend towards increased deployment and an intensification of the integration of large-scale identification technologies within the areas of border control, law and order and counter-terrorism, mobile communications, e-government, and cyberspace. At the same time there are serious concerns about the regulatory regime: the law is not prepared for the increased use of automated decision technologies. The legal environment in which smart surveillance operates in Europe is disjointed, lacking consistency in statue, application, and interpretation.

Citizens who contributed their views to the project showed that, while there is an acceptance that surveillance is a necessary function of modern society, there is also a marked level of anxiety and concern about surveillance deployment undertaken without the knowledge and consent of the wider population.

The project identified nine best practice criteria that could improve the promotion of privacy and data protection with smart surveillance technology use.

In addition, two key outputs of the SMART project with policy implications are (a) the model law and (b) a complementary toolkit. The model law introduces the concrete legal safeguards which have already been recognised as necessary by Europe's policy makers. The toolkit complements the model law by focusing attention on evidence of an evident mismatch between practice and the regulatory framework. It includes appropriate strategies and tools.

PARTNERS	COUNTRY
University of Central Lancashire (UCLAN)	UK
University of Ljubljana (UL)	Slovenia
Laboratorio di Scienze della Cittadinanza (LSC)	Italy
Babes-Bolyai University (BBU)	Romania
Universitetet i Oslo (UiO)	Norway
Universidad de Léon (ULE)	Spain
Law and Internet Foundation (LIF)	Bulgaria
Masarykova univerzita (MU)	Czech Republic
Edith Cowan University (ECU)	Australia
Georg-August-Universität Göttingen (UGOE)	Germany
University of Sheffield (SHEFU)	UK
Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Germany
Consiglio Nazionale delle Ricerche (CNR)	Italy
Univerzita Komenskeho v Bratislave (FMUNIBA)	Slovakia
Rijksuniversiteit Groningen (RUG)	Netherlands
University of Vienna (UNIVIE)	Austria
MORPHO (MORPHO)	France
Interpol (INTERPOL)	France
Universitat de Barcelona (UB)	Spain

SURPRISE / Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe

© Manuel Gutjahr - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285492
Total Cost
€4,396,297.56
EU Contribution
€3,424,109
Starting Date
01/02/2012
End Date
31/01/2015

Coordinator

OESTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
Institute of Technology Assessment
Strohgasse 45/5
A-1030 Vienna, Austria
Contact
Johann Čas
Tel: +43 1 51581 6581
Fax: +43 1 7109883
E-mail: jcas@oeaw.ac.at
Website: www.oeaw.ac.at/ita/welcome.htm

Project objectives

» Map key security challenges and related security policies and technologies;

» Identify factors influencing acceptability and acceptance of these security technologies;

» Identify technical design and legal/regulatory options and non-technical alternatives;

» Develop models and hypotheses about relations between privacy and security;

» Select two cases for empirical testing and perform a large scale participatory empirical testing of models;

» Synthesize empirical findings with theoretical models and practical options to design security solutions;

» Transform results into smaller scale participatory methods;

» Disseminate the findings widely throughout Europe and beyond.

Description of the work

SURPRISE re-examined the relationship between security and privacy, which is commonly positioned as a 'trade-off'. Where security solutions involve the collection of information about citizens, questions arise as to whether their privacy has been infringed. This infringement of individual privacy is sometimes seen as an acceptable cost of enhanced security. Similarly, citizens are seen as willing to trade-off their privacy for enhanced personal security in different settings. These common understandings of the security-privacy relationship, at both state and citizen levels, have informed policymakers, legislative developments and best practice guidelines concerning security developments across the EU. However, an emergent body of work questions the validity of the security-privacy trade-off, suggesting that this has over-simplified the consideration of the impact and acceptability of security solutions on citizens in current security policy and practice. Thus, the more complex issues underlying privacy concerns and public scepticism towards surveillance-oriented security solutions (SOSSs) may not be apparent to legal and technological experts.

In response to these developments, this project consulted with citizens from several EU Member and Associated States on the question of the security-privacy trade-off as they evaluate different security solutions. Through extensive preparatory work, the project identified and empirically examined the influence of a broad range of issues upon their evaluations. Using large scale citizen consultation meetings, a representative, fine-grained picture from across Europe was provided. Furthermore, citizens' understanding of privacy protection laws, their enforcement, and the acceptance levels of SOSSs, have been explained. Finally, a set of context-dependent dimensions for decision support concerning the acceptability of new SOSSs which promotes civil rights protection have been produced.

Results

The project involved about 2000 citizens from nine European countries in citizen "summits" and sitizen meetings to debate the relation between surveillance, privacy, and security. These participatory assessment activities confirmed the skepticism about the trade-off approach as a guideline for security policy.

Participating citizens requested that the protection of privacy and personal data should be strictly enforced, both in the context of commercial and law enforcement activities. The use of surveillance technologies should be justified and justifiable on a case-by-case basis; blanket mass surveillance is not accepted.

A key demand concerned safeguards for developing, implementing and using surveillance technologies in a way that effectively respects fundamental rights. Surveillance technologies should be subjected to comprehensive participatory technology assessments comprising privacy impact assessments and the integration of technical and organisational measures for a privacy compliant operation.

Concerning social cohesion the participants requested a more comprehensive, holistic and long-term approach to security, demanding a stronger focus on root causes of insecurity, i.e. tackling the enormous economic and social injustices resulting from the persistent economic crisis in Europe.

PARTNERS	COUNTRY
Oesterreichische Akademie der Wissenschaften (OEAW)	Austria
Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)	Spain
Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC)	Spain
Teknologiradet - The Danish Board of Technology (DBT)	Denmark
European University Institute (EUI)	Italy
VEREIN FUR RECHTS-UND KRIMINALSOZIOLOGIE (IRKS)	Austria
Medián Opinion and Market Research Ltd. (Median)	Hungary
Teknologiradet - Norwegian Board of Technology (NBT)	Norway
The Open University (OU)	United Kingdom
Akademien der Wissenschaften Schweiz Verein (TA-Swiss)	Switzerland
Unabhaengiges Landeszentrum fuer Datenschutz (ULD)	Germany

ASSERT / Assessing Security Research: Tools and Methodologies to measure societal impact

© istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
313062
Total Cost
€553,420.40
EU Contribution
€498,600.74
Starting Date
01/05/2013
End Date
31/07/2014

Coordinator

INSTITUTE FOR THE SOCIOLOGY OF LAW AND CRIMINOLOGY / INSTITUT FÜR RECHTS UND KRIMINALSOZIOLOGIE (IRKS)
Scientific Director: PD Dr. Reinhard Kreissl
Museumstraße 5/12
1070 – Vienna - Austria
Contact
PD Dr. Reinhard Kreissl
Tel: +43 1 526 15 16
Fax: +43 1 526 15 16 10
E-mail: ofice@irks.at
Website: http://www.irks.at

Project objectives

The need to consider the societal impact of EU security research has been acknowledged on many occasions by different actors. However, in traditional thinking, societal impacts are reduced to side effects of instrumental (technological and legal) security measures. This binary thinking has to be overcome.

ASSERT demonstrated that societal dimensions of security research could increase the variety pool of feasible solutions if taken into account from the very beginning of the “design process”.

Identifying and building on the state of the art in societal security research we identified best practice cases, exploring and assessing societal impacts of science and technology in the security domain and beyond. This was done in a multidisciplinary fashion from different perspectives, including end-users, stakeholders, researchers, evaluators, policy-makers, civil society and NGOs. Bringing together these different perspectives in a series of workshops created the basis for the development of a tool and a strategy for the sustainable implementation of societal impacts in future EU security research activities.

Description of the work

» Built a typology of the different ways that societal impact of security research is being assessed in security research programmes across the globe

» Analysed good practices of the exploration and assessment of the societal impact of broader areas of science and technology

» Assessed the extent to which these good practices are feasible and useful to security technology research

» Provided a user friendly knowledge base (online tool and database) to assist the European Commission in implementing the recommendations of ASSERT and other relevant research on assessing the societal impacts of security research

» Developed an online assessment tool for determining societal impact

» Organised a series of thematic workshops to engage with experts and stakeholders

» Organisde a “Master Class” for security research evaluators to discuss ASSERT results

» Broad engagement with experts and stakeholders along clearly identified intervention points through tailored dissemination strategies.

Results

- ASSERT produced an overview of good practices of the exploration and assessment of societal impact of broader areas of science and technology. This was made available as an entry in an internal Handbook (Encyclopedia) under: Reinhard Kreissl Florian Fritz, Lars Ostermeier: Societal Impact Assessment. *International Encyclopedia of the Social & Behavioral Sciences, 2nd edition* (http://dx.doi.org/10.1016/B978-0-08-097086-8.10561-6) 2015

- The database of experts and evaluators (full data protection compliance) is hosted with Partner Stirling Univ. and is accessible for use.

- Clear recommendations for mainstreaming security impact assessment tools and methodologies in security research have been distributed at two training events (master classes) in Stirling and Brussels

- A ready-for-use security research online impact assessment tool (SERIA) is available under http://assert.maisondx.com

- The ASSERT tool kit is being used for an online tutorial produced for the project SOURCE (Grant No. 313288)

- Findings from the ASSERT project flow into a project for the Austrian national security research to improve the cooperation between SSH and technological experts in security research. This project is in preparation and will be launched in 2016.

PARTNERS	COUNTRY
Institut für Rechts- und Kriminalsoziologie / Institute for the Sociology of Law and Criminology (IRKS)	Austria
Technical University Berlin (TUB)	Germany
Trilateral Research & Consulting LLP (TRI)	United Kingdom
King's College London (KCL)	United Kingdom
The University of Stirling (STIR)	United Kingdom
Hamburg-Consult Gesellschaft fuer Verkehrsberatung m.b.H. (HC)	Germany

COMPOSITE / Comparative Police Studies in the EU

© Hans van Rhoon – Erasmus University Rotterdam

Information

Grant Agreement N°
241918
Total Cost
€8,904,352.73
EU Contribution
€6,623,303
Starting Date
01/08/2010
Duration
48 months

Coordinator

ERASMUS UNIVERSITY ROTTERDAM
Rotterdam School of Management
Postbus 1738
3000 DR, Rotterdam
The Netherlands
Contact
Gabriele Jacobs
Tel: +31(0) 10 4082061
Mobile: +31(0) 6 57559341
Fax: +31(0) 10 4089015
E-mail: gjacobs@rsm.nl
Website:
www.composite-project.eu

Project objectives

Police forces all over Europe are faced with major challenges: new types of crime, open borders, new technologies, the threat of terrorism and tighter financial resources are but a few of the changes in European societies that affect the police. Many police forces react by changing their administrative structure, merging forces and modernizing tools and processes. Some of these changes reach their goals, but many fail or face serious problems along the way.

Within this context, the COMPOSITE project brings together a network of European academic and police institutions, to investigate how organizational and cultural factors facilitate or hinder successful change implementation in European policing.

In doing so, the COMPOSITE project aims to contribute to improvements in the planning and execution of change initiatives in the police, showing how these projects can be better aligned with the cultural and societal context per country, as well as how negative processes can be mitigated. In this way COMPOSITE seeks to enhance police capability and performance, both within individual police forces and across European joint operations.

Description of the work

The COMPOSITE project investigates change management practices in the police across 10 European countries. Based around 11 interconnecting work-packages, COMPOSITE seeks to identify the key triggers of change as well as the determinants of change processes and outcomes.

The project consists of two phases. In the first phase, work-packages investigate the *content* of current change programs in European policing, by analyzing the police's external challenges and identifying the internal resources and capabilities that serve to counter such threats. Other work packages in this phase research knowledge sharing and technology trends, providing insights into the organizational structures that promote change initiatives. The second phase of the research project focuses on change *processes* and on understanding the role of specific organizational features, national and organizational culture, identity, and leadership in the management of change.

The goal of COMPOSITE is not restricted to the extension of scientific knowledge and theory building. The project also aims to have strong practical outcomes, bringing about concrete improvements in the conception, planning, organization and implementation of change processes in European police forces. Thus COMPOSITE includes work packages focusing on dissemination, training and consultancy in order to reach relevant police communities and the general public alike. This dissemination process is further enhanced by the COMPOSITE photo project which runs alongside the main project, enriching the research process and facilitating the dissemination of results.

Expected results

The COMPOSITE project aims to provide a richer understanding of the key processes involved in police organizational change, as well as a range of practical tools and training solutions for police agencies, including:

» A comparative strategic analysis of strengths, weaknesses, opportunities and threats for police organizations in 10 European countries;

» Analysis of the planning and execution of change processes and best practices to meet current and future challenges;

» An annual European Police Monitor tracking how police forces across Europe are developing and improving.

PARTNERS	COUNTRY
Erasmus Universiteit Rotterdam	The Netherlands
University of Utrecht	The Netherlands
Police Academy, Apeldoorn	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Police Academy, Brandenburg	Germany
University of Durham	United Kingdom
Sheffield University	United Kingdom
University of Antwerp	Belgium
CNRS, Paris	France
Capgemini Telecom Media defence	France
University St. Kliment Ohridski, Skopje	Republic of Macedonia
Masaryk University, Brno	Czech Republic
Formit, Rome	Italy
Babes-Bolyai University, Cluj	Romania
Esade Business School, Barcelona	Spain

DESSI / Decision Support on Security Investments

© Jesus Conde - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261718
Total Cost
€1,902,303
EU Contribution
€1,561,095
Starting Date
01/01/2011
End Date
30/06/2013

Coordinator

DANISH BOARD OF TECHNOLOGY
Toldbodgade 12
DK-1253 Copenhagen
Denmark
Contact
Ida Leisner
Tel: +45 3345 5355
Fax: +45 3391 0509
E-mail: il@tekno.dk
Website:
www.securitydecisions.org,
www.tekno.dk

Project objectives

The DESSI project will develop a tool to support decision-makers in situations where different possible solutions for a perceived security-problem are available. It will enable comparison and evaluation of different security investments and serve as a way to achieve transparency of the security decisions.

Description of the work

There is an urgent need for a political framework whose underlying decisions on security investment are transparent and participatory, and which accounts for the context and multi-dimensionality of society. Security investments are made to avoid known or perceived threats. Threats could be conventional crime, cyber-crime, inner security, international conflicts, environmental hazards, and mixed forms of these.

It is important to first understand the nature of threats and their consequences, probability and impact (i.e., who is affected). Security investment implies choosing between different approaches to increasing security, and DESSI makes this choice explicit by describing and evaluating each security investment alongside its alternatives.

The DESSI tool will ensure decision-making process is explicit. The alternatives are identified or developed in a participatory process, including experts and stakeholders, who are informed by the threat description. Security investments can be highly controversial and disputed. This is not only because of political differences between actors but also due to societal phenomena (threat perceptions, technology insights, belief in alternative investments, etc.) which differently distributed and valued across all the actors. Accordingly, a rigorous investment assessment method needs to make use of a participatory approach which ensures this range of actors is taken on board.

Expected results

The DESSI project has created a novel procedure and a web-based decision support system to decision makers and users of security investments. The procedure and the decision support system (DSS) have been tested within the project and on several occasions afterwards. The consortium continues to develop the (DSS) and collaborate to further its use and development.

The DSS give stakeholders and decision makers insight into the pros and cons of specific security problems and investments. It contributes to a transparent and participatory decision making that accounts for the context and multi-dimensionality of society. As an additional feature not envisioned in the beginning of the project the DESSI procedure also prove to be an good method for user driven, open innovation, as participants are assisted in creating alternative strategies to address the security problems. It continues to be a useful procedure for public authorities, developers of security solutions, commercial enterprises and social organizations that have used the DESSI tool to make their own comprehensive assessment as an input to internal, strategic discussions and public debate.

PARTNERS	COUNTRY
Teknologiraadet - Danish Board of Technology (DBT)	Denmark
Peace Research Institute, Oslo (PRIO)	Norway
Teknologiraadet – Norwegian Board of Technology (NBT)	Norway
Verein für sozialwissenschaftliche Forschung und Beratung e.V. (SWFB)	Germany
Austrian Academy of Sciences, Institute of Technology Assessment (ITA)	Austria

ePOOLICE / early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems

© Thinkstock

Information

Grant Agreement N°
312651
Total Cost
€5,295,925.74
EU Contribution
€3,493,810
Starting Date
01/01/2013
Duration
36 months

Coordinator

INGENIERÍA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)
Defence and Security Division
Beatriz de Bobadilla, 3
E-28040 - Madrid - Spain
Contact
Raquel Pastor Pastor
Tel: +34 91 411 50 11
Mobile: +34 639 839 158
Fax: +34 91 411 47 03
E-mail: rpastor@isdefe.es
Website: www.epoolice.eu

Project objectives

The project aims at developing an efficient and effective environmental scanning system as part of an early warning system for the detection of emerging organised crime (OC) threats. The purpose is to improve LEA's situation in fighting OC by dealing with early signs of a emerging threats through a combination of technological resources and human actors.

Description of the work

ePOOLICE has been organized in different Work Packages:
WP1, Project Management and Coordination.
WP2 aims to ensure the commitment and involvement of End-users and other stakeholders in order to successfully achieve the project's goals; it will push the development of the methodological part of the project.
WP3 deals with the technical and legal/ethical constraints and the design of the system framework considering the user requirements (from WP2) and the relevant ethical and legal issues. WP4 will develop and define a data model for the Environmental Knowledge Repository (EKR) as a common, uniform representation of extracted information for WP5 Environmental radar, as well as for the derived fused information, inferred knowledge, hypothesis, etc. in WP6. WP7 comprises development of end-user tools for alert visualization and situation assessment, based on the signals and data captured by the radar. WP8 is responsible for the integration of the tools developed, considering the framework design in WP3. Finally dissemination and exploitation tasks are covered in WP9.

Expected results

ePOOLICE will support LEAs:

» to scan the environment to feed new and emerging threats into the serious and organised crime threat assessment processes

» to map changes within the OC situations that impact the security of the European Union Member States

» to enable the strategic decision makers to counterbalance detected upcoming threats before they materialize

by:

» using feedback from analysts to distillate and propose new indicators/signals and adjust its warning/alert levels;

» discovering and proposing new sources to be scanned;

» evaluating and estimating the importance of sources;

» providing more effective information into foresight to fight all sorts of organised crime.

» providing a better understanding of the new and upcoming technologies and trends, leading to the strategic planning into security issues of all stakeholders

PARTNERS	COUNTRY
Ingeniería de Sistemas para la Defensa de España SA (ISDEFE)	Spain
Aalborg Universitet (AAU)	Denmark
Commissariat a l Energie Atomique et aux Energies Alternatives (CEA)	France
Thales Communications & Security SAS (TCS)	France
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V. (FKIE)	Germany
Universidad de Granada (UGR)	Spain
Sheffield Hallam University (SHU)	United Kingdom
Inthemis (INTHE)	France
Legind Technologies AS (LTA)	Denmark
SAS Software Limited (SAS)	United Kingdom
Ministerio del Interior (MIR-GUCI)	Spain
West Yorkshire Police Authority (WYP)	United Kingdom
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Italy
Fachhochschule fur Offentliche Verwaltung und Rechtspflege in Bayern (FHVRP)	Germany
European Police Office (EUROPOL)	The Netherlands
Institutet for Fremtidsforskning Forening (CIFS)	Denmark
Thales Nederland BV (TRT-NL)	The Netherlands

ETTIS / European security trends and threats in society

© alexander kirch - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285593
Total Cost
€2,823,373.40
EU Contribution
€2,285,586.13
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

PEACE RESEARCH INSTITUTE OSLO
Security Dimensions Department
Hausmannsgate 7
PO Box 9229 Grønland
NO-0134 Oslo
0186 – Oslo – Norway
Contact
J. Peter Burgess
Tel: +47 22 54 77 38
Mobile: +47 909 23 949
Fax: +47 22 54 77 01
E-mail: peter@prio.no
Website: www.ettis-project.eu

Project objectives

The main goal of the project was to provide the means to establish a sustainable process of anticipating emerging threats to society and to societal security, and to translate them into research priorities. In the identification of research priorities, particular emphasis was put on the role of European policy to support the realisation of these collective priorities.

The ETTIS project met these objectives through the following substantive and methodological sub-objectives. It has:

» carried out an identification, integration and scenario-based assessment of:

- possible future **threats** resulting from trends, trend breaks and weak signals in technology and society;
- security-related **needs** of first responders, policy-makers and society at large;
- research-based **security opportunities** (using portfolio analysis, robust and adaptive strategies of priority-setting, new intelligence tools);
- comprehensive analysis of results and approaches of completed, ongoing and – to the extent possible - planned security research projects.

» Systematically derived a portfolio of **research priorities** that was geared towards the needs of user organisations, and rationales for policy intervention and the respective roles of European and national research and innovation policy;

» Developed a **methodological approach** for threat- and needs-based identification of research priorities, and generalized it as part of a continuous monitoring and assessment process and tested its applicability with stakeholder organisations;

» Helped increase the awareness of and attention to new insights generated by research among **first responders, policy-makers and industrial strategists**, as well as in wider **societal debates about civil security**. This included the identification of barriers and limitations to the uptake of research results;

» Assessed the relevance and success of the research.

The approach to be developed in ETTIS aimed to leave an imprint on the way future threats are to be dealt with in the future.

Description of the work

The underlying strategy of the ETTIS work plan had three main approaches:

» It took a broad and integrated approach to security that considered shifts in human/societal systems, reflecting the approach increasingly evident in the security strategies of more Member States and the EU;

» It seeked to adapt available research tools and results to better understand emerging threats and needs;

» It adopted an adaptive planning paradigm that addressed the security challenges in the dynamic, uncertain and complex security environment that our societies face, both in concept and in practice.

The project's work plan also included various dissemination activities as well as an important task devoted to identifying individual stakeholders, creating a taxonomy of stakeholders and identifying their interests, needs and drivers. This task, carried out early on, provided the basis for engaging stakeholders by means of interviews, focus groups, workshops and other means throughout the project and ensured that the consortium's analyses, findings and recommendations were based on stakeholder reality.

Results

ETTIS: *European Security Trends and Threats in Society* was a collaborative research project that ran from January 2012 to December 2014. ETTIS has contributed to a renewed conceptualisation of key elements of policy and priority setting in the field of security, in view of promoting societal security in Europe. ETTIS proposed an operational concept of societal security to support decision makers and end-users in practical settings.

It developed a taxonomy of R&I models, better suited to cover the broader boundaries of societal security, based on the rate of change and the type of concerns at stake. ETTIS developed tools, methodologies and processes to assist researchers and policy makers identify threats, needs, and solutions within the societal security domain. This includes a three-step process for the elaboration of context-based threat scenarios and subsequent identification of threats and societal security needs. Finally, ETTIS has developed an innovative method to identify research priorities and set research agenda for societal security by putting forward an adaptive four-phase model of planning. Potentially, this model has far reaching positive effects in socio-economic terms.

PARTNERS	COUNTRY
Peace Research Institute Oslo (PRIO)	Norway
Totalförsvarets Forskningsinstitut (FOI)	Sweden
DEN HAAG CENTRUM VOOR STRATEGISCHE STUDIES (HCSS)	The Netherlands
TRILATERAL RESEARCH & CONSULTING LLP (TRI)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI-INT)	Germany
CENTRE FOR IRISH AND EUROPEAN SECURITY (CIES)	Ireland
AUSTRIAN INSTITUTE OF TECHNOLOGY GmbH (AIT)	Austria
Morpho (MPH)	France
MAGEN DAVID ADOM (MDA)	Israel
Police Service of Northern Ireland (PSNI)	United Kingdom

EvoCS / The evolving concept of security: A critical evaluation across four dimensions

RESEARCH **COMPLETED**

Information

Grant Agreement N°
605142
Total Cost
€
EU Contribution
€882,201
Starting Date
01/06/2014
End Date
30/11/2015

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER)
Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT
Appelsgarten 2
53879 Euskirchen
Germany
Contact
Dr. Miloš Jovanović
Tel: +49 2251 18-265
Fax: +49 2251 18-38-265
E-mail: milos.jovanovic@int.fraunhofer.de
Website: www.evocs-project.eu

Project objectives

The EvoCS project dealt with 'evolving security concepts' as discussed in a public security context. These security concepts were made up of and modelled in multiple dimensions, the latter applying to documents from different source types, from government policy documents to newspapers and academic publications. These sources were chosen to produce a broad data base that reflected the written public security discourse. In total, EvoCS used and analysed over 4000 items. This high number was necessary to reach the goal of "providing a holistic view on the subject", i.e. the popular security discourse.

Description of the work

Our researchers used a process called "coding", i.e. characterising each item in relation to EvoCS' five dimensions. This captured documents between November 2013 and October 2014. In the second stage, analysis was broadened to include documents from 2004 to 2013. In this stage researchers did not code the documents, but analyzed them via classical desktop research to put the results into a broader historical perspective. Thus a quantitative-objective approach (the coding of the five dimensions) was combined with a qualitative-subjective approach (desktop research) to produce a comprehensive view on the public security discourse.

The five dimensions were:

1. Core values (e.g. Physical safety and security);

2. Actors (e.g. the government);

3. Levels (e.g. the national level);

4. Ethics and human rights, and

5. Security challenges (e.g. terrorism or climate change).

Results

The EvoCS project mapped the security discourses in selected EU member states and candidate countries. It concluded the following:

First, the concept of security in the EU is shifting from a state-centric model to one focused on the citizen. In the majority of analyzed countries the most salient core values were directly linked to the safety of individuals rather than that of the state. The most important value was "physical safety and security", which included threats such as corruption, natural hazards, cybercrime, road accidents, terrorism, both organised and petty crime, energy and food supply, and illegal migration. Even though some of these threats are traditionally associated with state security, EvoCS found that they were always discussed with regard to their implications for the individual citizen. Further, high salient core values linked to economic growth and political stability support this view of the citizen taking centre stage in EU security.

Second, this shift from state-centred to citizen-centred security is more dominant in the western EU countries than in eastern ones. In the former, the emphasis in the security discourse is on terrorism, cybersecurity and natural hazards, which are the most important threats to several core values – mostly safety of citizens in the physical and economic sense. In the latter region, the state is seen by citizens as largely weak, prone to external coercion, and thus insecure. Important themes in their security discourse were the Ukrainian crisis and Russian policies towards the former communist bloc; both are seen as a threat to the independence and territorial integrity of the state.

Third, citizens across Europe expect the state rather than the EU to address security threats. In all regions the security discourse focuses on the national government as the proper level of action to fight threats, improve resilience or recover from damages, and rarely addresses the EU in this regard. In other words, security is perceived across Europe as a national issue. Yet, expert-level documents discuss the utility of the EU for security. This finding suggests that even though the EU contributes to security, its efforts are of limited visibility, which may undermine people's perception of the importance of the EU.

PARTNERS	**COUNTRY**
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Istituto Affari Internazionali (IAI)	Italy
Polski Instytut Spraw Międzynarodowych (PISM)	Poland
The Hague Centre for Strategic Studies (HCSS)	The Netherlands
Scuola Superiore Sant'Anna di Studi Universitari e di Perfezionamento di Pisa (SSSUP)	Italy
Loughborough University (LUNI)	United Kingdom
Università Cattolica del Sacro Cuore	Italy
Procon Ltd.	Bulgaria

FESTOS / Foresight of Evolving Security Threats Posed by Emerging Technologies

© Nmedia - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217993
Total Cost
€971,799.62
EU Contribution
€824,552.7
Starting Date
01/03/2009
End Date
31/12/2011

Coordinator

INTERDISCIPLINARY CENTER FOR TECHNOLOGY ANALYSIS AND FORECASTING
Tel-Aviv University
69978 RAMAT AVIV,
TEL AVIV
Israel
Contact
Yair Sharan
Tel: +972 36407574
Mobile: +972 544381600
Fax: +972 36410193
E-mail: sharan@post.tau.ac.il
Website: www.festos.org

Project objectives

Analysing technological and societal developments over the next 20 years and beyond, this foresight study aimed to identify and assess security threats that could stem from recently developed or upcoming science and technology (S&T) breakthroughs.

FESTOS' overall strategy was based on three pillars of research:

» horizon scanning: identification of potentially threatening new technologies and field of techno-science research;

» evolving threats: assessment of emerging threats, construction of related threat scenarios, their impact on society and development of early-warning indicators;

» pathways towards solutions: developing preparedness measures and policy guidelines.

Results

FESTOS mainly focused its research on the fields of nanotechnology, biotechnology, robotics, new materials and information and communications technology (ICT). It also examined crime and terrorism as potential threats, but excluded industrial accidents or other potential disasters.

The project carried out a comprehensive literature scan of current and upcoming emerging technology research. This resulted in a report that categorised and provided an initial threat assessment of 80 potential technologies of interest. Some 288 experts participated in a survey where they were asked to assess the risk potential of leading future technologies, and to estimate a timeframe for each threat's realisation.

The result is a database of potentially abusable technologies, including a potential timeframe for their entry into the market. Potential misuse falls into three categories, namely the:

» the disruption of certain technological applications for malicious purposes;

» increased access to technologies previously confined to the military, specialist industry or unique heavily funded laboratories;

» surprising malicious use of new technologies developed for completely different, beneficial purposes.

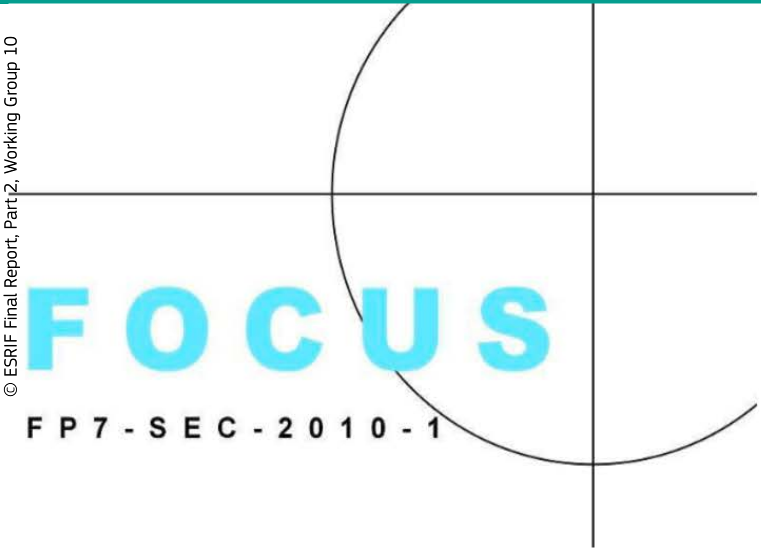
Each category of threats was divided into short, medium and long term timeframes of concern, with Category 3 ("surprising malicious uses") deemed as the high priority area since it can include a "wild card" exploitation of new technologies not previously associated with a security risk.

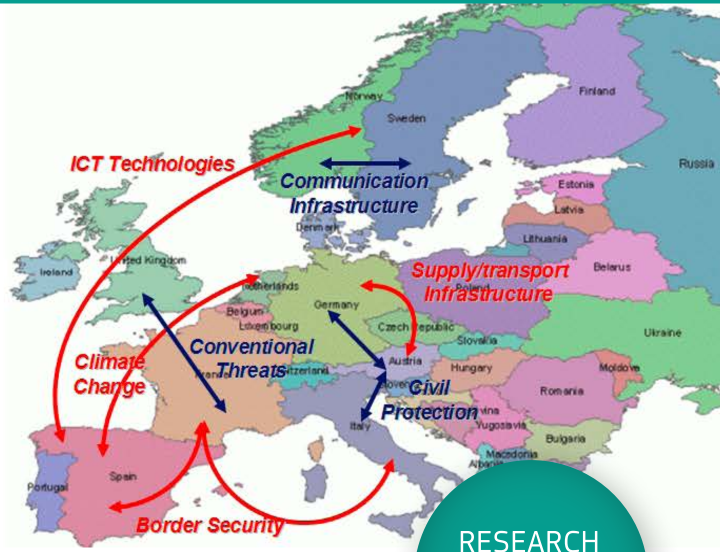
The potential wild card scenarios that were examined include a large-scale nano-technology out-break, swarms of robotic "cyber insects", the use of genetic engineering for personal blackmail and the creation of infectious viruses capable of altering human behaviour (eg. heightened aggression or depression).

By applying these assessments to different national contexts across the EU, the consortium came up with a series of policy recommendations and guidelines for national authorities and the EU on how to conduct their own risk assessments in these fields.

PARTNERS	COUNTRY
Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF)	Israel
Turku School of Economics, Finland Futures Research Centre	Finland
Foundation for European Scientific Cooperation	Poland
EFP Consulting	United Kingdom
Technical University of Berlin	Germany
Uniwersytet Lodzki	Poland

FOCUS / Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles





© ESRIF Final Report, Part 2, Working Group 10

RESEARCH COMPLETED

Information

Grant Agreement N°
261633
Total Cost
€4,372,012
EU Contribution
€3,407,075
Starting Date
01/04/2011
End Date
31/03/2013

Coordinator

SIGMUND FREUD PRIVATUNIVERSITAT WIEN GMBH
CEUSS | Center for European Security Studies
Schnirchgasse 9a
1030 Vienna
Austria
Contact
Alexander Siedschlag
Tel: +43 (0) 1 798 62 90 50
Mobile:
+43 (0) 699 113 69 717
Fax:
+43 (0) 1 798 62 90 52
E-mail: siedschlag@european-security.info
Website:
http://www.focusproject.eu

Project objectives

FOCUS will help shape European security research to enable the EU to effectively respond to tomorrow's challenges stemming from the globalization of risks, threats and vulnerabilities.

FOCUS will concentrate on alternative future EU roles to prevent or respond to incidents situated on the "borderline" between the internal and external dimensions of the security affecting the Union and its citizens. It will do so by elaborating multiple scenarios, based on IT-supported foresight, in the form of alternative futures. These will be plausibility-probed versus mere threat scenarios.

The main contribution of FOCUS is to develop an effective long-term foresight and assessment tool at the EU level, populated with the analyses carried out by the project. Moreover, FOCUS will deliver tangible products (such as an IT platform) and contents (i.e., a roadmap) for planning research and deciding on priorities. These products are usable beyond the project.

Description of the work

FOCUS will design and apply an "embedded scenario" method of integration. This will delineate options for future tracks and broadened concepts of security research within broader scenarios that involve EU roles for responding to transversal challenges (whose causes are external but whose effects are internal to the EU). This will be performed along five big themes:

» different tracks regarding the comprehensive approach as followed by European institutions, Member States and international strategic actors – including links between the internal and external dimension of security;

» natural disasters and environment-related hazards, with an emphasis on comprehensive risk reduction, civil protection and reconstruction;

» critical infrastructure and supply chain protection, centred on preventing, mitigating and responding to exogenous threats that could have a significant impact on EU citizens;

» the EU as a global actor regarding the so-called "wider Petersberg Tasks", and building on EU and member state instruments and capability processes;

» the evolution of the EU's internal framework and prerequisites for delivering a comprehensive approach, including Lisbon treaty provisions and relevant strategies (e.g. for engagement with other international actors) as well as ethical acceptability and public acceptance.

The "embedded scenario" method and IT-based tools will be adjusted and sharpened as applied to these five thematic scenarios. Interrelations among themes and scenarios will be particularly addressed: FOCUS will investigate cross-cutting issues that constitute transversal key drivers/constraints. The project will explore interfaces and translation mechanisms by which exogenous threats – such as those stemming from global change – directly confront EU citizens, their perception and their actual state of security. It will also take into account the differential impact of external threats on national and European research programmes designed to enhance capabilities.

Results

FOCUS elaborated five indicative scenarios to frame the alternative future security roles the EU could play by the year 2035. The aim was to use these scenarios to derive the future security research needed to support those EU roles. The 2035 scenarios were:

» The EU evolves into a common "securitisation model". It rests on a much closer integration of national security research programmes with that of the EU to help Europe deal with security incidents.

- By 2035, competing national and regional policies beyond their borders are producing an increasingly fragmented world, split into tiny privileged elites versus the teeming masses of "have-nots." The rapidly evolving risk for everyone is a disastrous collapse of society and civilisation.

- Security management is a risk-driven process. Collaboration between international organisations, member states, EU bodies, civil society organisations and the private sector via security data compilation, crowd sourcing and information sharing has led to the establishment of a harmonised risk management approach.

- The EU's policy to counter cyber-attacks is paramount since this form of societal defence has become all-encompassing for Europe's economic, industrial, and scientific development. Continuous cooperative vulnerability assessments involving as many countries as possible have become a priority.

- The EU is the governing authority of scientific and technological innovations related to security of the citizen. Capability development leads to a convergence of research in the fields of civil security, policing needs, emergency response, and disaster management. This links the EU's internal decision-making structures to its external strategic environment.

FOCUS's foresight work led to its ultimate result: an IT-based interactive roadmap for security research. Based on the project's five indicative scenarios, it allows users to modulate its parameters to determine their most appropriate future research options.

PARTNERS	COUNTRY
SIGMUND FREUD PRIVATUNIVERSITAT WIEN GMBH (SFU-CEUSS)	Austria
ATOS ORIGIN SOCIEDAD ANONIMA ESPAÑOLA (ATOS)	Spain
BOC ASSET MANAGEMENT GMBH (BOC)	Austria
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (CSDM)	Bulgaria
CROSS-BORDER RESEARCH ASSOCIATION (CBRA)	Switzerland
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)	Spain
CESKE VYSOKE UCENI TECHNICKE V PRAZE (CVUT)	Czech Republic
SECEUR SPRL (SECEUR)	Belgium
UNIVERSITAET FUER WEITERBILDUNG KREMS (DUK)	Austria
UNIVERSITY OF HAIFA (U HAIFA)	Israel
UNIVERSITAET FUER BODENKULTUR WIEN (BOKU)	Austria
INSTITUTO NACIONAL DE TECNICA AEROESPACIAL (INTA)	Spain
CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)	Germany

FORCE / FOResight Coordination for Europe

Information

Grant Agreement N°
607858
Total Cost
€1,056,513.40
EU Contribution
€930,510.74
Starting Date
01/04/2014
Duration
24 months

Coordinator

EFPC (UK) LTD
19 Broomburn Court, 14
Broomburn Drive
G77 5JG - Newton Mearns
Scotland
Contact
Michael Remes
Tel: +44 141 563 6853
Mobile: +972 544 801 255
Fax: +972 893 27362
E-mail:
michael@efpcgroup.com
Website: www.efpcgroup.com

Project objectives

» To examine previous Security Research foresight studies and horizon-scanning activities in FP7 and elsewhere in Europe

» To produce, based on this work, a foresight model and intelligent decision support system (IDSS), which is scalable with future foresight research activities conducted in Europe. These tools will help policy makers and stakeholders in the security domain do strategic planning with regard to relevant trends and threats by using methodologies and information from available studies.

Description of the work

FORCE activities will include:

» Examining outputs from Security Research projects funded in FP7 and other sources related to foresight and horizon-scanning activities via: literature review, workshops; interviews; collaboration with national and international foresight networks

» Assessing methods used in security foresight studies in the last five years regarding their strengths and weaknesses

» Identifying possible gaps between potential future threats and methods used so far

» Producing a foresight model that isscalable and sustainable beyond the project's life

» Developing the IDSS as an end-user tool and producing and running test scenarios against which the system can be evaluated

» Supporting the visibility and take up of security research results at stakeholder level, especially vis-a-vis end users through dissemination of the foresight model and corresponding IDSS

Expected results

A foresight model (including online mapping tool for interrogating available security related foresight studies, methodologies and tools) and an Intelligent Decision Support System (IDSS) to help identify emerging threats and other factors for policy makers and security stakeholders. These tools will be evolvable and sustainable beyond the end of the project.

PARTNERS	COUNTRY
EFPC (UK) Ltd (EFPC)	United Kingdom
Globaz, S.A. (GLOBAZ)	Portugal
Technische Universitat Berlin (TUB)	Germany
Inovamais – Servicos De Consultadoria Em Inovacao Tecnologica S.A. (INOVA+)	Portugal
Tel Aviv University (TAU), the Unit for Technology and Society Foresight	Israel
Atos Spain S.A.	Spain

FORESEC / Europe's evolving security: drivers, trends and scenarios

© Cornelius - Fotolia.com

Information

Grant Agreement N°
218199
Total Cost
€942,202
EU Contribution
€942,202
Starting Date
01/02/2008
End Date
30/11/2009

Coordinator

CRISIS MANAGEMENT INITIATIVE
Pieni Roobertinkatu 13 B
24-26
00130 Helsinki
Finland
Contact
Kristiina Rintakoski
Tel: +358 9 4242 810
Fax: +358 9 4242 8110
E-mail:
kristiina.rintakoski@cmi.fi
Website:
http://www.foresec.eu

Project objectives

FORESEC was a foresight project aimed at assessing the evolution of Europe's security landscape in the coming decade. Its goal was to identify likely upcoming security threats, and to categorise the potential added value in EU-level action for tackling such threats. Finally, the project sought to suggest research priorities to support these goals.

To fulfil this objective, FORESEC decided to create – or where it already existed strengthen – networks of experts from across various professions and backgrounds in European security.

Results

The main output of FORESEC was a series of specialist reports. These included 12 country reports on national security strategies, a global trends report, a concept paper on European security, a threat taxonomy assessment and a scenario development report.

These key publications can be found for public consumption at: www.foresec.eu

The development of an interactive web site for stakeholders and the professional networking undertaken during the projects workshops can also be seen to have contributed to the development of security expert groups at the EU level.

A particular focus of this research was on the potential added value of EU level cooperation in security. FORESEC research shows that the EU's combination of "effective multilateralism" – the benefits of international institution membership, resource and knowledge sharing – combined with the EU's natural comparative advantage in combining civilian, military and diplomatic spheres, are all positive contributions to Member State security policy. EU level policy also allows smaller states to benefit from capabilities and insights beyond their individual means.

Yet despite these advantages, FORESEC research – including six national research workshops – shows that a shared concept of security does not yet exist amongst Member States. An appreciation of national approaches is thus encouraged.

Looking forward, FORESEC recommends that future security research should shift from a state centric approach to one that acknowledges the comprehensive and citizen-centred strategies now advocated in most national security strategies.

PARTNERS	COUNTRY
Crisis Management Initiative	Finland
Austrian Research Centres System Research	Austria
International Institute for Strategic Studies	United Kingdom
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Centre for Liberal Studies	Bulgaria
European Commission - Joint Research Centre (JRC)	Italy

SIAM / Security Impact Assessment Measures

© L Robert Wilson - Fotolia.com

Information

Grant Agreement N°
261826
Total Cost
€2,777,307.68
EU Contribution
€2,168,640
Starting Date
01/02/2011
Duration
36 months

Coordinator

TECHNICAL UNIVERSITY BERLIN
Centre for Technology and Society
Human Technology Lab
Hardenbergstraße 16-18
10623 Berlin,
Germany
Contact
Dr. Leon Hempel
Tel: +49 (30) 314 25373
Mobile:
+49 (0) 176 111 20 400
Fax: +49 (30) 314 26917
E-mail:
hempel@ztg.tu-berlin.de
Website:
www.siam-project.eu

Project objectives

The SIAM decision support system will ease the complexity associated with the assessment of security measures and technologies. Where today decision makers have to oversee a wide range of relevant knowledge from different academic fields and national and cultural interests, SIAM will provide knowledge needed for assessing security technologies in a structured manner. The objective of SIAM is to produce a SIAM database and guidelines that allow quick access to information, not only on the effectiveness and the cost-benefit ratio but also on societal, ethical and legal aspects of security technologies. The interdisciplinary character of SIAM makes it unique. The participation of seven leading academic institutions from five countries and partners in the security research guarantees a high level of variety of perspectives. Additionally, the involvement of end users provides an empirical base for the theoretical research.

Description of the work

SIAM will combine various methodologies to conduct the research. SIAM entails four case study partners to gather field information in security measures and technologies (SMTs) as well as counter infringement technologies (CITs). The new capital airport Berlin Brandenburg International (BBI) will introduce state of the art technologies and will be one of the most modern airports on the European continent. SIAM will also compare airport security with the well established Ben Gurion Airport Tel Aviv, which uses a different approach in airport security. As a contrasting case, SIAM also focuses on the public transportation systems of London and Turin. SIAM will compare the London transportation, which is large and long standing, with the newly constructed full automatic transportation system in Turin. By conducting these four case studies featuring a significant level of security measures and technologies, SIAM integrates the practical experience with such technologies into the decision support system, as it will be flanked by extensive literature reviewing and the gathering of the knowledge of Europe's leading security and civil rights experts. The practitioner perspective will be extended by state of the art knowledge. SIAM will also complement the state of the art of SMTs and CITs by analyzing research projects for future technologies. This will be accomplished by conducting Delphi studies and interviews with leading experts in this domain of research.

SIAM is also analyzing threats towards SMTs and its efficiency and effectiveness to counter them. By analyzing past incidents, SIAM will develop threat scenarios on which it will test the implemented and future technologies.

Focus is also directed at freedom infringements by SMTs and at how effective CITs can be implemented. The legal dimension of technology assessment will be scrutinized in order to take accountability and transparency criteria into account when assessing SMTs.

Beyond that, SIAM is building an actor network to initialize the relationships needed for sustained cooperation and future fruitful interaction in the field of security. Participative elements such as stakeholder conferences open up the security field to a wider public and include more actors in the process.

Expected results

To decide on new SMTs is a complex task that requires the decision maker to evaluate a great number of heterogeneous aspects. SIAM ties together these aspects and reduces their complexity by providing a number of guidelines and a database for easy decision making. One major impact is that SIAM will continue to close this gap between the threat perspective and the freedom perspective that still characterizes the security field strongly. This will help to protect the freedom of European citizens and passengers, foster accountability and transparency in the use of security technology and help to avoid economic loss caused by investment flops and a lack of acceptance.

PARTNERS	COUNTRY
Technical University Berlin (TUB)	Germany
University of Kassel (UNIKASSEL)	Germany
University of Newcastle (UNEW)	United Kingdom
Kingston University London (KU)	United Kingdom
Higher Institute on Territorial System for Innovation Torino (SITI)	Italy
Tel Aviv University (ICTAF)	Israel
Vrije Universiteit Brussels (VUB)	Belgium

BESECURE / Best practice Enhancers for Security in Urban Regions

© TNO

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285222
Total Cost
€4,321,420.40
EU Contribution
€3,468,092
Starting Date
01/04/2012
End Date
31/03/2015

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK
TNO Behavioural
and Societal Sciences
Schoemakerstraat 97
PO Box 6060
2600 JA Delft,
The Netherlands
Contact
Heather Griffioen-Young
Tel: +31 8886 65931
Mobile: +31 6224 61065
Fax: +31 3463 53977
E-mail:
heather.griffioen@tno.nl
Website:
www.besecure-project.eu

Project objectives

Urban security is a complex challenge to modern urban environments. Many factors influence urban security, from the physical layout to the social and economic makeup of urban zones, from the national landscape to the daily practices of local public services. Europe has seen rapid expansion of its urban environments, and the rise of new types of communities due to migration, economic tensions and social developments. Unfortunately, this has also resulted in recent instances of urban unrest and failing urban regeneration plans. These developments demand a better understanding of urban security throughout Europe, and a more sensible policy development to create safer urban environments.

The BESECURE project aimed to contribute to this challenge through comparative exploration of urban security in Europe, and providing policy makers with shared knowledge and informative policy support tools.

Description of the work

Recent instances of urban unrest have once again shown that seemingly small events can trigger a sudden escalation of unrest in neighbourhoods that have been under social tension for a prolonged period of time. In order to prevent such escalations, policy makers should understand the interdependency of factors that affect the urban area in question, and base their policies on that comprehension. However, in reality, most decisions are made on the basis of local, long-standing best practices. Given the universal importance of urban security, it is vital to share knowledge and practices among stakeholders throughout Europe, and to jointly work on a better common understanding of urban security.

The project 'Best practice Enhancers for Security in Urban Regions' (BESECURE) worked towards a better understanding of urban security through examination of different European urban areas. In each area, the BESECURE project interacted with local policy makers and stakeholders to learn local best practices on urban security, and on which basis they are made. This included an appreciation of the data and background information available to policy makers, and a characterisation of the area on aspects relevant to urban security, such as social and cultural makeup of the target area, the economic state, crime rates and the public perception of security. By comparing the outcomes of the case studies, the BESECURE project gained a comprehensive understanding of the underlying factors that impact the effectiveness of urban security policies. The knowledge and data gathered throughout the project were used to devise tools that can alert policy makers to security issues in their target area and help them comprehend the effectiveness of their interventions.

The BESECURE project worked with the following urban regions: Belfast (UK), The Hague (NL), Freiburg (GER), London Tower Hamlets (UK), London Lewisham (UK), Naples (IT), Reggio di Calabria (IT), Poznan (PL).

Results

The BESECURE project aims to improve the way policy makers use knowledge, experiences and data in the urban security decision-making processes. We developed novel tools that emphasize knowledge sharing and evidence-based policy design, grounded in an extensive review of urban security practices from across Europe. Through case studies in eight urban areas (Belfast, The Hague, Freiburg, London Tower Hamlets and Lewisham, Naples, Reggio di Calabria, Poznan), we gathered a wide set of practices that give inspiring insights into urban security approaches across Europe. These practices were captured through a robust information structure that enables analysis, comparison and sharing. The BESECURE support system brings these innovations together through three interconnected platforms. The Inspirational Platform helps policy makers find relevant practices from other cities from a repository of practices and publications. The Urban Data Platform provides easy-to-use data visualisation and analysis features, and includes an early warning system that can project the evolution of data into the near future. The Policy Support Platform guides users through a step-wise policy design process, and helps build up an evidence-base from stored practices and publications. The system also includes a versatile risk-assessment tool that allows for critical assessment of a policy proposals.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
University of Ulster (UU)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
Albert-Ludwigs-Universität Freiburg (ALU)	Germany
ITTI Sp.zo.o. (ITTI)	Poland
The Stephen Lawrence Charitable Trust (SLCT)	United Kingdom
Downey Hynes Limited (DHP)	Ireland
JVM Limited (JVM)	United Kingdom
Crabbe Consulting Ltd. (CCLD)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR)	Italy
Università degli Studi Mediterranea di Reggio Calabria (UMRC)	Italy
Experian Nederland BV (EXP)	The Netherlands
Stichting Dr. Hilda Verwey-Jonker Instituut (VJI)	The Netherlands
Institute for Housing and Urban Development Studies B.V. (EUR)	The Netherlands

EUSECON / A new agenda for european security economics

© 2 JEN- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218105
Total Cost
€3,009,542.74
EU Contribution
€2,357,188
Starting Date
01/03/2008
End Date
30/04/2012

Coordinator

GERMAN INSTITUTE FOR ECONOMIC RESEARCH
Department of International Economics
Mohrenstr. 58, 10117 Berlin
Germany
Contact
Prof. Dr. Tilman Brück
Tel: +49 30 89789 591
Fax: +49 30 89789 108
E-mail: tbrueck@diw.de
Website: www.economics-of-security.eu/eusecon

Project objectives

EUSECON strives to create an analytical framework for complementary research within the discipline of security economics. This framework relates human-induced insecurity (terrorism and organised crime) to other forms of insecurity (industrial accidents, natural disasters, geopolitical insecurity) and security measures.

Beyond creating this framework and defining the field of security economics, EUSECON provides policy advice for security policy makers, security research programme makers, and security research analysts. This is achieved by focusing scholarship on the relationships between human-induced insecurity (terrorism and organised crime), security provision, and the prevailing socio-economic policy framework.

EUSECON will investigate the relationship between security, insecurity, and the economy by drawing on the research activities of the project participants, the most relevant European players in this field.

This research capacity has allowed research to focus on the underlying micro-economic processes and resulting macro-economic impacts both conceptually and in the European context.

Description of the work

EUSECON's strategy focuses on utilizing an overarching theoretical framework to relate human-induced security threats, such as terrorism or organised crime, to other forms of insecurity such as natural disasters, industrial accidents, and conflict.

It will employ the following methods:

» Acknowledging Historical Context: The work strategy will revisit occurrences of insecurity in their historical contexts, going beyond identifying the conceptual and practical similarities and differences between forms of insecurity;

» Analyzing Perceptions of Insecurity: Efforts will be focused on understanding the responses of stakeholders of various levels, on differentiating between inter- and intranational conflict, and on understanding the historical notions of insecurity among the different member states of the EU;

» Filling Knowledge Gaps: A research strategy will be implemented that strives to fill data gaps and overcome the current methodological problems in order to account for the economic repercussions of security and insecurity.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
German Institute for Economic Research	Germany
Institute for Peace Research and Security Policy at the University of Hamburg	Germany
Economics Institute of the Academy of Sciences of the Czech Republic	Czech Republic
Charles University Prague	Czech Republic
University of Patras	Greece
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom
Ingeniería de Sistemas para la Defensa de España, S.A.	Spain
Basque University	Spain
RAND Europe	United Kingdom
Hebrew University Jerusalem	Israel
University of Thessaly	Greece
University of Linz	Austria
International Peace Research Institute, Oslo	Norway
Institute of Social Studies	The Netherlands
Athens University of Economics and Business - Research Center (AUEB-RC)	Greece

SECONOMICS / Socio-Economics meets Security

© Ulrich Mueller - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285223
Total Cost
€4,723,323.44
EU Contribution
€3,451,096.14
Starting Date
01/02/2012
End Date
31/01/2015

Coordinator

UNIVERSITÀ DEGLI STUDI DI TRENTO
Department of Information Engineering
and Computer Science
Via Sommarive 14
38123 Povo, Trento, Italy
Contact
Fabio Massacci
Tel: +39 0461 282086
Mobile: +39 329 2105004
Fax: +39 0461 283987
E-mail:
Fabio.Massacci@unitn.it
Website: www.seconomics.eu

Project objectives

Policy makers are often in the unenviable position of having to make regulatory and investment decisions on security based on incomplete information about the risk structure, and unknown or unknowable preferences of their stakeholders. The presence of Knightian uncertainty (i.e., uncertainty of uncertainty and uncertainty of the outcomes in security problems) renders many conventional "rules of thumb", or "broad policy generalizations", unworkable.

SECONOMICS was a collaborative project on the socio-economics of security, with a specific focus on the interplay between information security and physical security, driven by three key cases studies in critical infrastructure protection: in international air transportation, in local transportation and in energy distribution. These sectors are all critical to the economic and social lives of EU member states. The scientific approach integrated expertise into social, economic, system and risk modelling and provided a basis for initial developments of decision-support methodologies and tools for policy makers.

Description of the work

The SECONOMICS project was primarily structured around three case studies that were designed to address the core themes of the call and can be applied to the majority of the missions that are outlined within the CORDIS Cooperation Security Theme. They covered:

» *WP1:* Airports and airport security;

» *WP2:* Critical Power Infrastructure;

» *WP3:* Regional and Urban Transport.

The initial task was to identify the concrete issues in security missions for these case studies. Once the menu of security missions has been characterized, R&D work-packages (WP4, WP5, WP6), then began to characterize the threats and distillate socio-economic methodologies based on rigorous and well-developed methodologies from the social sciences, risk and operations research, and economics and systems models.

» *WP4* identified the qualitative societal impact scenarios, from the future or emergent threat. Quantification of the social cost was made by contingent valuation;

» *WP5*'s role was in the identification of the outcome space and associated risk measures. In addition WP5 analysed the threat environment and potential security measures and their effectiveness;

» *WP6* developed economic and systems models of the policy interactions with the architecture of the physical and ICT system under threat and developed an optimal set of policy tools and control instruments designed to optimally deal with the future or emergent threat, subject to social cost constraints;

» *WP7* consolidated the results of the three case studies to cross-mission relevance results and assisted in consolidating the validation assessment between WP4, WP5 and WP6. Loosely speaking it was "hand-booking" the results of the concrete case studies;

» *WP8* provided the necessary computer-aided support to manage real data, by providing tools that map the research models either to collected or to simulated data (for instance backing out the policy parameters from structural models of economic risk and risk preferences);

- A specific WP (*WP9*) was devoted to the issue of dissemination and exploitation.

Results

SECONOMICS achieved a methodological revolution in security policy modeling by integrating sociological, economic, and security science into usable and actionable models for policy-makers responsible for civil protection and critical infrastructure protection. An important aspect of the project has been a continuous validation loop with key stakeholders (e.g., National Grid security team, the UK/US Energy Transmission Operator, the Council of Airport Directors etc.). This has allowed the project to distill an evidence-based policy toolkit to assist decision-makers who seek to identify optimal policy options for emerging security problems.

One example was the treatment of risk-based vs. rule-based security policies: the choice of the optimal policy for regulating the security of energy transmission operators was discussed at the UK Cabinet Office, and was further presented at an EU presidency meeting for DG-HOME and a DG-ECHO by an ENTSOE representative. A part of the project methodologies was also embedded into an amendment to the Common Vulnerability Scoring System, the worldwide standard for software vulnerability assessment.

PARTNERS	COUNTRY
UNIVERSITA' DEGLI STUDI DI TRENTO (UNITN)	Italy
DEEP BLUE SRL (DBL)	Italy
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
UNIVERSIDAD REY JUAN CARLOS (URJC)	Spain
THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN (UNIABDN)	United Kingdom
FERROCARRIL METROPOLITA DE BARCELONA SA (TMB)	Spain
ATOS SPAIN SA (ATOS)	Spain
SECURENOK AS (SNOK)	Norway
INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION (ISAS CR)	Czech Republic
NATIONAL GRID ELECTRICITY TRANSMISSION PLC (NGRID)	United Kingdom
ANADOLU UNIVERSITY (AU)	Turkey

VALUESEC / Mastering the Value Function of Security Measures

RESEARCH
COMPLETED

Information

Grant Agreement N°
261742
Total Cost
€4,473,885
EU Contribution
€3,443,210.10
Starting Date
01/02/2011
End Date
31/01/2014

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute
for Factory Operation
and Automation IFF
Sandtorstrasse 22
39106 Magdeburg
Germany
Contact
Christian Blobner
Tel: +49 391 4090 371
Fax: +49 391 4090 93 901
E-mail: Christian.blobner@iff.fraunhofer.de
Website: www.valuesec.eu/

Project objectives

The objective of the ValueSec project was to develop a tool-set to support decision makers with overall policy objectives, political and ethical values as well as societal concerns. To achieve this, the consortium developed means to make costs and benefits associated with decisions on security more transparent. The objectives of the project were :

» *Objective 1:* To survey the field of security economics, and the field of applicability of cost-benefit-tools and their links to societal issues relevant to security;

» *Objective 2:* To provide a tool-set for the analysis of cost and benefits of security measures, based on explicit requirements of policy level end-users;

» *Objective 3:* To test and validate the developed tool-set in realistic use cases;

» *Objective 4:* To evaluate the results from different perspectives of decision makers in security, from the policy, economic and societal point of view; and

» *Objective 5:* To determine the research needs and to give recommendations for further R&D.

Description of the work

ValueSec brought together an interdisciplinary team of researchers and end-users to generate a knowledge base of the current state and trends in theory and in practical applications of methods of economics, applied to security decision making. The project's main challenge was to combine economic factors and societal effects of security measures into a "value function" to establish a basis for a cost-benefit approach. In effect, the project brought together quantitative and qualitative information and combined it in a common methodological framework and integrated it into a decision support tool.

The consortium was gathering inputs from public decision makers regarding their requirements for an efficient cost-benefit analysis in a security framework. Additionally, current approaches in cost-benefit analysis and in how far they were applicable to meet the decision maker's requirements were surveyed and mapped onto available methodologies. This was a major research effort for the subsequent integration into a software-based decision support tool.

ValueSec ensured the applicability of the developed approach and the subsequent software tool through validation in realistic use cases. These use cases were built around typical scenarios for decisions in a security context. These use cases were developed in close cooperation with end-users and external stakeholders to guarantee maximum relevance. End-user input was provided by the Valencia Local Police, which which also provided an application scenario for a use case validation. Valencia provided ample opportunities to validate the developed approach and the subsequent support tool, e.g. in a use case comprising strategic planning elements for the Formula One Grand Prix organized in the city.

Results

The ValueSec project developed a decision support methodology and accompanying software prototype tool for policy level stakeholders in the field of security. The main characteristic of the methodology and tool is to provide an expanded cost-benefit analysis taking into account three separate pillars of analysis, namely a Risk Reduction Assessment, a (strictly monetary) Cost Benefit Assessment, and a Qualitative Criteria Assessment.

With the development of the methodology and tool, the ValueSec consortium aimed to support policy decision makers in the field of security to make better informed decisions. The developed ValueSec methodology and the subsequent software implementation in the so-called ValueSec toolset, increased the transparency of potential costs and benefits of security measures. Based on the individual and consolidated results of ValueSec's analysis pillars, decision makers will have a better opportunity to make decisions based on their individual preferences. In this respect, it should be noted that ValueSec does not provide for a "total-optimiser" solution, which provides decision makers with the "optimal solution" or "best decision". Instead, the ValueSec tool will provide a better fundamental reason to base a decision on.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IFF)	Germany
VTT Technical Research Centre of Finland (VTT)	Finland
Centre for European Security Strategies (CESS)	Germany
International Peace Research Institute (PRIO)	Norway
University of Stavanger (UIS)	Norway
ATOS Origin S.A. (Atos)	Spain
Institute of Innovative Technologies (EMAG)	Poland
White Cyber Knight (WCK)	Israel
Policía Local de Valencia (VPD)	Spain

ARCHIMEDES / Support to security end users

© Cristian Baitg - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285061
Total Cost
€1,539,056
EU Contribution
€1,353,848
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Avenue de Tervuren 270
B-1150 Brussels, Belgium
Contact
Moureen Schobert
Tel: +32 2 775 82 97
Mobile: +32 483 227 941
Fax: +32 2 775 81 12
E-mail: moureen.schobert@eos-eu.com
Website: www.eos-eu.com

Project objectives

ARCHIMEDES' mission was to increase the R&T uptake in Europe by focusing on end-users & operators' needs and involvement in the innovation cycle. To do that it aimed at promoting a sustainable public – private dialogue between the demand and the supply side, and at making European research activities more end-user friendly, for a better identification of capability gaps and operational needs. ARCHIMEDES facilitated end-users & operators' participation in security Research & Innovation programmes and made recommendations on how the innovation process from basic research through to development, standardization, certification and validation and finally deployment could be improved.

Description of the work

ARCHIMEDES carried out research on Innovation Management tools, procedures and best practices (e.g. on Pre-Commercial Procurement, regulations, standardisation, etc.), end-users & operators' early R&T demand and common operational needs. In addition to testing, validation and certification issues in the security domain, it also looked into possible improvements of the legal and operational environment.

The results consisted of recommendations that were explored, refined and validated with end-users & operators during several sector-specific roundtables. These roundtables were held in different EU countries and gathered existing networks of end-users and operators to support a dialogue and exchange information.

These networks were then organised and linked through a "Virtual Forum for Security End-Users & Operators." This forum continuously informed and encouraged the debate among end-users on R&T activities, funding, new EU regulations and other developments that might impact their ability to innovate.

ARCHIMEDES had the unique opportunity to maximise its impact on the planning of European and national security research activities by leveraging its Partners' established links with policy-makers. ARCHIMEDES guaranteed the follow-up of the project results by making them available to the broadest network of European, local and national stakeholders.

Results

The EU-funded ARCHIMEDES project is a proposed solution to redefine security innovation in Europe through 10 round-table discussions held in different European countries. It supports the validation of research results and exploitation by bringing demand and supply closer together.

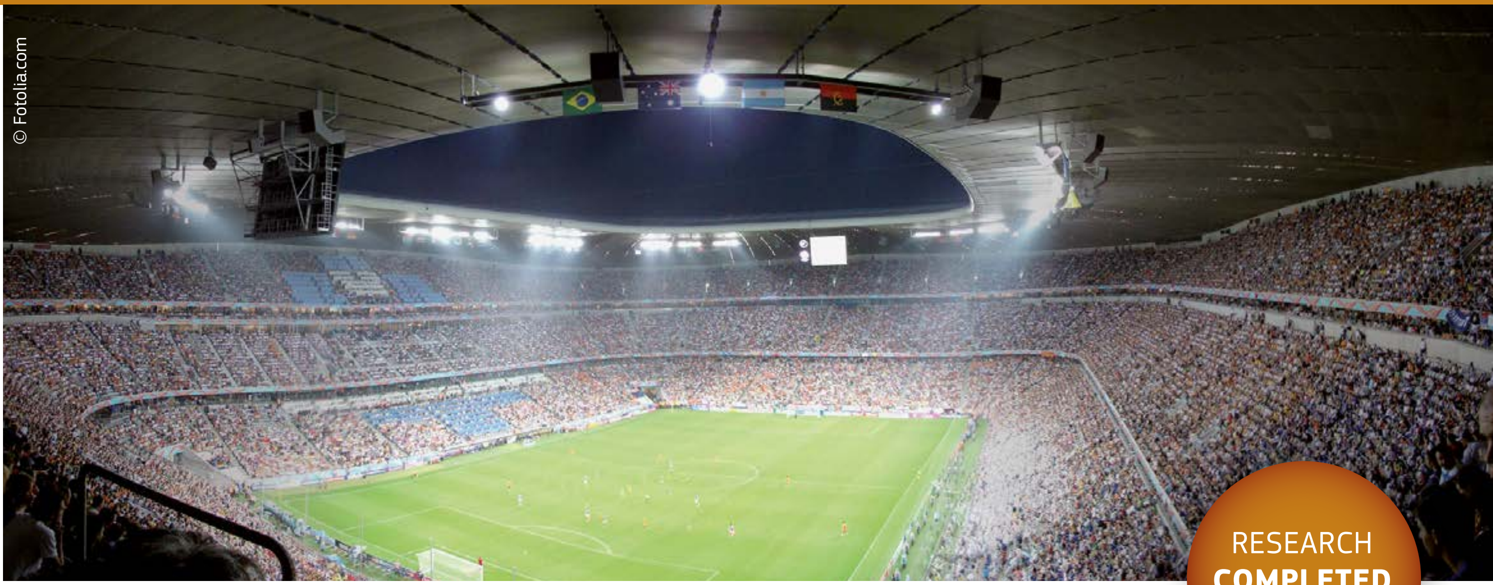
To provide end users with tools, procedures and best practices for maximising R&I outcomes, project partners developed an innovation management methodology to foster a common innovation management culture among end users and operators.

The project delivered a series of recommendations on innovative management practices, end user and operator needs for R&I participation and funding schemes, specific operational needs in 10 key security market areas, and on building strong public-private dialogue. They specifically target security end users and operators, the EC's Security Research Programme, and European and national policymakers. In addition, a manual was produced to familiarise end users and operators with European research procedures and funding schemes, and participation and application processes.

Finally, a European network of national organisations for security was proposed in order to establish permanent dialogue and sustainable cooperation between organisations within the EU tasked with coordinating national security demand and supply.

PARTNERS	COUNTRY
European Organisation for Security (EOS)	Belgium
Ministerio Del Interior (MIR-ES)	Spain
Ingeniera De Sistemas Para La Defensa De España SA-ISDEFE (ISDEFE)	Spain
Universite catholique De Louvain (UCL)	Belgium
Haut Comite Francais Defense Civile (HCFDC)	France
German European Security Association EV (GESA)	Germany
Przemyslowly Instytut Automatyki I Pomiarow (PIAP)	Poland
@ Mediaservice.Net SRL (MEDIASERVICE)	Italy

EU-SEC II / Coordinating National Research Programmes and Policies on Security at Major Events in Europe



© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218076
Total Cost
€2,829,013.06
EU Contribution
€2,527,000
Starting Date
01/07/2008
End Date
31/10/2011

Coordinator

UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE
Security Governance
and Counter-Terrorism
Laboratory
10127- Turin
Italy
Contact
Alberto Pietro Contaretti
Tel: +39 011 6537 111
Fax: +39 011 6313 368
E-mail: contaretti@unicri.it
Website: www.eu-secii.org

Project objectives

EU SEC II was a coordination action organized by the United Nations Inter-regional Crime and Justice Research Institute (UNICRI), Europol and 22 European countries to develop the research cooperation begun by the first EU-SEC project (concluded in 2008).

EU-SEC II aimed to establish a comprehensive EU-wide network of national authorities in the field of Major Event security as well as common security planning standards to foster future European coordination in this area.

Its ultimate goal was the creation of the "European House of Major Events Security" (known as "the House") – a coordination tool to provide technical assistance to Major Event security planners on the basis of commonly elaborated planning methodologies. In this way, the House will contribute to the realization of the objectives of the EU Internal Security Strategy and the Stockholm Programme: the achievement of a common European policing approach.

Results

A key component of the project was the desire to avoid duplication of efforts and to incorporate the lessons learned and best practices already established into the House. A series of meeting allowed partners to elaborate common research priorities and policies endorsed by the whole research consortium.

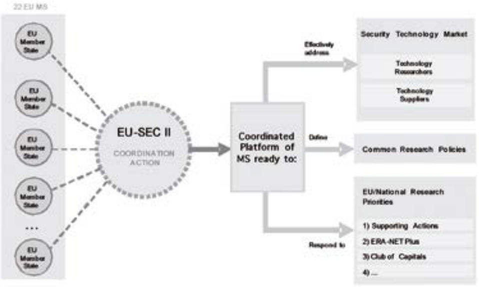
One of EU-SEC II's objectives was to investigate which services the House could offer, focusing in particular on public-private partnerships (PPPs), common research standards and media management. The final output was a pilot research strategic roadmap to direct future research priorities.

To validate these ideas, EU-SEC II tested the services to be offered by the House in relation to seven Major Events. These were: the 2009 Champions League Final held in Rome, Italy; the Climate Change Conference 2009 held in Copenhagen, Denmark; the Pope's 2010 visit to Cyprus; the 2011 Champions League Final held in Madrid, Spain; the EU Presidencies of Hungary in 2011 and Cyprus in 2012; and, the 2011 G20 meeting held in France.

Finally, a manual was produced to guide ownership and operation of the House. The Manual lays the foundations for the further development of international coordination services aimed at improving and strengthening European level cooperation in Major Event security research and planning. It includes a detailed description of the Coordination Tools and Methodologies (CTMs) to be made available to European security planners via the House.

These efforts produced the following benefits:

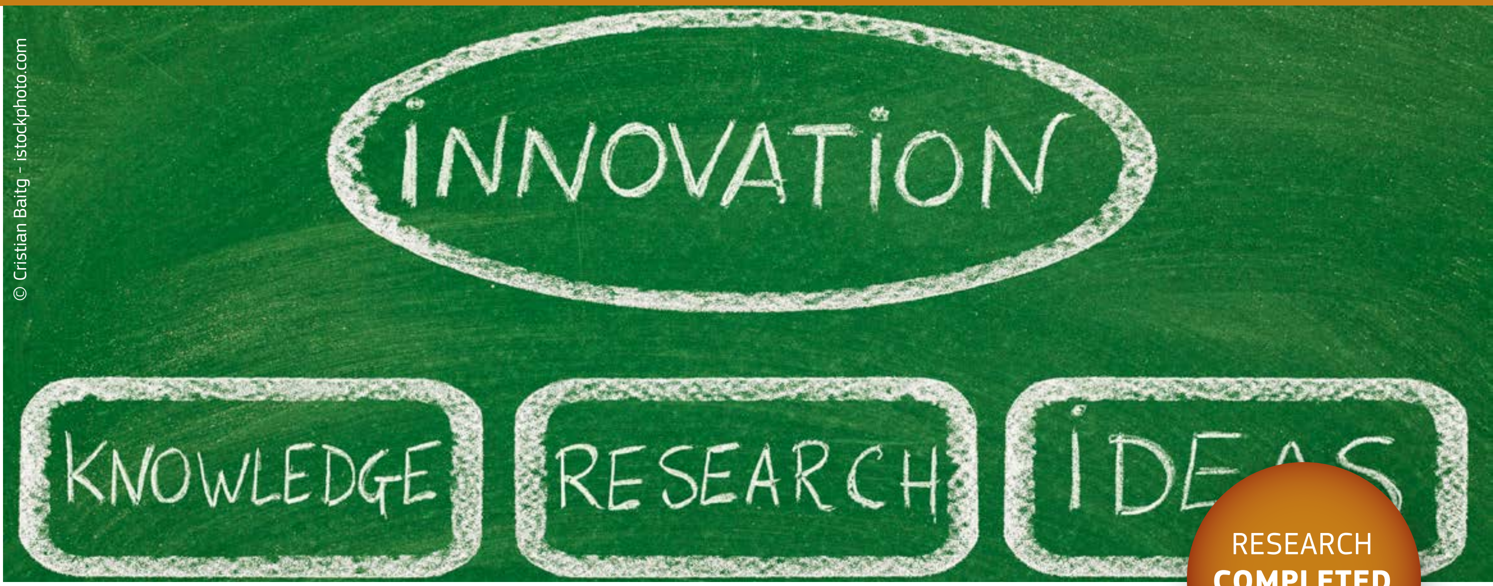
- » stronger cooperation and coordination among the relevant security stakeholders, including the private sector, to develop integrated and comprehensive operational security plans;
- » implementation of specific training curricula to disseminate common policing methods and a culture of increased attention to the development of relationships with the general public and the media.



© EU-SEC II

PARTNERS	COUNTRY
United Nations Interregional Crime and Justice Research Institute	Italy
Europol	The Netherlands
Bundesministerum für Inneres / Ministry of the Interior	Austria
German Police University	Germany
Cuerpo Nacional de Policía	Spain
Ministry of the Interior / Police Department	Finland
Direction Générale de la Police Nationale	France
Metropolitan Police Service	United Kingdom
An Garda Siochana	Ireland
Ministero degli Interni	Italy
Ministry of Justice	The Netherlands
Ministry of the Interior / Higher Institute on Police Sciences and Internal Security	Portugal
Centre for Security Studies	Greece
Police Academy of Latvia	Latvia
Ministry of Interior and Administration Reform General Inspectorate of the Romanian Police	Romania
Ministry of Interior of the Slovak Republic	Slovakia
Academy of the Ministry of the Interior	Bulgaria
Policijska uprava Maribor	Slovenia
Personal Protection and Law Enforcement Police	Estonia
Cyprus Police	Cyprus
Hungarian National Police Headquarters	Hungary
Malta Police Force	Malta
Swedish National Police Board	Sweden
National Police Department / National Police College	Denmark
Ministry of the Interior of the Republic of Latvia (State Police)	Latvia

INNOSEC / Innovation management models for security organisations



© Cristian Baitg - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285663
Total Cost
€1,651,765
EU Contribution
€1,289,778
Starting Date
01/02/2012
End Date
31/01/2014

Coordinator

FUNDACIÓN TECNALIA RESEARCH & INNOVATION
Innovation and Society Division
Parque Tecnológico de Bizkaia. Edificio 204
E-48170, Zamudio (Bizkaia), Spain

Contact
Amaia Sopelana
Tel: +34 946 400 450
Mobile: +34 667 17 89 33
E-mail: amaia.sopelana@tecnalia.com
Website: www.innosec-project.eu

Project objectives

The aim of the Project was to develop a novel innovation model for the security sector based on networked relationships between the actors and its associate organisational framework that allowed end-users to develop the ability to handle and utilise currently available and forthcoming innovations. It fostered the balance between innovation strategies, creating dynamic capabilities, and including absorptive capacity, allowing adequate structural and cultural organisational conditions that permited them to handle real environmental threats. This balance between a flexible model for implementing innovation management and the respect for current practices in general management and operation was called the InnoSec paradigm.

Description of the work

In order to achieve the objectives of the project the consortium:

» Analysed the end-user organisations' environment and innovation management processes. By analysing the operating environment and identifying end-users' current practices of innovation management, lessons were drawn for the development of an innovation model;

» Analysed models of innovation and innovation management processes in non-security sectors. A development of a typology of these innovation models and practices was conducted, in respect of their suitability for different types of embedding organisational environments;

» Developed a modular innovation model for security organisations (Innosec Model). This model aimed at helping these organisations to design and implement innovation management processes and practices;

» Tested the Innosec model. The modular innovation model previously developed was customised and tested in end-user organisations;

» Developed an Implementation Roadmap that guided public and private security providers as well as their regulatory bodies and other stakeholders towards a successful implementation of the novel model.

Results

InnoSec's results were:

- A complete modular innovation management model that includes both organisational aspects such as innovation strategy and the cultural and human resources environment, and the practical aspects of selecting, designing, and implementing specific innovations in, technology innovations. The model is provided as a theoretical framework where each element or module is broken down into innovation practices in a way that it is possible for any organisation to partially or completely apply it since the modules are loosely coupled.

- An implementation roadmap composed of diagnosis and decision making tools. These have proven to be key in the actual implementation of InnoSec since they enable the organisation to collect knowledge about innovation practices currently in place and assess the gap between them and the objectives that the management considers adequate in their plans. Supported by an on-line tool and with or without the help of external consultants, each organisation is then able to select the modules that contribute to bridge apparent gaps or reach excellence in the areas already deemed strong.

- An exploitation plan for the expansion of InnoSec to the security organisations in Europe. The plan suggests a development of awareness raising and commercial activity depending on the type of security organisations, both public and private, taking into account size or spread, but also the modality of collaboration, including external consultants or mixed teams.

- A report of potential new topics for the research programme drawn from the issues encountered both during the research and during the implementation tests in the end-users associated to the project. The topics are classified according to these research areas: data handling, technology watch, societal impacts, funding, innovation measurement and evaluation, legal issues, and training. A more specific list of research arising from questions not completely responded to during the project is offered separately in a future research map which addresses more academic themes such as innovation niches, risk aversion, role of procurement or social expectations.

- Dissemination of InnoSec continues via its website beyond the commitment of the contract with the EC (end of January 2015). Moreover, InnoSec is being presented at conferences and workshops such as the International Police Course.

PARTNERS	COUNTRY
Fundación Tecnalia Research & Innovation (TECNALIA)	Spain
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Ministerio de Defensa de España (MDE)	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Austrian Institute of Technology GmbH (AIT)	Austria
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
The University of Manchester (UNIMAN)	United Kingdom
Österreichisches Rotes Kreuz – Austrian Red Cross (ÖRK ARC)	Austria
Prosegur Compañía de Seguridad SA (PROSEGUR)	Spain

INSEC / Increase Innovation and Research within Security Organisations

© mtrommer - fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285287
Total Cost
€1,576,867.60
EU Contribution
€1,126,862
Starting Date
01/04/2012
End Date
31/07/2014

Coordinator

ALMA CONSULTING GROUP SAS
Innovation Department
55, Rue René Cassin
CP 418
69338 Lyon France
Contact
Michel MOULINET
Tel: +33 (0)4 72 35 89 04
Mobile:
+33 (0)6 22 92 98 12
Fax: +33 (0)4 72 35 80 31
E-mail:
mmoulinet@almacg.com
Website:
www.insec-project.eu

Project objectives

The INSec project was striving to improve the Innovation and Research processes within the security organisations, so that they can integrate new technologies, enabling them to evaluate novel approaches and services dedicated to the safety of citizens.

The project focused on two main areas:

- The development of a new internal innovation management model. This allowed the security organisations to better manage both the financial impacts and the added value of innovating projects;
- The development of an external innovation platform in order to promote the networking between European security SMEs and public/private security organisations. This increased the visibility of SMEs among security organisations and henced diversify the range of services and technologies for them.

Two major European-scale events were organised to share good practices in the field of innovation management, and dissemination was done though e-learning training modules developed within the project.

Description of the work

With a consortium of consulting companies and security end-users (public and private security organisations), the INSec project focused on the existing needs and practices of four types of organisations:

- Rescue Services;
- Police and National Security Office;
- Academies of Security Sciences;
- National Security Infrastructures (port, border control).

As described below, eleven main tasks grouped by the following type of activities were implemented:

Activity 1 - Analysis and Studies

- Analyse the main aspects of Innovation Management in the security-related operators (end-users), both public and private;
- Assess the Level of Innovation inside the organisation;
- Foster new business models for Security;
- Promote the security and privacy requirements at the early stages of systems development ("Security and Privacy by design");
- Analyse and evaluate the impact of new technologies and review their legal implications.

Activity 2 - Innovation Ideas and Technology boost

- Create a new innovation model based on the needs of security organisations identified during the creativity sessions;
- Build an open platform which integrated effective tools for technology watch, forecasting and roadmapping for the security sector. The aim was to provide an integrated framework for technology screening activity at European level in order to identify weak spots and early demand in R&D;
- Find services related to the platform tools which encouraged an appropriate use of technology or the implementation of innovative ideas for responding to new threats, in the medium to long-term.

Activity 3 - Best practices and networking

- Create networking activities and exchanges of best practices between security end-users in Europe;
- Establish for the four types of management systems a European best practices list.

Activity 4 - Training

- Define training needs and create an ‘innovation’ vocational training system framework for end-users available for the entire European Security Organisation.

Results

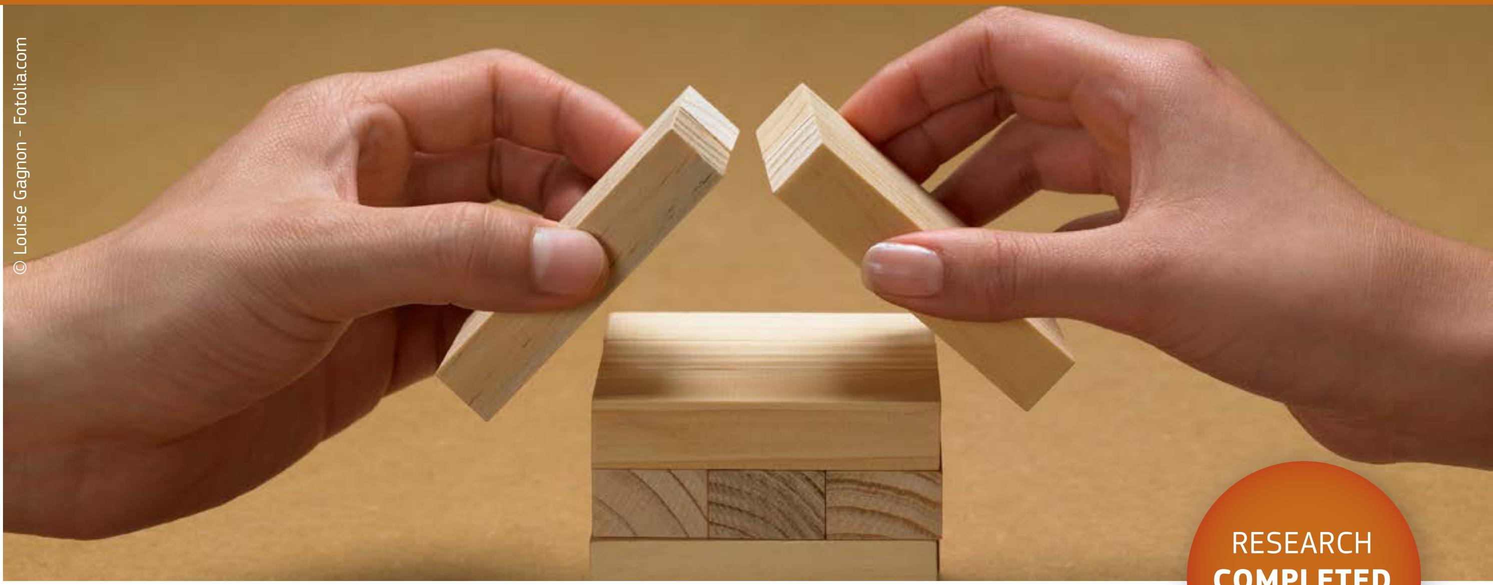
INSEC’s goal was to contribute to the increase of innovation and research within security organisations in security-related operators (end-users). The consortium established a framework that will contribute to better performance of the end-user organisations, focusing on their RDI management system as a fundamental method to create knowledge and transform it into economic and social wealth.

The project captured the internal know-how for generating innovation by using the stage-gate innovation model and by bringing external knowledge through technology watch and open innovation practices in order to create external innovative solutions. The work was focused on two main areas: the development of a new internal innovation management model and the development of an external innovation platform. This platform was the main technical achievement of the project (http://platform.insec-project.eu).

The platform based on innovation management model created by the consortium is easy to use and gives possibilities to recognise gaps in innovation management system and get advice on action plan for future activities.

PARTNERS	COUNTRY
ALMA CONSULTING GROUP SAS (Alma)	France
EFPC (UK) LTD (EFPC)	United Kingdom
FM MANAGEMENT CONSULTANCY SRL (FMMC)	Romania
PROXIMA CENTAURI SAS (KAOS)	France
ADVISIO OU (ADVISIO)	Estonia
GLOBAZ SA (GLOBAZ)	Portugal
EVERIS SPAIN SLU (EVR)	Spain
INOGATE- CONSULTORIA EM INOVACAO EMPRESARIAL SA (INOGATE)	Portugal
SISEKAITSEAKADEEMIA (EASS)	Estonia
ACADEMIA DE POLITIE ALEXANDRU IOAN CUZA (AICPA)	Romania
GRAD SKOPJE (CoS)	Former Yugoslav Republic of Macedonia
AUTORIDAD PORTUARIA DE GIJON (PAG)	Spain
HUNGARIAN MINISTRY OF INTERIOR (ORFKV)	Hungary
OU BALTIC INNOVATION AGENCY B.I.A. (BIA)	Estonia
ROMANIAN MINISTRY OF ADMINISTRATION AND INTERIOR (MAI)	Romania

THE HOUSE / Enhancing European Coordination for National Research Programmes in the Area of Security at Major Events



© Louise Gagnon - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285099
Total Cost
€2,203,411.50
EU Contribution
€2,203,411.50
Starting Date
01/03/2012
End Date
31/05/2014

Coordinator

UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI)
Security and Governance
Viale Maestri del Lavoro 10
10127 – Turin - Italy
Contact
Leif Villadsen
Tel: +39 0116537115
Fax: +39 0116313368
E-mail: villadsen@unicri.it
Website: www.unicri.it

Project objectives

Promote a major-events security integrated approach in the European Union (EU) and design the right technological infrastructure to support it.

Description of the work

The seven common standards developed by The HOUSE project were linked to eight real major events for which a security plan was drafted and/or took place in the consortium member states' territory during the two years of the project implementation.

The common standards were the following:

1. The Security Planning Model (also used as Evaluation Standard);
2. Best Practices in Public-Private Partnership;
3. Media Management Guidelines for Major Events;
4. Ethical and Operational Standards for Security Products;
5. Specialist Technical Equipment Pool (STEP) database;
6. European Major Events Register (EMER) database; 7. Training Curricula

The eight major events were selected during the project's implementation following the indications of consortium partners. The coordinator and representatives of the seven hosting member states within the consortium helped link the project to the selected events.

Further, the hosting member state facilitated the consortium's access to the planning/evaluation process of the major event, whilst UNICRI (in addition to its coordinator role and its capacity as WP leader) oversaw use of the coordination tool with the activities of the project's task leaders. UNICRI was supported by an ad hoc team composed of consortium members, with technical support from its advisory board.

Results

The seven common standards for major events security planning tested and adopted by participating partners.

It has contributed to the implementation of the Stockholm Programme

PARTNERS	COUNTRY
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Italy
Bundesministerium für Inneres-Ministry of the Interior (BM.I)	Austria
Academy of the Ministry of the Interior (Academy of MoI)	Bulgaria
Cyprus Police	Cyprus
The Danish National Police (POSD)	Denmark
Ministry of the Interior (MoI)	Estonia
Ministry of the Interior Police Department (SM PO)	Finland
Direction Générale de la Police Nationale (D.G.P.N.)	France
Deutsche Hochschule der Polizei (DHPol)	Germany
Center for Security Studies (KEMEA)	Greece
Orszagos Rendor Fokapitanysag (ORFK)	Hungary
An Garda Siochana (AGS)	Ireland
Ministero dell'Interno (MinInterno)	Italy
State Police of the Ministry of Interior of the Republic of Latvia (State Police)	Latvia
Police department under the Ministry of the Interior of the Republic of Lithuania (PD)	Lithuania
Malta Police Force (MinMALTA)	Malta
Ministry of Security and Justice (MinJus)	The Netherlands
Wyzsza Szkola Policji W Szczytnie (WSPol)	Poland
Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI-MAI)	Portugal
Ministry of Administration and Interior-Inspectorate General of Romanian Police (MoAI)	Romania
Ministry of Interior of the Slovak Republic (MINV)	Slovakia
Policijska uprava Maribor (PU Maribor)	Slovenia
Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía (CNP)	Spain
Swedish National Police Board (Polisen)	Sweden
Metropolitan Police Service (MetPo)	United Kingdom

CIPRNet / Critical Infrastructure Preparedness and Resilience Research Network

© CIPRNet

Information

Grant Agreement N°
312450
Total Cost
€7,663,168.20
EU Contribution
€6,569,842.50
Starting Date
01/03/2013
Duration
48 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER)
Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS
Adaptive Reflective Teams Department (ART)
Schloss Birlinghoven
53757 – Sankt Augustin
Germany
Contact
Erich Rome
Tel: +49 2241 14 2683
Fax: +49 2241 14 4 2683
E-mail: erich.rome@iais.fraunhofer.de
Website: www.ciprnet.eu

Project objectives

CIPRNet has four general scientific and technological objectives:

» To strengthen and structure the European Critical Infrastructure Protection (CIP) research area by establishing a network of shared CIP knowledge and expertise that offers and transfers knowledge to isolated CIP and adjacent research areas.

» To provide support from CIP research communities to emergency managers, governmental agencies and policy-makers, enhancing their all-hazard preparedness for, response to, and recovery of disrupted, failed or destroyed Critical Infrastructures (CI) and their cascading effects.

» To enhance the resilience of CI by improving the knowledge and understanding, preparation and mitigation of CI disruptions and their consequences.

» To lay the foundation for a long-lasting virtual centre of competence and expertise in CIP, the "European Infrastructures Simulation & Analysis Centre" (EISAC).

CIPRNet will reach these objectives by:

» Implementing new capabilities for supporting more effective responses to disasters that affect or originate from CI,

» Building the required capacities for creating these new capabilities, and

» Founding a long-lasting virtual centre of competence and expertise in CIP (VCCC).

Description of the work

CIPRNet's joint R&D activities towards implementing new capabilities include:

» Creating added-value, decision-support capabilities with consequence analysis for national and multi-nation emergency management and CI owners based upon integrating technologies available at CIPRNet partners,
» Supporting the secure design of Next Generation Infrastructures (such as Smart Grids),
» Creating a 'what if' modelling, simulation and analysis capability for emergency managers for exploring different courses of action in crises.

CIPRNet has a dedicated agenda for further extending and integrating existing technology such as interoperability middleware and creating new simulator federations for the new capabilities.

The second cluster of joint activities addresses capacity building, for reaching the specific goal of creating a critical mass of expert knowledge and expertise in CIP. This includes

» Cooperation and coordination with other CIP related networks
» Staff exchange and training
» Collaboration and exchange with and training of end users and other stakeholders
» Dedicated dissemination, training and teaching activities

CIPRNet will conduct training exercises, bringing together tools and expertise to develop realistic, complex scenarios. To increase their impact and visibility, CIPRNet will demonstrate the new capabilities in a real crisis management exercise. For this, CIPRNet will investigate a real or realistic emergency scenario; produce consequence analysis of CI failures and cascading effects; perform a vulnerability analysis and hazard analysis within that scenario; and derive courses of actions with their consequences for decision-makers.

The distributed VCCC will allow the integration and coordination of research activities, the dissemination of results, and offer services to the CIP community and end-users. An electronic platform will support the VCCC, deploying new community services via Internet This will include enquiries to experts, an online glossary on CIP, CIP bibliographies and project lists, and more.

Expected results

Expected tangible results of CIPRNet include:

- A new Decision Support System capability with consequence analysis for single or multi-nation emergency management (for training and hot phase support)
- A new 'what if …' modelling, simulation and analysis capability for emergency managers (for training) and short term predictions (for hot phase support)
- More and better trained researchers and experts as a result of the various dissemination and training activities of CIPRNet
- The VCCC, providing support from the CIP research communities to stakeholders. Its services will be accessible through the CIPRNet web site
- An association fostering the evolution of the VCCC to EISAC for sustaining support beyond the duration of CIPRNet

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V. (Fraunhofer)	Germany
Agenzia Nazionale per le Nuove Tecnologie, L'Energia e lo Sviluppo Economico Sostenibile (ENEA)	Italy
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)	The Netherlands
Union Internationale des Chemins de fer (UIC)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
The European Union represented by the European Commission represented by the Joint Research Centre (JRC)	European Union
Stichting Deltares (Deltares)	The Netherlands
University of Cyprus (UCY)	Cyprus
Uniwersytet Technologiczno-Przyrodniczy im. Jana i Jędrzeja Śniadeckich w Bydgoszczy (UTP)	Poland
Università Campus Bio-Medico di Roma (UCBM)	Italy
The University of British Columbia (UBC)	Canada
ACRIS GmbH (ACRIS)	Switzerland

EUROFORGEN-NOE / European forensic genetics network of excellence

© Euroforgen

Information

Grant Agreement N°
285487
Total Cost
€8,192,996.63
EU Contribution
€6,613,680
Starting Date
01/01/2012
Duration
60 months

Coordinator

UNIVERSITÄTSKLINIKUM KÖLN
Institute of Legal Medicine
Melatengürtel 60/62
50823 Köln (Cologne),
Germany
Contact
Peter M. Schneider
Tel: +49 221 478 88345
Fax: +49 221 478 88370
E-mail: peter.schneider@uk-koeln.de
Website: www.euroforgen.eu

Project objectives

This initiative aims to achieve **long lasting cooperation leading to the emergence of a virtual research centre in forensic genetics embedded in the security domain.** For the implementation, a series of specific actions is needed such as:

» To establish a directory of forensic genetics research institutions across Europe;

» To identify the processes involved in handling and analyzing forensic genetic evidence from crime scene to courtroom;

» To facilitate the exchange of information between research institutions, stakeholders and end users;

» To integrate research needs and capacities into a sustainable virtual network.

EUROFORGEN-NoE – will serve to connect the efforts named above and to lay the foundations of a European virtual centre of research in forensic genetics aimed at introducing an international, self-sustained body fully supported by national activities.

Description of the work

EUROFORGEN-NoE comprises 12 partners from 8 countries, among them some of the leading groups in European forensic genetic research. The network initiative proposes an integration of existing cooperation, as well as establishing new ones, in this security field by integrating all the relevant parties and stakeholders.

Stimulating cooperation between research centres and industry is key to continued success. Thus, the main thrust of activities is aimed towards exchange of information, dissemination of knowledge, and networking. EUROFORGEN-NoE will carry out a series of actions in this regard. One of these actions is the execution of **three short exemplar projects**, where leading European research groups are collaborating as an example for other groups. These exemplar projects will prepare the ground for the publication of a **competitive call for additional projects** to be funded and subsequently integrated into the second phase of the project period.

Furthermore, forensic genetic research has to be **embedded into an ethical and societal framework** required for a positive acceptance of this relatively new technology by the public. An adequate response to public concerns regarding a potentially too intrusive use of new forensic DNA applications is seminal for a wider application of these methods in the near future. Only then can the consequences and future perspectives be addressed adequately. The essential development and **publication of an ethical guideline on forensic genetics** will be a major element of this process.

Finally, **educational structures will be established** both at the local as well as at the European level ensuring that scientists applying the forensic genetic technology in the context of security and the justice system are in line with the most recent scientific developments.

An **advisory board** with highly recognized experts from the fields of ethical, legal, and forensic sciences ensures that the challenges defined in the network programme will be met.

Expected results

EUROFORGEN-NoE will have **a long-lasting societal effect** by building an efficient research network – a **European Virtual Centre for Research in Forensic Genetic**: It enables the **most important stakeholders** to meet, to exchange and to disseminate information, to develop **new directions in research**, and to integrate its output into **outstanding new training concepts**. It will identify public perception of genetic forensic technologies and its potential for ethical conflicts - resulting in the development of **ethical guidelines**.

PARTNERS	COUNTRY
Universitätsklinikum Köln (UHC)	Germany
Universidade de Santiago de Compostela (USC)	Spain
Nasjonalt Folkehelseinstitutt (NIPH)	Norway
Queen Mary and Westfield College, University of London (QMUL)	United Kingdom
Københavns Universitet (UCPH)	Denmark
Netherlands Forensic Institute (NFI)	The Netherlands
Medizinische Universitaet Innsbruck (IMU)	Austria
Universitetet for Miljø og Biovitenskap (UMB)	Norway
Uniwersytet Jagiellonski (JU)	Poland
University of Northumbria at Newcastle (UNN)	United Kingdom
Epiontis GmbH (EPTS)	Germany
GABO:mi Gesellschaft fuer Ablauforganisation:milliarium mbH & Co. KG (GABO:mi)	Germany

PLANTFOODSEC / Plant and food biosecurity

© Monika Wisniewska - Fotolia.com

Information

Grant Agreement N°
261752
Total Cost
€5,609,529.69
EU Contribution
€4,624,499
Starting Date
01/02/2011
Duration
60 months

Coordinator

UNIVERSITA DEGLI STUDI DI TORINO
Centro di Competenza per l'innovazione in campo agro-ambientale (AGROINNOVA)
Via Leonardo da Vinci, 44
10095, Grugliasco (Torino)
Italy
Contact
Maria Lodovica Gullino
Tel: +39 011 670 8539
Fax: +39 011 6709307
E-mail: marialodovica.gullino@unito.it
Website: www.plantfoodsec.eu

Project objectives

PLANTFOODSEC is a Network of Excellence aiming to enhance preparedness for preventing, responding and recovering from the possible use of plant pathogens as biological weapons against crops, and the microbiological contamination of feed and food in the European agrifood system.

PLANTFOODSEC pursues the following specific objectives:

» obtaining scientific knowledge on plant disease epidemiology;

» enhancing the prevention, recognition, response and recovery from foodborne illness due to the contamination of fresh produce;

» improving planning of effective and efficient national and regional responses to agro-terrorism acts;

» improving disease surveillance and detection systems by facilitating international laboratory cooperation and by developing diagnostic tools;

» preventing the establishment and spread of deliberately-introduced pathogens;

» building a strong culture of awareness and compliance with plant and food biosecurity for those with responsibilities in all sectors of agriculture and food production;

» improving awareness among stakeholders and the general public on biosecurity issues;

» overcoming the fragmentation of partners' research.

Description of the work

This project will focus on biological threats having the capacity to affect and damage agriculture, infect plants and ultimately affect food and feed at any stage in the food supply chain. These threats are multifaceted, interrelated, complex and increasingly transnational in their impact.

Recent trends in biosecurity recommend a shift from a largely national approach towards greater international cooperation.

The Network of Excellence will renew and reinforce already established partnerships and enlarge them by including new countries, institutions and topics to establish a virtual Centre of Competence. It will be able to deal with issues of crop and food biosecurity and become a Centre of reference at the European level.

The project strategy is based on the bio-preparedness approach to prevent, respond and recover from a biological incident or deliberate criminal activity threatening European agrifood systems, thus including:

» actions to identify and update the biology, epidemiology and impacts of high priority pathogens also through the optimization of detection and diagnostic tools;

» actions to develop effective responder strategies by defining specific protocols on emergent pest and disease management;

» actions to enhance knowledge of target groups and to inform relevant stakeholders taking into account the balance between confidentiality and public access;

» actions to overcome the fragmentation of partners' research and to facilitate and coordinate responder networks.

Expected results

A more risk-based approach will move biosecurity from a reactive towards a proactive position which focuses more on prevention and better anticipates emergences of entirely new threats.

By following this strategy, PLANTFOODSEC will increase the quality and impact of plant and food biosecurity training and research in Europe thus providing timely scientific inputs to respond to biosecurity threats posed to the European agriculture, farming and agrifood industry.

PARTNERS	COUNTRY
Università degli Studi di Torino (UNITO-AGROINNOVA)	Italy
National Institute of Agricultural Botany	United Kingdom
The Secretary of State for Environment, Food and Rural Affairs	United Kingdom
Rheinische Friedrich-Wilhelms-Universitaet Bonn	Germany
Institut National de la Recherche Agronomique	France
Regional Environmental Center for Central and Eastern Europe	Hungary
Imperial College of Science, Technology and Medicine	United Kingdom
Middle East Technical University	Turkey
SPIN-TO Srl	Italy
United Nations Interregional Crime and Justice Research Institute	Italy
The Agricultural Research Organisation of Israel – The Volcani Centre	Israel
Oklahoma State University	The United States
Kansas State University	The United States

SEREN / Security Research NCP network – Phase 1

© Andres Rodriguez - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217937
Total Cost
€743,597.40
EU Contribution
€557,692.04
Starting Date
01/02/2008
End Date
31/07/2009

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
European Affairs Directorate
91191 Gif-sur-Yvette
France
Contact
Frédéric Laurent
Tel: +33 1 64 50 25 22
Fax: +33 1 64 50 11 57
E-mail: pcn_securite@cea.fr
Website: www.seren-project.eu/

Project objectives

Security Research presents several specificities as compared to other Cooperation's FP7 thematic priorities. Indeed, it is a new theme within FP7 and therefore the Security Research community has only a limited experience gained during the 3 years of the Preparatory Action for Security Research.

Moreover, projects need to be mission-oriented and as such must involve end-users who are not familiar with FP.

Also, the Security products' market is complex, large, and relatively new. Finally, by its very nature, the Security research theme has introduced sensitivity issues into the 7th Framework Programme.

As a consequence, perhaps more than in the other specific programmes and themes, there is a strong necessity to inform and support the European Security Research community in its participation to FP7. One way to facilitate this is through a stronger National Contact Points (NCPs) network.

SEREN will thus aim at strengthening the Security research NCP network by raising the knowledge level of its members, initiate coordination and, as a matter of fact, the ability of its members to deliver a high level of service to the community.

Description of the work

The aim of the SEREN-phase 1 coordination action is to link the different Security Research NCPs, to identify fields of improvement for the structuring of the network, to initiate coordination and to start promoting joint activities. In order to reach those objectives, SEREN will tackle four main issues:

Identification of the network needs and initiation of coordination among its members.

This will be mainly obtained through surveys in order to gain a better understanding of the needs of the Security Research community and of the requirements that NCPs must fulfil in order to deliver a high level of service. Also, coordination will be initiated in order to raise the level of knowledge of NCPs. This will be obtained by making common guides and setting up a website where all the deliverables will be made available.

Increase NCP knowledge and awareness of the European Security landscape.

In order to deliver advices in their respective country, NCPs must have a minimum understanding of the European security landscape. Therefore, a mapping of the Security research programmes launched in Member States will be made. In addition, a mapping of competencies will be initiated. This latter task will aim at the identification of support structures such as government agencies, professional associations, end-users associations, SMEs associations, clusters involved in Security Research across Europe.

Coordination to ease transnational cooperation and training.

The EU community potentially interested in Security Research faces a high level of fragmentation. Therefore, participants are confronted with difficulties finding other potential partners with whom they might collaborate. Hence, it is extremely important that the NCPs network delivers a high level service for the partner searches.

SEREN will initiate coordination in this field by agreeing on standardised partner search templates. In addition one training session focussed on the evaluation will be organised.

This shall enable an increase of the average advice quality delivered by the network and further optimize its services to the Security Research community.

Security research policies

SEREN will produce synthesis papers on key policies issues related to Security research in order to raise awareness on the contextual framework surrounding ESRP.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Tarptautiniu mokslo ir technologiju pletros programu agentura	Lithuania
Achimedes Foundation	Estonia
Foundation For Research & Technology – Hellas	Greece
National Office for Research and Technology	Hungary
Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk	Poland
Matimop, Israel Industry Center For Research & Development	Israel
Agenzia per la Promozione della Ricerca Europea	Italy
Romanian Space Agency	Romania
Norges forskningsråd	Norway
The Scientific and Technological Research Council of Turkey	Turkey
Service d'information scientifique et technique / SPP Politique scientifique – Dienst voor Wetenschappelijke en Technische Informatie/POD Wetenschapsbeleid	Belgium
Österreichische Forschungsförderungsgesellschaft mbH	Austria
Agência de Inovação, Inovação Empresarial e Transferência de Tecnologia, S.A	Portugal
Centro para el Desarrollo Tecnologico Industrial	Spain
SenterNovem	The Netherlands
Technologické centrum	Czech Republic
Research Promotion Foundation	Cyprus
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Euresearch	Switzerland
Council for Scientific and Industrial Research	South Africa
Riga Technical University	Latvia
Centre for National Security and Defense Research	Bulgaria
Malta Council for Science and Technology	Malta
Home Office	United Kingdom
Luxinnovation GIE	Luxembourg
Danish Agency for Science Technology and Innovation -Ministry of Science, Technology and Innovation	Denmark
Agentura na podporu vyskumu a vyvoja	Slovakia

SEREN2 / SEcurity REsearch Ncp network – phase 2

© kabliczech - Fotolia.com

Information

Grant Agreement N°
261814
Total Cost
€1,801,696.23
EU Contribution
€1,499,546.21
Starting Date
01/04/2011
Duration
24 months

Coordinator

ROMANIAN SPACE AGENCY
Headquarters
21-25 Mendeleev Street
010362 – Bucharest
Romania
Contact
Anca Liana RACHERU
Tel: +40 (0) 21 3168722
Fax: +40 (0) 21 3128804
E-mail: Anca.racheru@rosa.ro
Website: www.rosa.ro

Project objectives

The main objective of this project is to continue promoting and enhancing trans-national cooperation among Security National Contact Points (NCP) (at the level of both people and institutions appointed in this respect), by reaching a balanced distribution of proficient services to be delivered by Security NCPs to their clients while assisting them to write high quality proposals to be submitted in the future calls.

Description of the work

WP1 – Capacity Building aims at *improving the Security NCPs' capabilities and reinforcing the network to become more efficient and effective. Technical trainings on general and specific issues, twinning schemes and staff exchange* are focused on sharing experiences, expertise and good practices, by promoting intensive trans-national cooperation.

WP 2 – Joint Brokerage Events aims at *improving the quality of the cooperation between security research stakeholders* (researchers, large companies, SMEs, end-users) by *providing the necessary support* to ease the process of finding appropriate partners for *building successful consortia*. Trans-national events shall be organised to the benefit of cross-border audiences.

WP 3 – Mapping of security research competencies focus on the identification of Security Research Competencies in Europe, to *increase the visibility of security related research in Europe and to optimize the networking* between research facilities, universities, public authorities, end users and suppliers of security solutions and operators of critical infrastructures.

WP 4 – Partner Search is dedicated to *promote transnational cooperation by facilitating the access of potential participants to future Security calls.*

WP 5 - Monitoring of Security research area aims at *providing both NCPs and stakeholders with an improved flow of security research area information*. An *in-depth mapping of security research systems and programmes* is foreseen.

WP 6 – Communication and dissemination has as the objective to oversee and organize all aspects which are related to communication and dissemination of the project results and activities. A scientific approach of communication and dissemination will be applied for this project by stimulating and strengthening the relationship between persons and problems. Making project achievements and activities widely accessible and easily exploitable by project customers will be a challenge for this WP.

Expected results

Results from SEREN2 will help decision making related to:

- Underpinning the realization of NCP value chains in the security topic for simplifying access to FP7 calls, for lowering the entry barriers for newcomers and raising the average quality of submitted proposals;
- Improve and increase the effectiveness of third country organizations' participation alongside European organizations;
- Strengthen the competitiveness of the European R&D in the Security theme.

PARTNERS	COUNTRY
Romanian Space Agency (ROSA)	Romania
Foundation for Research & Technology – HELLAS (FORTH)	Greece
Agenzia per la Promozione della Ricerca Europea (APRE)	Italy
Österreichische ForschungsförderungsgesellschaftmbH (FFG)	Austria
Euresearch Head Office Berne (EURESEARCH)	Switzerland
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Mokslo Inovaciju Ir Technologiju Agenturaa (MITA)	Lithuania
SIHTASUTUS ARCHIMEDES (Archimedes)	Estonia
Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk (IPPT PAN)	Poland
MATIMOP - Israel Industry Center for Research & Development (MATIMOP-ISERD)	Israel
Norges forskningsråd – Research Council of Norway (RCN)	Norway
The Scientific and Technological Research Council of Turkey (Tubitak)	Turkey
Dienst voor Wetenschappenlijke en Technische Informatie / Service d'Information scientifique et technique (STIS)	Belgium
Centro para el Desarrollo Tecnologico Industrial (CDTI)	Spain
Technologické centrum Akademie ved Ceske republiky (The Technology Centre of the Academy of Science - TC AS CR)	Czech Republic
Research Promotion Foundation (RPF)	Cyprus
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Council for Scientific and Industrial Research (CSIR)	South Africa
Riga Technical University (RTU)	Latvia
Centre for National Security and Defense Research (CNSDR)	Bulgaria
Malta Council for Science and Technology (MCST)	Malta
Zilinska Univerzita v Ziline (UNIZA)	Slovakia
Finnish Funding Agency for Technology and Innovation (TEKES)	Finland
Hrvatski institut za tehnologiju/ Croatian Institute of Technology / Odjel za međunarodnu suradnju/ International Cooperation Unit (HIT)	Croatia
Fundacao para a Ciencia e Tecnologia (FCT)	Portugal
National Institute of Aerospace Technology of Spain (INTA)	Spain

SOURCE / Virtual centre of excellence for research support and coordination on societal security

© Kim Erlandsen, NRK P3

Information

Grant Agreement N°
313288
Total Cost
€5,576,210.00
EU Contribution
€4,997,588.00
Starting Date
01/01/2014
Duration
60 months

Coordinator

INSTITUTT FOR FREDSFORSKINING STIFELESE (PRIO)
Dimensions of Security
Hausmanns gate 7
0186 – Oslo – Norway
Contact
J. Peter Burgess
Tel: +47 22547738
Mobile: +47 90923949
E-mail: jpeterburgess@prio.org
Website: www.prio.org

Project objectives

The aim of the SOURCE project is to create a robust and sustainable virtual centre of excellence which explores and advances the societal issues of security research and development.

Description of the work

SOURCE is built upon five types of activities: networking activities, research, information gathering, education and training and, finally, knowledge-sharing. Together these address the ambitions and the expected impact of the EU's Work Programme specific to the Security call.

Via an integrated information-gathering hub, education programmes across security sectors, and a comprehensive programme of networking activities, SOURCE's virtual centre will gather experts and actors from all levels of the security chain (researchers, industry actors, policy-makers, civil society, end-users and the public at large). All will be linked by a common effort of documenting, analysing and understanding the links between security and society where the former is played out.

Expected results

The project will relay on an array of networking activities, meetings, scientific and popular publications, film, press and social media, a scholarly journal and the formation of an international association for the study and improvement of societal security. SOURCE's Network of Excellence will raise awareness among policy makers and end-users, increase the security industry's competitiveness by better responding to the social "layers of insecurity" across society and, as a consequence, contribute to the improved well-being and security of European citizens.

PARTNERS	COUNTRY
Institutt for fredsforskining stifelese (PRIO)	Norway
Totalforsvarets Forskningsinstitut (FOI)	Sweden
Centre for Irish and European Security Limited (CIES)	Ireland
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung e.v (Fraunhofer)	Germany
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)	The Netherlands
Centre for European Policy Studies (CEPS)	Belgium
Vrije Universiteit Brussel (VUB)	Belgium
IRKS-Research GesmbH	Austria
King's College London (KCL)	United Kingdom
European Organisation for Security (EOS)	Belgium
Fundacion Tecnalia Research & Innovation (TECNALIA)	Spain
Fondation Nationale des Sciences Politiques (Sciences Po)	France

VIDEOSENSE / Virtual Centre of Excellence for Ethically-guided and Privacy-respecting Video Analytics in Security

© iofoto - Pavel Losevsky - Hunta - NZ-Photos - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261743
Total Cost
€6,412,895
EU Contribution
€5,282,366
Starting Date
01/05/2011
End Date
30/04/2015

Coordinator

THE UNIVERSITY OF READING
Intelligent Media Systems and Services Research Laboratory, School of Systems Engineering
Whiteknights Campus
PO Box 217
RG66AH Reading
United Kingdom
Contact
Prof. Atta Badii
Tel: +44 (0) 118 378 7842
Fax: +44 (0) 118 975 1994
E-mail:
atta.badii@readiing.ac.uk
Website:
www.imss.reading.ac.uk

Project objectives

The objectives of VideoSense were to investigate Video Analytics RTDI and Ethical issues and update the stakeholders including both citizens and implementers on the latest actionable insights regarding the optimisation of acceptable and effective Video Analytics adoption including how best to:

- Implement Ethical and Privacy Safeguards;
- Minimise False Alerts;
- Minimise Network (data) traffic bandwidth demand arising from VA deployment;
- Minimise the required human attention bandwidth in using VA surveillance;
- Ensure easy, cost-effective, efficient and effective deployment of VA systems;
- Establish a sustainable business case and revenue model for VA technology uptake;
- Minimise the storage requirements for VA deployment;
- Integrate with identification technologies;
- Trust interoperability between VA systems;
- Conduct benchmarking and comparative evaluation of alternative products.

VideoSense, through its joint programme of research studies sought to examine: a) the recent achievements, b) the breakthroughs that are needed to achieve the expected results, c) the disciplines that are relevant and need to be applied to problems, and d) the best approach for establishing and managing a benchmarking and evaluation framework.

Description of the work

VideoSense integrated leading European research groups to create a long-term open integration of critical mass in the twin areas of Ethically-Guided, and, Privacy Preserving Video Analytics where the advent of new data intelligence technologies against the background of dynamic societal and citizen goals, norms, expectations, safety and security needs and thus surveillance requirements have all contributed to a complex interplay of influences which deserved in-depth study and solution seeking in order for European society, citizens and industry to strike the optimal balance in resolution of the various challenges in this arena. Accordingly VideoSense provided for: i) Fostering increased sustainable relationships between existing national research groups; ii) Momentum building by integrating existing researchers and resources to push forward new paradigms and the knowledge basis for the resolution of ethically guided, sensible, selective, useful, cost–effective solutions to society's surveillance needs; iii) Establishing a Virtual Centre of Excellence and expandable framework, based on Pan-European integration of complementary expertise and optimisation of shared, flexible, modular and interconnected resources including knowhow, laboratories and people to support collaborative research and agenda setting; iv) Two external Boards of Industrial and Scientific Advisors to keep the targeted research focused and responsive to the needs of European citizens, society and industry; v) Establishing a standard framework for Ethical Compliance Audit Management based on a suitably evolved Compliance Audit Maturity Model (CAMM) and associated Training and Certification services as both a service to organisations and revenue streams to ensure longer-term sustainability of the Video-Analytics Centre of Excellence.

Results

Respect for civil liberties and privacy were the guiding principles as reflected in the results of the VideoSense Demonstrator as showcased at the IEEE DSP in Jakarta on the 16th of September, 2014. The results filled socio-ethical and technical gaps in video-analytics and provided clear added-value to privacy by design for security surveillance via the following:

- A VideoSense Centre of Excellence (VCE, see www.videosense.eu) for the integration of existing researchers to support socially responsible privacy preserving analytics solutions for security needs
- A standard framework for Ethical Compliance Audit Management and associated Training and Certification as a service and a VCE revenue stream
- A framework to support various standardisation stakeholders, e.g. JPEG and MPEG communities
- The organisation of more than 20 research exchanges at senior research leader, post-doctorate, and internships levels
- Summer and winter school training for socio-ethical privacy preserving systems development and Dual-Use/Malevolent-Use risk analysis
- A number of Privacy Filtering Grand Challenges and related databases under the MediaEval 2012-2015
- Joint research activities as "mini projects" that led to a significant number of Video-Analytics and Evaluation innovations as reported in project deliverables.

PARTNERS	COUNTRY
THE UNIVERSITY OF READING (UoR)	United Kingdom
QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)	United Kingdom
EURECOM (EURECOM)	France
THALES SECURITY SOLUTIONS & SERVICES SAS (THALES)	France
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SAÇISDEFE (ISDEFE)	Spain
TECHNISCHE UNIVERSITAET BERLIN (TUB)	Germany
ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE (EPFL)	Switzerland
INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)	Belgium

VOX-Pol / Virtual Centre of Excellence for Research in Violent Online Political Extremism

Information

Grant Agreement N°
312827
Total Cost
€5,554,326.28
EU Contribution
€5,129,681.00
Starting Date
01/01/2014
Duration
60 months

Coordinator

DUBLIN CITY UNIVERSITY (DCU)
School of Law
& Government
Glasnevin
Dublin 9, Ireland
Contact
Maura Conway
Tel: +353 (0)1 700 6472
Mobile:
+353 (0)87 295 1284
Fax: +353 (0)1 700 7374
E-mail:
info@voxpol.eu
maura.conway@dcu.ie
Website: www.voxpol.eu

Project objectives

» Promote long-term relationships between established national research groups and new researchers/research groups;

» Provide training via conferences, summer schools, and workshops to researchers, PhD students, early career researchers and those who monitor or respond to VOPE about the tools, methods and substantive issues of violent online political extremism;

» Raise awareness about the interplay of e-research ethics, privacy, surveillance, freedom of speech, and responses to violent online political extremism;

» Outreach to diverse publics via mass media, public lectures and other public events, free-to-access publications, etc., which describe our research and its purposes;

» Influence European and international research agendas in key aspects of violent online political extremism.

Description of the work

» Integration and networking of research activities within EU and globally of those working on violent online extremism and its effects, including the online strategies of: violent jihadists, the extreme right, violent nationalist-separatist and ethnic separatist movements;

» Creation of a sustainable critical mass of innovative activity among today's fragmented group of researchers and research topics through joint research, networking events, and teaching and learning activities;

» Create an archive of politically extreme Internet-based content as the basis for joint research activity; develop new analytical tools and methodologies, teaching and training, and dissemination activities;

» Harness software tools used in other domains to collect and analyse violent online political extremist content;

» Forge long-term relationships between established national research groups, new researchers, security practitioners, the Internet industry, civil society and policymakers to develop a multi-disciplinary Virtual Centre of Excellence for Research in Violent Online Political Extremism;

» Ensure that EU and Member State strategies targeting violent online political extremism are based on concrete evidence, experience, and knowledge.

Expected results

- Critical mass of research excellence in the relevant research areas within the EU together with VOX-Pol's international partners;
- Synergy on approaches, methodologies, and technologies currently being developed independently by disciplinarily and/or geographically distinct research communities;
- Better informed policy agendas on national, European, and international levels in key aspects of responses to violent online political extremism.

PARTNERS	COUNTRY
Dublin City University (DCU)	Ireland
University of Oxford (UOXF)	United Kingdom
Indraprastha Institute of Technology Delhi (IIITD)	India
King's College London (KCL)	United Kingdom
Universiteit van Amsterdam (UVA)	The Netherlands
Nederlandse Organisatie voor Toegepast Natuurwetenschappel (TNO)	The Netherlands
Institut fur Friedensforschung und Sicherheitspolitik anDer Universitat Hamburg (IFSH) at the University of Hamburg	Germany
Central European University (CEU)	Hungary
University College London (UCL)	United Kingdom

3D-Forensics / Mobile high-resolution 3D-Scanner and 3D data analysis for forensic evidence

© IOF

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312307
Total Cost
€1,770,435
EU Contribution
€1,420,262
Starting Date
01/05/2013
End Date
31/08/2015

Coordinator

Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V. (FhG)
Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF
Albert-Einstein-Straße 7
07745 Jena,
Germany
Contact
Peter Kühmstedt
Tel: +49 (0)3641 807 230
Fax: +49 (0)3641 807 602
E-mail: peter.kuehmstedt@iof.fraunhofer.de
Website: www.3D-Forensics.eu

Project objectives

1) Development of a mobile high-resolution 3D scanning system for forensic evidence recovery at crime scenes.

2) Development of 3D data analysis and processing software tools to provide results which may be used in the investigation and prosecution of crime.

3) Test and evaluation of the 3D scanning system with processing and analysis software by members of the forensic community.

4) To supplement the expertise of an SME-based consortium with further end-user and applied research knowledge for efficient and effective development of a new product.

Description of the work

In the first phase of the project the technical requirements placed on the design of the 3D scanning and analysing system were confirmed and further detailed. This was achieved by considering the present use of traces in the investigation and prosecution of crime and the potential offered by the application of the 3D scanning technology. An important result was confirmation of the types of traces the scanning system should focus on, most probably footwear and vehicle tyre impressions.

In the second phase of the project the complete system was designed, consisting of two parts. Firstly, a mobile handheld 3D-sensor system based on high-resolution fringe projection, including embedded FPGA-based electronics for fast data processing, designed for direct use at crime scenes. Secondly, a set of software tools designed for collection of 3D-data, the easy extraction of 3D-features out of scanned traces and their forensic analysis. The design needed to ensure that the data provided by the system was of a type and quality that police could use it for investigations and, where necessary, be admissible as evidence in court.

The third phase of the project was development and integration of the system's modules as determined by the previous design phase. The development of two prototypes was foreseen. They were tested in the fourth phase of the project, which was focussed on the test and evaluation of the development results.

Dissemination, exploitation and management activities run throughout the course of the project.

The project responded to a topic in the FP7 Security Research work programme that was specifically targeted towards Small and Medium sized Enterprises (SMEs). Five of the seven partners were SMEs. The work in the project was focussed towards providing a solution which was sufficiently attractive to the police community to be commercially exploited by the SMEs.

Results

3D-Forensics has developed a prototype mobile high resolution 3D-scanner, and 3D data analysis software for forensic evidence recording and analyses. These tools can record and analyse footwear and tyre impressions, as well as profiles, left at crime scenes in 3D and colour by using optical scanning technology.

The scanner is designed as a handheld device which can be used outdoors with battery power. The scans provide highly resolved 3D point clouds, and colour images are taken simultaneously with an attachable high resolution camera. The integrated 3D measurement and colour data can be analysed with a set of software tools to investigate the characteristics of footwear and tyre impressions. The software has been designed to allow analysis of the new 3D data in a way in which forensic experts are used to working with traditional techniques. Individual identification characteristics such as holes and tears in footwear impressions can be compared against scans of suspects' shoes or the actual shoes. A workflow and methods approach have been implemented to ensure the integrity and authenticity of the data. The system was successfully tested in relevant environments, i.e. similar to crime scenes. The results are assessed as having reached the Technology Readiness Level (TRL) 6 and a 30-month plan has been developed to take the project results through to the launch of a concrete product (TRL 9) with the support of police forces and a forensic institute.

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V. (FhG)	Germany
Regio Politie Zeland	The Netherlands
DelftTech BV	The Netherlands
Lucas Instruments GmbH	Germany
Enclustra GmbH	Switzerland
Gexcel srl	Italy
Crabbe Consulting Ltd	United Kingdom

GRAFFOLUTION / Awareness and Prevention Solutions against Graffiti Vandalism in Public Areas and Transport

Information

Grant Agreement N°
608152
Total Cost
€1,921,748
EU Contribution
€1,497,040
Starting Date
01/03/2014
Duration
24 months

Coordinator

SYNYO GMBH (SYNYO)
Research & Development Department
Otto-Bauer-Gasse 5/14
1060 – Vienna - Austria
Contact
Bernhard Jäger
Tel: +43 1 9962011 6
Mobile:
+43 699 18 940 006
Fax: +43 1 99 620 11 77
E-mail: bernhard.jaeger@synyo.com
Website:
www.graffolution.eu
www.synyo.com

Project objectives

The key objectives of Graffolution are to:

1. Enforce fundamental research studies on graffiti vandalism in public areas and transport, and identify relevant stakeholders, roles and processes.

2. Analyse initiatives, measures, technical methods and best practices against graffiti vandalism in Europe and survey requirements of all affected stakeholders.

3. Elaborate concepts and solutions against illegal graffiti, and design a web-based awareness and prevention framework for stakeholders and the public.

4. Develop a collaborative knowledge base for local experts and affected stakeholders to improve the exchange of know-how and support decision makers at European level.

5. Provide an open information hub that adopts social media technologies to increase awareness among sprayers and citizens through information and visualisations.

Description of the work

Graffolution seeks to counteract the increase of graffiti vandalism in public areas and transportation networks by focusing on smart awareness and positive prevention solutions for all affected stakeholder groups, including those who have used street art as part of city regeneration and placemaking strategies.

The project will work to deliver an extensive set of "collaborative tools and resources" that would include:

(a) a secure space for duty holders, with case studies and other methods of evidencing successful practice, to empower city administrations, public transport services and law enforcement agencies, to share knowledge and more widely promote best practices.

(b) an interactive "Open Information Hub" targeting local communities, citizens and sprayers to strengthen public awareness and enforce the prevention of illegal spraying activities, using effectual tools and visualisations. Social media features and channels will also be integrated to reach young people, graffiti writers and other connected parties.

Expected results

Graffolution will provide a new and comprehensive approach to discover unused potential for collaboration and knowledge exchange on a pan-European level that involves the public to significantly reduce illegal graffiti on the sustainable basis of a low cost, web-based platform.

Some expected results from Graffolution include:

» Facilitate knowledge exchange between key stakeholders on a pan-European level

» Increase awareness on graffiti vandalism

» Improve security in public areas and transport

» Improve living environments and minimise feelings of insecurity

» Minimise costs on removal and prosecution

PARTNERS	COUNTRY
SYNYO GmbH (SYNYO)	Austria
Universitat de Barcelona (UB)	Spain
The University of Arts London (UAL)	United Kingdom
Sine-Institute gGmbH (SINE)	Germany
Ferrocarrils de la Generalitat de Catalunya (FGC)	Spain
London Borough of Islington (LBI)	United Kingdom
Union Internationale des Chemis de Fer (UIC)	France
Eticas Consulting (EC)	Spain

MISAFE / The Development and Validation of Microbial Soil Community Analyses for Forensics Purposes

RESEARCH **COMPLETED**

Information

Grant Agreement N°
313149
Total Cost
€2,604,269.40
EU Contribution
€1,991,000.00
Starting Date
01/06/2013
End Date
31/05/2015

Coordinator

THE HEBREW UNIVERSITY OF JERUSALEM (HUJI)
Plant Pathology and Microbiology
Faculty of Agriculture, Food and Environment 12
76100, Rehovot, Israel
Contact
Edouard Jurkevitch
Tel: 972-8-9489167
Fax: 972-8-9489062
E-mail: edouard.jurkevitch@mail.huji.ac.il
Website:
https://sites.google.com/site/fp7misafe/

Project objectives

Soil is a complex and heterogeneous material. However, that complexity can make it a useful form of trace evidence in crime investigation. It is easily transferable - attaching, staining and smearing to inanimate objects, as well as to live and dead bodies - it is a potentially valuable asset for use in forensic analysis since its characteristics are affected by its origin, history, environment and management. However, largely due constraints of the current methodology of analysis, soil use as forensics tool is limited.

Soil provides an enormous phylogenetic and functional microbial diversity, with up to one billion cells and many thousands of bacterial species per gram. Soil bacterial communities also are affected by their environment, and have the ability to reflect the history of a given soil, thereby providing a unique and powerful tool for tracing soil origin. Soil evidence is often comparative; as soils differ in microbial content, a comparison of the communities inhabiting soils may reveal if samples from different scenes are derived from the same or from some other, unrelated, location.

Taking advantage of the advent of powerful molecular technologies, and associated big data handling approaches, soil bacterial DNA can be isolated and used to profile the bacterial communities associated with a soil sample. These DNA-based technologies are ripe for forensic analyses and their implementation, discriminating between sites, even between closely related sites.

The objectives of MiSAFE were to develop soil DNA tools for profiling soil bacterial communities in forensic samples, and setting up and implementing protocols and working procedures based on the most powerful DNA technologies. MiSAFE also constructed a framework for a pan-European database of soil microbial communities and soil properties for potentially comparing forensic soil samples. This project was a partnership between two SMEs, two police forces and three academic institutions.

Description of the work

The expertise of each partner was called upon for the development of specific aspects of the project, and for their integration. This included:

» Setting standard parameters of soil DNA extraction and selecting a best performing procedure;

» Developing sampling and storage procedures;

» Evaluating and comparing DNA technologies applied to soil forensics;

» Delimiting spatial and temporal boundaries of soil microbial profiling, and set up a soil profile database;

» Developing and implementing bioinformatics and statistical tools required for soil microbial profiling;

» Evaluating and validating the protocols and the material, providing legal support to the approach.

Results

» MiSAFE aimed at developing and implementing protocols for using bacterial community analysis in a forensics context. MiSAFE developed and validated:Soil DNA extraction procedures

» Identified adequate marker genes for use in soil DNA PCR amplification

» Specified sampling and storage protocols

» Selected DNA analytic technologies compatible with the forensics laboratory

» Developed data handling and analysis protocols and bioinformatics platforms

» Proposed a legal and operational framework.

MiSAFE showed that soil bacterial communities can be used to discriminate between soil samples originating from various soils or different locations within the same soil type. MiSAFE also revealed that soil microbial DNA analysis is robust, providing similar results with different technological approaches. It also showed that soil samples can be conserved over long periods of time and that standard forensics labs can easily apply the approach.

PARTNERS	COUNTRY
The Hebrew University of Jerusalem (HUJI)	Israel
Libragen (LIB)	France
CLC Bio (CLCBio)	Denmark
Ecole Centrale de Lyon (ECL)	France
James Hutton Institute (JHI)	United Kingdom
Ministry of Public Security (MOPS/INT)	Israel
Ministerio del Interior (GC)	Spain

OSMOSIS / Overcoming security market obstacles for SMEs' involvement in the technological supply chain

© Beboy - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242416
Total Cost
€726,706.60
EU Contribution
€580,889
Starting Date
01/04/2010
End Date
31/03/2012

Coordinator

CIAOTECH SRL
Via Palestrina 25
00189 - Rome
Italy
http://www.ciaotech.com
Contact
Mr. Paolo SALVATORE
Tel: +39 06 33268972
Fax: + 39 06 33267022
E-mail:
p.salvatore@ciaotech.com
Website:
www.osmosisecurity.eu

Project objectives

The OSMOSIS project objective is to foster the involvement of SMEs in the security technology supply chain and to facilitate the collaboration between SMEs and the key stakeholders in the European Security domain.

OSMOSIS will create a nurturing environment for the involvement of SMEs in the overall Security Market, through a set of services including:

» Identification of untapped market potentials in the technology security market supply chain;

» Liaison with large organisations to foster the involvement of SMEs in the security technology supply chain, including the involvement in joint R&D activities;

» The creation of a database of qualified SMEs that will create "meta-clusters" where Large Enterprises could identify partners for their engineering and/or R&D projects;

» Full support to SMEs to favour their involvement in the security supply chain;

» Dissemination and networking events to create a collaborative environment among key stakeholders.

Description of the work

The OSMOSIS method is strongly based on the background of the consortium, and on their unique capabilities and expertise as technology transfer organisations providing services to Large Organisations and SMEs in Europe.

The project methodology will be driven by the following three main pillars:

» Actions towards Key Stakeholders operating in the Security Technology supply chain, to stimulate and support such organisations in involving SMEs in engineering projects as well as in research projects, and to gather relevant information about untapped market potentials;

» Actions towards SMEs, to create awareness on technology supply chain opportunities and provide specific services that help SMEs to enter the overall market supply chain;

» Actions aimed at setting up means to facilitate communication and networking among key stakeholders and organizations.

An added value proposition will be carried out for the engagement of large enterprises. The focus will be placed on the added value that OSMOSIS could provide to them:

» the competitiveness improvement of the ecosystem of the large organization,

» the capability of benefit from innovations and technological expertise offered by SMEs, and

» achievement of corporate social responsibility objectives.

In addition, the OSMOSIS website, will be a reference point for key stakeholders looking for pre-qualified organisations with specific competences/skills in the security sector. The website includes services as:

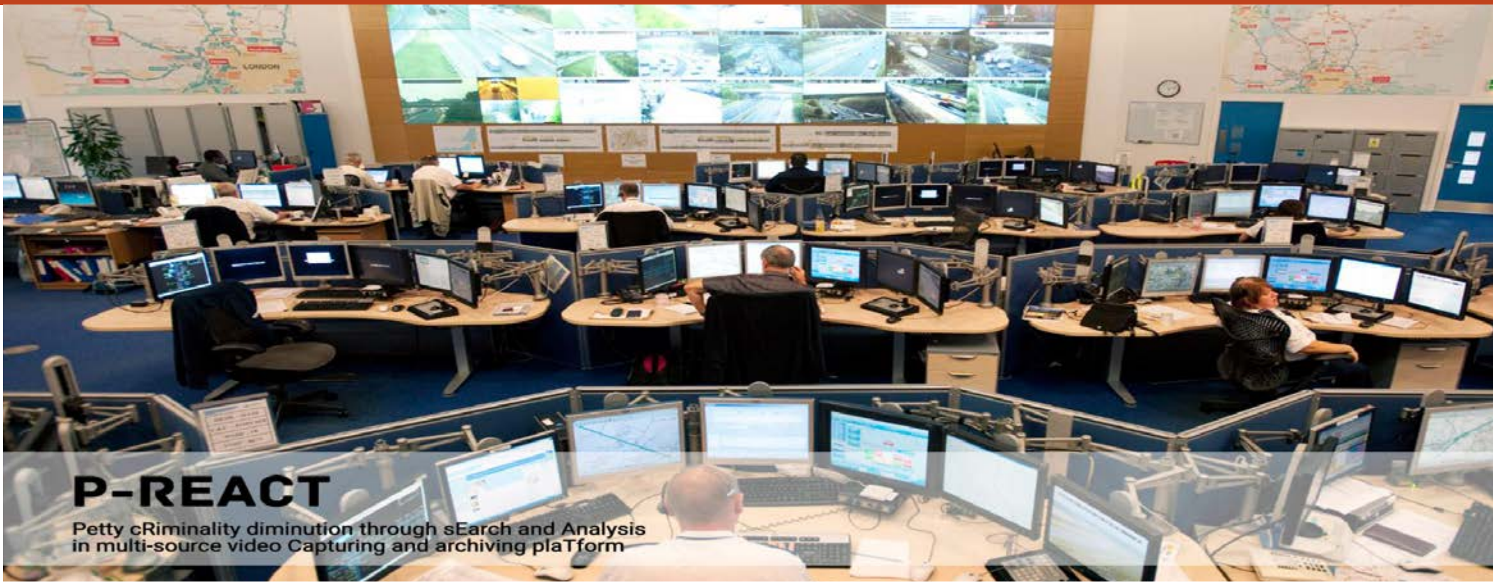
- Access to a database of SMEs, classified following a specific taxonomy and including only relevant SMEs operating in security related engineering and/or research activities;
- A list of security research opportunities that could be exploited by SMEs to collaborate with large organizations;
- Information on security-related grants;
- Interactive communication tools to allow the communication of the identified opportunities and the transfer of specific knowledge to SMEs of the different meta-clusters.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
CiaoTech Srl (CTECH)	Italy
SESM Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l.	Italy
GMVIS Skysoft, S.A.	Portugal
Consorzio Interuniversitario Nazionale per l'Informatica	Italy
Technische Universität München (TUM)	Germany
INNOSTART Nemzeti Uzleti es Innovacios Kozpont Alapítvany	Hungary
Honeywell, spol. s r.o.	Czech Republic
Instituto Nacional de Tecnica Aeroespacial	Spain
Fundación madrimasd para el Conocimiento	Spain
ELSAG Datamat S.p.a.	Italy
PNO Consultants S.A.S.	France

P-REACT / Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform


P-REACT
Petty cRiminality diminution through sEarch and Analysis
in multi-source video Capturing and archiving plaTform

Information

Grant Agreement N°
607881
Total Cost
€1,893,606
EU Contribution
€1,489,396
Starting Date
01/04/2014
Duration
24 months

Coordinator

FUNDACIÓN CENTRO DE TECNOLOGÍAS DE INTERACCIÓN VISUAL Y COMUNICACIONES VICOMTECH (VICOM)
Security Projects
Paseo Mikeletegi 57
20009 – Donostia / San Sebastián – Spain
Contact
Juan Arraiza
Tel: +34 943 30 92 30
Fax: +34 943 30 93 93
E-mail:
security@vicomtech.org
Website:
www.vicomtech.org

Project objectives

P-REACT aims to:

» design and develop a cost-effective solution for petty crime detection, response, investigation and analysis;

» deliver novel video and audio analytics to detect petty crime incidents and develop crime reporting and analysis solutions to strengthen decision-making and responses;

» design and develop a novel, cloud-based Video Content Management System (VCMS) that is capable of being delivered as a service;

» exploit the use of semantic technologies to aid crime analysis and mapping which will help forecast, prevent and detect future petty crimes;

» analyse technical barriers in the standardisation and scalability of the technologies and to ensure that any societal, ethical and legal issues are properly balanced and addressed;

» Organise the demonstration, validation and evaluation of the proposed system according to defined user scenarios.

Description of the work

The P-REACT project will design and develop a low cost surveillance platform that will ensure communication between key users with a focus on increasing the ability of on the ground police and security personnel to respond. The solution will encompass intelligent video and audio sensors to detect petty crime incidents and a cloud-based monitoring, alert detection and storage platform.

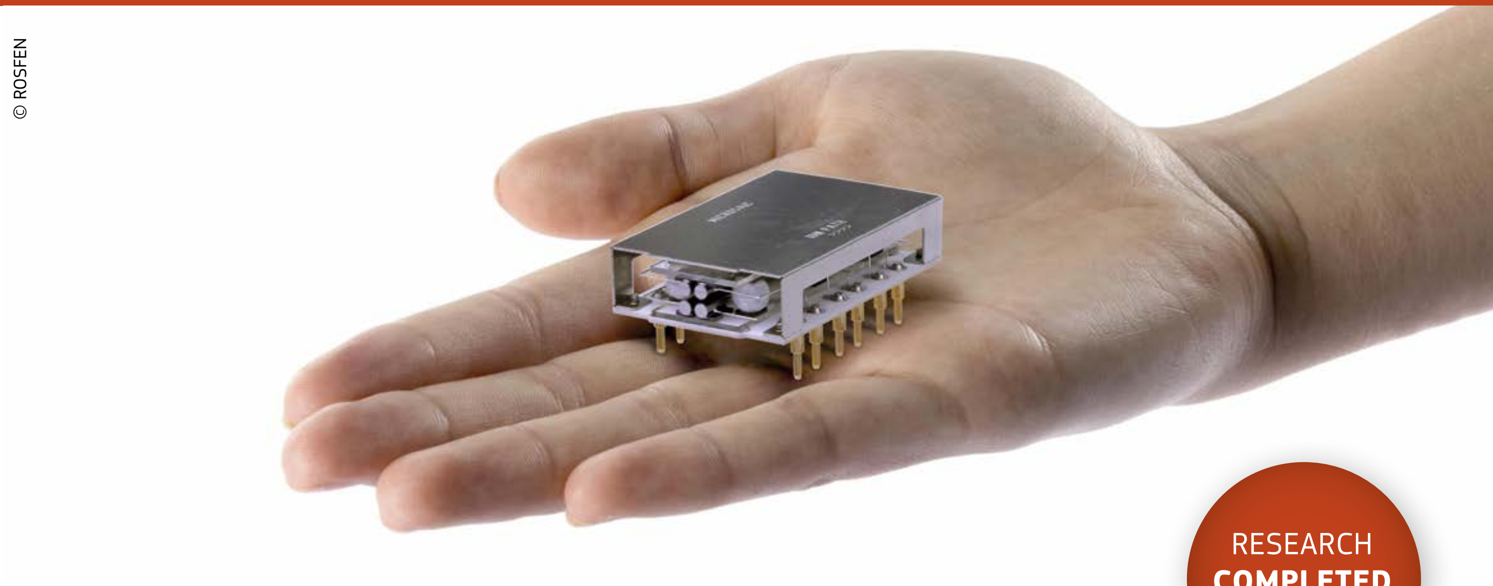
An incident detected by sensors will initiate a work flow including alerting relevant Security Personnel and/ or police with the relevant video and intelligence information, ensuring the appropriate response. The solution will encourage community participation in the reporting of petty crime and as such will be designed to receive information (images, video) captured by mobile smart devices or unconnected surveillance system.

Expected results

1. Intelligent management of multi-sources camera and sensors (IR, depth, etc.) though embedded systems.
2. Light visual and video analytics at the embedded system level.
3. The development of novel cloud service Video Surveillance as a Service (VSaaS) for the video archive integration.
4. The development of a video platform which small business can report incidents and upload relevant video footage from surveillance systems or mobile devices.
5. Assure the privacy and the security of the surveillance data.
6. Security framework ensuring the data privacy, data protection and access level control to the P-REACT system.
7. Present trials in real conditions based on pragmatic scenarios.

PARTNERS	COUNTRY
Fundación centro de tecnologías de interacción visual y comunicaciones Vicomtech (VICOM)	Spain
Kinesense Limited (KS)	Ireland
Aditess Advanced Integrated Technology Solutions & Services (ADI)	Cyprus
Future Intelligence LTD (FINT)	United Kingdom
Center for Research and Technology Hellas (CERTH)	Greece
Center for Security Studies (KEMEA)	Greece
Società Reti e Mobilità SRL (SRM)	Italy

ROSFEN / Rapid On-site Forensic Analysis of Explosives and Narcotics


© ROSFEN

RESEARCH **COMPLETED**

Information

Grant Agreement N°
321829
Total Cost
€1,997,635
EU Contribution
€1,420,262
Starting Date
01/04/2013
End Date
31/07/2015

Coordinator

University College Cork, National University of Ireland, Cork, Tyndall National Institute (Tyndall-UCC)
Tyndall National Institute
Lee Maltings,
Dyke Parade, Cork,
Ireland
Contact
Aidan Quinn
Tel: +353 21 490 4424
E-mail: aidan.quinn@tyndall.ie
Website: www.tyndall.ie

Project objectives

Forensic analysis is an essential resource in the battle against organised crime and terrorist attacks. A key challenge in forensics is the detection of trace explosive residues at a post-blast scene or on the hands or clothes of an alleged suspect. Detection of the high-explosive primer charge (e.g., Pentaerythritol tetranitrate, PETN) is often hampered by higher-concentration residues from the main charge, e.g., ammonium nitrate. Detection of the primer can be essential in order to secure a prosecution, especially if the materials that comprise the main charge are commonly available, e.g., ammonium nitrate is present in fertiliser.

ROSFEN's goal was to deliver an advanced forensic platform for rapid, on-site direct detection and lab-quality analysis of narcotics, explosives and their precursors. The ROSFEN platform was based on a novel chip-based triple quadrupole mass spectrometer with an advanced front-end ion filter and a sample introduction/pre-concentration module. The performance targets were detection limits down to 1 ng/mL for the ion-filtered mass spectrometer with 1 % false alarm rate. The response time target was < 10 seconds for a single scan with < 30 minutes set-up time.

The field-deployable ROSFEN platform was a fraction of the size, power consumption and weight of 'state of the art' lab-based tandem mass spectrometer products, with a target weight of 40 kg; power consumption of 450 W and size of 35 cm (W) × 70 cm (L) × 35 cm (H).

Description of the work

ROSFEN focused on design and development of

» Field-deployable, chip-based tandem mass spectrometer (MS) system with in-line ion filter (FAIMS-AIMS2) for on-site direct analysis of narcotics, explosive compounds and precursor materials.

» Macromolecules and high-surface area templates for molecular recognition-based "trapping" of explosive compounds.

» Modules for sample introduction, vapour collection and multi-pass analyte recycling

» The performance of the system was assessed in a forensic analysis laboratory by forensics experts and also in a secure "real-world" proving ground by crime-scene officers.

Results

The ROSFEN consortium developed an ion-filtered mass spectrometer platform aimed at rapid, on-site forensic analysis of narcotics and explosives. Within the project, the sub-systems developed included a novel ion filter (Environics), a miniaturised triple quadruple mass spectrometer (Microsaic), as well as a sample introduction and heating module for on-site desorption of analyte material from forensic swabs (Environics).

The prototype system was integrated by Environics and assessed in a lab environment by Forensic Science of Northern Ireland. Detection of explosives (including PETN) at 10 ng levels as well as drugs of abuse and chemical warfare agents were achieved.

Additional innovations included development of high-surface area templates (Tundall-UCC) and novel molecular receptors (University of Basel) for specific adsorption (pre-concentration) of PETN. The operation and performance of these molecular traps was also investigated, using atomistic simulations (Tyndall-UCC).

PARTNERS	COUNTRY
University College Cork, National University of Ireland, Cork, Tyndall National Institute (Tyndall-UCC)	Ireland
Microsaic Systems (Microsaic)	United Kingdom
Environics OY (Environics OY)	Finland
Universitaet Basel (UNIBAS)	Switzerland
Department of Justice Northern Ireland, Forensic Science Northern Ireland (FSNI)	United Kingdom
Police Service of Northern Ireland (PSNI)	United Kingdom

SMARTPREVENT / Smart Video-Surveillance System to Detect and Prevent Local Crimes in Urban Areas

Information

Grant Agreement N°
606952
Total Cost
€1,943,448.00
EU Contribution
€1,499,995.50
Starting Date
01/03/2014
Duration
24 months

Coordinator

TREELOGIC TELEMATICA Y LOGICA RACIONAL PARA LA EMPRESA EUROPEA SL (TREELOGIC)
R&D Department
Parque Tecnológico de Asturias, Parcela 30
33428- Llanera- Asturias (Spain)
Contact
SERGIO GARCÍA ÁLVAREZ
Tel: +34 985 966 136
E-mail: sergio.garcia.alvarez@treelogic.com
Website: www.smartprevent.eu

Project objectives

The SmartPrevent project focuses on the detection and prevention of frequent petty crimes that are of high impact to local communities and citizens in urban scenarios, considered to be a low-cost video-surveillance system oriented to end-users.

The objectives of SmartPrevent project are:

- Detection of crime on persons and local businesses in urban areas;
- Crime prevention over persons and local businesses in urban areas;
- Video-surveillance system oriented for end-users.
- Video-surveillance system as an effective and efficient punitive tool that protects people's privacy;
- Temporal and spatial adaptability;
- Low-cost video-surveillance system.

Description of the work

The increase of criminal activity is manifested in an increased frequency of small crimes like graffiti, theft, robbery, and destruction of rubbish bins. This has had a big impact for local governments, citizens and businesses.

Current video-surveillance systems in urban scenarios are very limited and only consist of a presentation of visual information captured by the visual sensors network, not oriented to end-users, limiting their capacity to help and prevent the criminal activity. Furthermore, the visual-surveillance systems usually do not have any automatic process to store the most relevant evidence to be used in the legal punitive process of criminals.

SmartPrevent will address this challenge by:

- Studying the characteristics of frequent criminal activities in real urban scenarios including typical variations and unanticipated criminal situations;
- Developing a low-cost, adaptable video-surveillance system in order to detect and prevent criminal activities;
- Building a video-surveillance system that functions as a punitive tool in order to store the most relevant evidence of the detected criminal activities.

Rather than providing new methodologies or tools, SmartPrevent will focus on: a) improving already-existing methodologies by means of a set of guidelines for the use of video-surveillance systems; and b) providing a set of tools capable to improve the existing crime detection systems. Our solution will be validated by deploying a realistic prototype scenario, which will actively involve the detection and prevention of crimes in urban areas and the management of these detections by final users.

Expected results

We will develop and provide four important benefits: i) Systematic characterization of usual petty crimes in an area under automatic surveillance; ii) automatic detection of the most usual and frequent criminal activities; iii) a set of automated tools capable of alerting the appropriate responders; and iv) early prevention of crimes by prediction and early detection of crimes.

PARTNERS	COUNTRY
Treelogic Telematica Y Logica Racional para la Empresa Europea SL (TREELOGIC)	Spain
QUeen Mary and Westfield College, University of London (QMUL)	United Kingdom
Vision Semantics Limited (VSL)	United Kingdom
Emza Visual Sense Ltd (EVS)	Israel
Ayuntamiento de Las Rozas de Madrid (ALR)	Spain
Ankara Strateji Enstitusu Dernegi (ASED)	Turkey

CRESCENDO / Coordination action on risks, evolution of threats and context assessment by an enlarged network for an r&d roadmap

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218026
Total Cost
€521,281
EU Contribution
€499,523
Starting Date
01/07/2009
End Date
30/06/2011

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Centre de Saclay- Bât 476
F91191 Gif-Sur-Yvette
Cedex
France
Contact
Mr. Jean-Louis SZABO
Tel: +33 1 69 08 33 71
Mobile: +33 6 07 44 07 13
Fax: +33 1 69 08 18 19

Project objectives

» To strengthen, enlarge and render sustainable the networks created by SeNTRE and STACCATO with Associated Countries;

» To analyse the evolution of threats (aggressions) and risks (accidents) assessment taking into account the balance between security and civil liberties;

» To analyse the policies, the regulations and standardization and encourage the harmonisation of European-wide security related regulations and standards by benefiting from the on-going national and European relevant activities with the support of CEN in connection with existing networks and associations;

» To analyse the innovation process (the demand the supply chain and the links between actors Academia, RTOs, Industries, SMEs, Service sector and End-users);

» To elaborate recommendations for key themes for the Security Research Programme such as emerging technologies, maturity of current systems and areas of improvement, evolution of standards to enhance systems connectivity, regulatory issues if any across EU27 and associated countries in an integrated roadmap;

» To advise on the implications for future programmes as well as on the best way to continue the network and optimize the dialogue between all stakeholders.

Description of the work

On the basis of SeNTRE and STACCATO PASR supporting activities, CRESCENDO will focus on keeping this unique, results-driven, multi-sector public private network alive but also on expanding it, so as to include as many as possible private sector security research requirement owners, operative end-users and technology supply chain experts, including from the new MS in the enlarged EU-27 and the Associated Countries. To achieve the objectives of the project, CRESCENDO work plan is divided into 6 technical work packages:

Organisation and operation of the network

» Experts & stakeholders Identification;
» Expert & stakeholders assessment methodology;
» Network organisation and methodology / workshops;
» Network support tools.

Society security evolutions (threats and risks)

» Assessments of threats and risks;
» Translation into security policies;
» Changing providers of security. The balance between civil liberties and security;
» Supporting the evolution of the security market.

Policies, regulation and standardization

» Regulations Mapping and Analysis;
» Standards Mapping and Analysis;
» Development of a network/expert body for policy suggestions;
» Development of a network/expert body for standardisation and regulations harmonisation proposals;
» Development of working methods and processes for the networks.

Innovation process

- Demand structuring and development;
- Regulation and supply chain;
- Ways to improve the links between the academic sector and industries, SMEs and the service sector;
- ESTIB structuring and supply chain development.

R&D Roadmaps

- Coordination with ongoing research programmes;
- Proposed R&D implementation;
- Launch of other initiatives and programmes (beyond R&D).

Consolidation and continuous dialogue and recommendations for future programmes/projects

- Proposals and recommendations.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique (CEA-LIST)	France
European Aeronautics Defence and Space Company EADS France SAS	France
Astrium SAS	France
Finmeccanica- Societa Per Azioni	Italy
Morpho (SGM)	France
Thales avionics SA	France
Österreischiches Forschung- und Prüzentrum Arsenal GesmbH	Austria
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
European Materials research society	France
Tübitak Marmara research centre information technology institute	Turkey
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.	Germany
Stiftelsen SINTEF	Norway
Fundación Robotiker	Spain
Fondation pour la Recherche Stratégique	France
Instituto Affari Internatiozionali	Italy
European Commission - Joint Research Centre (JRC)	Belgium
European Biometrics forum limited	Ireland
Association française de normalisation	France
Ministère de l'intérieur	France
Center for Security Studies	Greece
AIT Austrian Institute of Technology GmbH (AIT)	Austria

ESC / European Security Challenge

© Lom - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261566
Total Cost
€527,034
EU Contribution
€468,279
Starting Date
01/03/2011
End Date
29/02/2012

Coordinator

GLOBAL SECURITY CHALLENGE LLP
57 Gloucester Place,
London W1U 8JJ
United Kingdom
Contact
Mr Simon Schneider
Tel: +44 (0) 207 224 0110
Email: schneider@globalsecuritychallenge.com
Website:
www.omnicompete.com

Project objectives

Other regions of the world, particularly the US, use competitive incentives such as awards and prizes to encourage innovation in security research, but Europe has lagged in this area.

The focus of this one-year project was to examine how such a model could be used to Europe's advantage. ESC's three-member consortium, consisting of Global Security Challenge LLP (UK), Jožef Stefan Institute (Slovenia) and PR agency 3D Communications (France), was tasked to design prize competitions that encourage innovators (from industry, academia, etc.) to deliver innovation solutions in European security – and to provide ideas and guidelines to the European Commission for doing so.

A parallel objective was to examine how competitions could visibly involve EU citizens in the innovation process.

Results

The ESC team conferred with experts, policymakers, companies and other stakeholders to shape its work, surveying 523 SMEs and interviewing 24 international innovation decision-makers from both public and private sectors, for example.

This led to the definition of three competition packages as options for the Commission to use in the future. The three are:

» the "UAV Crisis Response Challenge", designed to advance unmanned aerial systems (UAS) technology for emergency response to disasters;

» the "Citizens' Frontline Emergency Management Competition" to create open source software applications for emergency management, based on use of social media and modern communications technology;

» the "Cloud Castle Challenge" to encourage the creation of an open source software repository, or 'toolbox', for cyber security and the protection of cloud computing.

ESC's final report will allow European policy-makers to assess the potential for using prize competitions to boost innovation in security.

"Our analysis has shown that both applicants/innovators and prize promoters/sponsors can benefit from prizes," says the team. It adds that contest applicants and winners profit from wide media coverage and easier access to funding for the commercialisation of their research, while contest promoters and sponsors pull in participants from non-conventional fields that traditional methods fail to reach. Indeed, other methods for attracting innovation such as research grants or patents are discussed in the report and compared to prize competitions.

The report ends with a suggestion to integrate prize competitions in the EU's existing funding schemes.

PARTNERS	COUNTRY
Global Security Challenge LLP (GSC)	United Kingdom
3D Communications	France
Institute Jozef Stefan (JSI)	Slovenia

ESCORTS / European network for the security of control and real-time systems

© TebNad- Fotolia.com

RESEARCH COMPLETED

Information

Grant Agreement N°
218217
Total Cost
€1,108,701.75
EU Contribution
€673,603.47
Starting Date
16/06/2008
End Date
15/12/2010

Coordinator

COMITÉ EUROPÉEN DE NORMALISATION (CEN)
Rue de Stassart 36
BE – 1050 Bruxelles
Belgium
Contact
Luc Van den Berghe
Tel: +32 2 550 09 57
E-mail:
luc.vandenberghe@cen.eu
Website:
www.escortsproject.eu/

Project objectives

ESCoRTS was a joint endeavour among EU process industries, utilities, leading manufacturers of control equipment and research institutes, to foster progress towards cyber security of control and communication equipment in Europe. This coordination action addressed the need for standardisation in this area (where Europe lags behind other world actors), indicating R&D directions by means of a dedicated roadmap.

ESCoRTS aimed at the dissemination of best practices on Supervisory Control And Data Acquisition (SCADA) security implementation, thus ensuring convergence and hastening the standardisation process worldwide, and paving the way to establishing cyber security testing facilities in Europe.

Networked computers reside at the heart of critical infrastructures and systems on which people rely, such as the power grid, the oil & gas infrastructure, water supply networks etc. Today these systems are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, or expose private information.

Attacks compromising security of monitoring and control systems may also have negative impact on the safety of personnel, the public and the environment by causing severe accidents like blackouts, oil spills, release of pollutants in the air, water and soil.

Pressure to ensure cyber security of control and communication systems is strong in the US, where industry sectors - electricity, oil, gas etc. are issuing guidelines and have set up a common platform, the Process Control Systems Forum. There national facilities where to test the security of control and communication components are available. In the EU, the importance of the issue starts to be recognized as well: vendors and many users are trying to accommodate what emerges as best practice security. Nevertheless, a common strategy towards standardisation is lacking; the efforts are scattered across industrial sectors and companies. In addition, due to the lack of testing facilities in the EU, manufacturers and operators currently need to resort to US cyber security facilities to verify their products and services.

Description of the work

The key objectives of ESCoRTS include:

» Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation, accompanied by a raising awareness programme reaching all stakeholders;

» Identifying and disseminating best practice, possibly in a joint endeavour between manufacturers and end users, resulting in a joint capability and technology taxonomy of security solutions;

» Stimulating convergence of current standardisation efforts. Liaising with international efforts and especially with the US Process Control Forum;

» Developing a strategic R&T and standardisation roadmap;

» Developing and deploying a secure ICT platform for the exchange of relevant data among the stakeholders;

» Identifying requirements for appropriate test platforms for the security of process control equipment and applications.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
COMITÉ EUROPÉEN DE NORMALISATION (CEN)	Belgium
AREVA T&D SA (Areva)	France
Enginet srl (EngiNet)	Italy
UNINFO - Associazione di Normazione Informatica (UNINFO)	Italy
OPUS PUBLISHING GENERAL PARTNERSHIP (OPUS)	The United States
COMPANIA NATIONALA DE TRANSPORT AL ENERGIEI ELECTRICE TRANSELECTRICA SA (Transelectrica)	Romania
ENEL PRODUZIONE. S.P.A. (ENEL)	Italy
MEDITERRANEA DELLE ACQUE S.p.A. (Med-d-Acque)	Italy
SIEMENS AG (Siemens)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
ABB SCHWEIZ AG (ABB)	Switzerland
Enel Ingegneria e Innovazione SpA (ENEL spa)	Italy

ETCETERA / Evaluation of critical and emerging technologies for the elaboration of a security research agenda

© ETCETERA

RESEARCH COMPLETED

Information

Grant Agreement N°
261512
Total Cost
€1,996,728
EU Contribution
€1,512,742
Starting Date
01/10/2011
End Date
30/09/2013

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen
Appelsgarten 2
53879 Euskirchen,
Germany
Contact
Joachim Burbiel
Tel: +49 2251 18 213
Fax: +49 2251 18 38 213
E-mail: joachim.burbiel@int.fraunhofer.de
Website: www.etcetera-project.eu

Project objectives

The ETCETERA project is a contribution to effective and efficient security research planning on a European level. Its aim is three-fold:

- » to develop novel methodologies for future strategic research planning;
- » to identify risks and potential benefits associated with Critical Dependencies and Emerging Technologies with security implications; and
- » to recommend a research agenda to deal with these risks and potential benefits.

Description of the work

ETCETERA's structure is separated into strands, one for Critical and the other for Emerging Technologies. These strands are separate but interrelated. Each strand is further divided into three Work Packages that will be carried through in a sequential manner. Two consultation campaigns will generate input from technical experts, end-users, and public authorities.

Strand 1: Critical Technologies

The first research strand (Work Packages 1 to 3) can be envisaged as a filtering exercise. Starting from all possible technologies, technologies indispensible for European security now and in the near future will be identified through extensive consultations within the consortium and with external experts.

In the second work package, the validated list of Critical Technologies will be checked for Critical Dependencies. Critical Dependencies arise if European industry is not self-sufficient in providing critical technologies/systems/capabilities to end users. Those dependencies could be caused by extra-European intellectual property rights (IPR), trade and academic restrictions, restrictions due to high classification in dual-use technologies, and economic challenges (e.g. shifting production sites, hindering or underdeveloped norms and standards, failing business models).

The last work package of Strand 1 will propose and prioritise alternative solutions to alleviate the Critical Dependencies identified. Strand 1 is associated with the 1st Consultation Campaign which includes five parallel workshops held at five locations and in six languages.

Strand 2: Emerging Technologies

In the first work package of Strand 2, Emerging Technologies are scanned for their security implications in 10 to 20 years time. Three scanning methods are implemented in a parallel fashion by AIT, Fraunhofer INT, and Isdefe. A comparative analysis of the results of these three methods will then be performed.

Emerging Technologies identified to be most relevant will be analysed in depth in the second work package of this strand. Furthermore, it is envisaged to adapt the originally military Disruptive Technology Assessment Game (DTAG) to civil scenarios and to set up an evaluative scenario workshop.

In the last work package of the strand, all results on Emerging Technologies will be considered when developing recommendations for an Emerging Security Technology Research Agenda (ESTRA).

Results

Several new approaches for research planning have been developed and analysed. Among these is an enhanced and novel technology scanning method based on three established techniques. Other methods applied and compared were participatory processes and technical approaches utilising scientific metrics. Based on this broad methodological framework, tentative results concerning the development of research agendas to overcome critical dependencies and to harness opportunities of emerging technologies were developed. Ethical aspects have been taken into account at all levels of the project. The final report is available at www.etcetera-project.eu

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Ingeniería de Sistemas para la Defensa de España, S.A. (Isdefe)	Spain
Universität Duisburg-Essen (UDE)	Germany
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
VDI Technologiezentrum GmbH (VDI-TZ)	Germany
Morpho (MPH)	France
Ansaldo STS S.p.A. (ASTS)	Italy
COMSEC Unternehmensgruppe (COMSEC)	Germany
Centre for Science, Society and Citizenship (CSSC)	Italy
Storstockholms brandförsvar (SSBF)	Sweden

SECURECHAINS / Integration of security technology supply chains and identification of weaknesses and untapped potential

© bisougue - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242417
Total Cost
€1,082,006.63
EU Contribution
€820,032
Starting Date
01/05/2010
End Date
30/04/2012

Coordinator

SERVIÇOS DE CONSULTADORIA EM INOVAÇÃO TECNOLÓGICA, S.A.
Contact
Alexandre Almeida
E-mail: alexandre.almeida@inovamais.pt
Website:
www.securechains.eu

Project objectives

The SecureCHAINS project's main mission is to contribute to more competitive Security Technology Supply Chains (STSC). The project will cooperate with the industry to gain a better understanding of the nature and structure of the STSC from prime contractors to subcontractors coming from the various tiers of the supply chains.

The SecureCHAINS project will have the following **six main objectives**:

» identify supply chains and stakeholders;

» detect untapped potential that can be integrated in the European STSC;

» engage innovative low tier suppliers in the STSC;

» contribute to the building of R&D competences in the STSC;

» develop awareness building activities in Security related RTD topics; and

» promote and facilitate a communication platform/website and open dialogue in the fields related to Security Technology management, regulation, policy and forecasting.

Description of the work

The SecureCHAINS project will be carried out along the following four main axes of activities:

» To identify opportunities and weak spots in the supply chains. The technology tree drawn up for a research project will involve areas of technology of different degrees of maturity. We will apply the concept of 'technology readiness levels' to determine technical maturity. Immature technology so identified would be considered as a weak spot and the SecureCHAINS project would advise on how this might be strengthened;

» To involve the best intellectual and technological capabilities available throughout Europe in the security technology supply chains;

» To help organisations (SMEs, RTOs, Large Firms, etc.) to understand security related targets, mechanisms and opportunities;

» To facilitate the organisations' access to the main stakeholders and integrators, while protecting their intellectual property.

The SecureCHAINS project is structured into 5 workpackages (WP):

» *WP1* Security Technology Supply Chains framework setting;

» *WP2* Analyses of the Supply Chains;

» *WP3* Increasing SME engagement in the STSC;

» *WP4* Technology Search & Transfer;

» *WP5* Dissemination and Future exploitation results and activities.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Serviços de Consultadoria em Inovação Tecnológica, S.A. (INOVAMAIS)	Portugal
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Deutsche Post World Net Market Research and Innovation GmbH (DHL Innovation Center)	Germany
INNOVA SPA	Italy
SOLLERTA Ltd	United Kingdom
FUNDACION ROBOTIKER	Spain
Mr. Juergen K. von der Lippe and Dr. Jean Cornier	Germany
UNIVERSITATEA DIN CRAIOVA	Romania
ALMA CONSULTING GROUP SAS	France
TECHNICAL SUPPORT FOR EUROPEAN ORGANISATIONS SPRL	Belgium
SOUTHEASTERN EUROPE TELECOMMUNICATIONS & INFORMATICS RESEARCH INSTITUTE	Greece

SecurePART / Increasing the engagement of civil society in security research

Information

Grant Agreement N°
608039
Total Cost
€966,039.50
EU Contribution
€889,888.00
Starting Date
01/05/2014
Duration
24 months

Coordinator

BANTEC CONSULTORES INICIATIVAS EMPRENDEDORAS S.L. + (BAN)
European projects
Parque Empresarial Zuatzu
6, piso 1, puerta 2
20018
San Sebastián, Guipuzcoa,
Spain
Contact
Elizabeth Isaacs
Tel: +34 943314990
Mobile: +34 942277887
Fax: +34 943314990
E-mail: ei@bantec.es
Website: www.bantec.es

Project objectives

SecurePART seeks to achieve four main objectives:

1. To study civil society organisations (CSOs) and CSO networks, identify bottlenecks and untapped potential for their engagement in security research, and foster their collaboration with other stakeholders, including: technology developers, public security providers, policy makers and researchers

2. To explore opportunities for funding offered within the EU security research programme, and provide advice to the EU Commission in order to overcome barriers to CSO participation

3. To develop a strategy and action plan to help increase CSO involvement in the delivery of security research projects and in shaping the EU research programme.

4. To promote a more inclusive, responsive and legitimate approach to security research and innovation

Description of the work

There is a need for a more structured civil society engagement at European level regarding security research. The SecurePART project is implementing eleven main tasks grouped by type of activity:

Activity 1 – Analysis and studies

a. Analyse the content and status of FP7 security research projects.

The project will conduct research about the current CSO involvement in security research actions, based on the six different roles they can play: policy observers, project evaluators, programme agenda influencers, partners in projects, commissioners of research, and programme & project disseminators. Following the quantitative analysis, a pooling by experts will enable qualitative analyses to be carried out.

b. Review of non-security focused research that also has a similar problem of acceptance by society.

Identify best practices in other technology R&D sectors which face similar challenges of inclusion and acceptance by society, like the chemical technology industry, genetics technology, etc.

c. Societal & CSO analyses

Analyse the intra-, inter- and trans-CSO dimensions. A model of public policy stakeholder management along criteria of high/low power and high/low interest will map the relative influence of CSOs in research, and identify weaknesses, strengths, risks and opportunities.

Activity 2 – Increase the engagement of CSOs in security research

d. Development of a communications plan about potential benefits of security research activities

The main objective here is to bring together stakeholders from all sectors – CSOs & other security research stakeholders – to work out a 'case for action', creating awareness and fostering mutual dialogue.

Activity 3 – Future strategy & Action plan

e. Strategy for increasing CSO participation & action plan

The action plan will make recommendations on how to/integrate CSOs within the security research policy cycle.

Expected Results

SecurePART is committed to increasing awareness amongst CSOs and other stakeholders about benefits and opportunities to participate in EU-funded security research under the Horizon 2020 research programme and beyond.

PARTNERS	COUNTRY
Mr. Juergen K. Von der Lippe and Dr. Jean Cornier (VDL)	Germany
European Network of National Civil Society Organizations (ENNA)	Belgium
Nexus Institute fur Kooperations Management und Interdisziplinare Forschung (NEXUS)	Germany
Johann Wolfgang Goethe Universitaet Frankfurt am main (GUF)	Germany
The University of Salford (SAL)	United Kingdom
GLOBAZ, S.A. (LOBA)	Portugal

STRAW / Security Technology Active Watch

© Nmedia - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218132
Total Cost
€1,341,933.33
EU Contribution
€998,537
Starting Date
01/10/2008
End Date
31/05/2010

Coordinator

ATOS ORIGIN SAE
Atos Research & Innovation
Albarracín, 25.
28037 Madrid
Spain
Contact
Aljosa Pasic
Tel: +34 91 214 88 00
Fax: +34 91 754 32 52
E-mail: aljosa.pasic@
atosresearch.eu

Project objectives

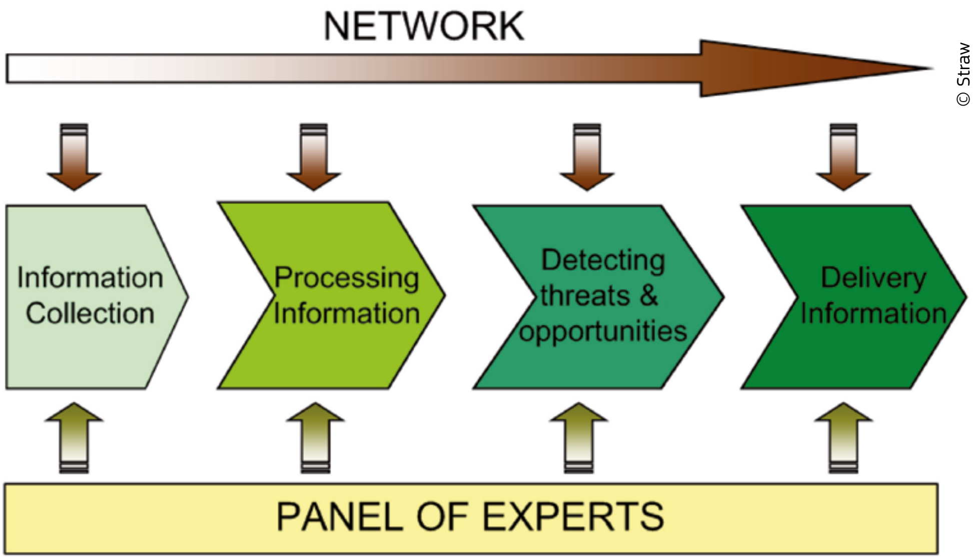
The STRAW project aimed to enhance European civil security by facilitating cooperation amongst various stakeholders, including researchers, technology providers and end-users.

Its mission was to monitor the security domain in order to detect relevant and applicable security technology developments, knowledge, experience and stakeholders. It also strove to deliver this information to the right audience at the right time to better exploit the information.

Results

The project began by creating a comprehensive review and cataloguing framework for evaluating thematic, technical and structural developments in security technology. This included creating a taxonomy structure for defining a concept map composed of classes, sub¬classes and name relations between technology areas. This served as the core of the semantic processing tool for the project's Security Technology Watch.

The main outcome of the project was "STRAWiki", an online portal tool based on wiki software that allows users to constantly update technology information in an online depository.



© Straw

PARTNERS	COUNTRY
Atos Origin SAE	Spain
Aerospace and Defence Industries Association	Belgium
Thales Services	France
Sitftelsen SINTEF	Norway
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Instituto Nacional de Técnica Aeroespacial	Spain
Elsag Datamat S.p.A.	Italy
Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España	Spain
Fondazione Rosselli	Italy
European Organisation for Security	Belgium

DITAC / Disaster Training Curriculum

© Arkadi BojarÜinov - iStockphoto

Information

Grant Agreement N°
285036
Total Cost
€4,466,505.80
EU Contribution
€3,498,668
Starting Date
01/01/2012
Duration
36 months

Coordinator

UNIVERSITY CLINIC BONN GERMANY
Department of Orthopaedics and Trauma Surgery
Sigmund Freud Street. 25
53127 Bonn, Germany
Contact
Dr. Philipp Fischer
Tel: +49 1607234539
Mobile: +49 1607234539
Fax: +49 1607234539
E-mail: philipp.fischer@ukb.uni-bonn.de
Website: www.ditac.info

Project objectives

The DITAC Project will:

» analyse concepts, methods, and doctrines of crisis response and identify the relevant European competences of crisis management;

» analyse existing initiatives on generating curricula for crisis management;

» identify the requirements of the local actors in crisis management education;

» identify the needs of relevant actors and the resulting stakeholder requirements for significant improvement of trainings in international disaster response and crisis management;

» develop a didactic concept to transmit common standards for crisis management education, using state of the art methods for teaching and training;

» organize a pilot study course for suitable participants from European countries;

» prove an evaluation tool for the course based on the developed curriculum.

Description of the work

The DITAC project proposes to develop a holistic training curriculum for first responders and strategic crisis managers dealing with international crises. The DITAC Curriculum will address the key challenges for the management of disaster incidents.

It will develop a standardised strong, comprehensive and efficient EU wide approach to crises and disasters to feature the added value by EU coordinated actions in the field of crisis response. The curriculum will improve the preparedness and availability of trained personnel by providing a common language, common objectives and common tools leading to better results in the protection and assistance of people confronted with large scale crises.

The focus is on international crisis management, but the benefit of a standardised training programme in crisis and disaster response can also be used to increase Europe's resilience in facing disasters and crises within the European Union. Establishing curricular training on how to respond to an international crisis and making it accessible to pertinent organizations throughout the EU will be a first step towards building a European Emergency Response Centre. Collaboration of specialists for disaster response as single experts in the field of international crisis management with local, regional and international authorities, NGOs, training institutes, scientific societies, research institutes and the cooperation of experts with backgrounds in medical, psychological and technical emergency assistance, logistics, conflict analysis and security challenges will create synergies towards improved disaster response capacity in the European Union.

The DITAC Project will use open sources for dissemination during the project period in order to get continuous feedback, and will organize public meetings and congresses to reach a consensus about the curriculum's content.

Expected results

- » addresses the overall effectiveness and performance of the response and not just of the individual agencies;
- » can be adapted to different geopolitical, organisational and geographic settings;
- » creates an environment supporting progressive learning and enrichment, even beyond the scope of the project;
- » supports effective collaboration and dialogue between EU member states and beyond;
- » defines and develops educational tools which allow for preparing for and responding to major disasters in general.

PARTNERS	COUNTRY
University Clinic Bonn Germany (UKB)	Germany
Prehospital and Disaster Medicine Centre (PKMC)	Sweden
Hanover Associates (HA)	England
Center for Research in Emergency and Disaster Medicine (CRIMEDIM)	Italy
Clinical Emergency Hospital Bucharest (URGENTA)	Romania
Nations Health Career School of Management gGmbh (NHSC)	Germany
General and Teaching Hospital Celje (SBC)	Slovenia
Istanbul Aydin University (AFAM)	Turkey
Croatian urgent medicine and surgery association (CROUMSA)	Croatia
German Aerospace Center (DLR)	Germany
Bonn International Center for Conversion (BICC)	Germany
GABO:mi Gesellschaft für Ablauforganisation:milliarium mbH & Co. KG (GABO)	Germany

LEILA / Law Enforcement Intelligence Learning Applications

Information

Grant Agreement N°
608303
Total Cost
€1,978,327.45
EU Contribution
€1,499,837.00
Starting Date
01/04/2014
Duration
24 months

Coordinator

GLOBO TECHNOLOGIKI – PLIROFORIKI ANONYMI ETAIREIA, IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALEIAS
R&D
37 A Psaron str.
152 32 – Halandri – Greece
Contact
Manos Foufoudakis
Tel: +30 2121217216
Mobile: +30 6936660395
Fax: +30 2106466165
E-mail: mfoufoudakis@globogr.com
Website:
www.leila-project.eu

Project objectives

Intelligence analysis (IA) professionals are faced with daily challenges to meet high demands for rapid, accurate assessments that require discovery and marshalling of evidence, integration and synthesis of data from disparate sources, interpreting and evaluating information that is constantly changing, and providing documentation and recommendations (intelligence products).

The definition of the new competences and skills needed by the next generation of intelligence analysts is crucial to the design of effective learning curricula that can better address the training needs of law enforcement agents.

The emerging learning model for intelligence analysis should integrate methodologies and tools designed to improve critical thinking, awareness of cognitive biases, improved capabilities in filtering and analyzing massive amount of data (even available online and in different languages), decision making under social and time pressure, collaboration skills, creative intelligence, reporting and communication skills.

The aim of the LEILA project is to provide law enforcement organizations with innovative learning methods to address the improvement of intelligence analysis in regards to the aforementioned capabilities and skills.

The radical innovation of the LEILA holistic approach is due to the combination of several fields which are normally explored and applied separately, such as:

» psycho-sociological and cognitive factors in decision making (e.g. decision biases, critical thinking, multiple reasoning strategies, creativity);

» decision making strategies under uncertainty (e.g. Bayesian approaches, game theory);

» group interaction dynamics in intelligence analysis.

A variety of learning experiences (e.g. games of deterrence, intelligence analysis under stress, emergence in highly collaborative situations) are simulated and computerized in different games that offer the possibility to actively acquire the new IA skills from different angles.

To reach these aims, the project evolves towards three research outcomes:

1. Analyze and describe the specific skills and competences of the intelligence analysts by exploring different characteristics and abilities and identifying learning needs and areas of improvement;

2. Design an innovative methodology and a set of learning experiences to address the specific needs of intelligence analysts;

3. Develop and validate a set of serious games that enable trainees to acquire the skills and competencies requested by their role.

Description of the work

The work plan is based on an iterative and action oriented user-centric approach that involves different actors and guarantees the substantive quality of the technological research. More specifically, the different participants include end-users, domain experts, cognition specialists, educational experts, and technological and learning game designers, allowing for each actor to bring its particular competence to the project. The LEILA project covers both the practical and theoretical perspectives in an interrelated manner.

Expected results

The expected results of LEILA project is to provide the trainee with a comprehensive and consistent set of tools enabling him/her to appropriately analyze available data, search for extra data, transform raw data into meaningful information with respect to the case under consideration, and draw conclusions about this case, as well as to support all enabling factors that help the trainee to accomplish the task efficiently.

PARTNERS	COUNTRY
GLOBO TECHNOLOGIES SA	Greece
ORT France	France
Alphalabs Sarl	France
Zanasi & Partners	Italy
FVA New Media Research	Italy
National Defense University CAROL I	Romania
Center for Security Studies	Greece

SAFECITI / Simulation Platform for the Analysis of Crowds Behaviour in Urban Environments with Training and Predictive Capabilities

Information

Grant Agreement N°
607626
Total Cost
€1,899,049.28
EU Contribution
€1,442,733.96
Starting Date
01/03/2014
Duration
24 months

Coordinator

NEXT LIMIT S.L (NL)
SAFECITI
Calle Angel Cavero 2
28043 Madrid (Spain)
Contact
Victor Gonzalez
Tel: +34 917 160 214
Fax: +34 917 219 464
E-mail:
safeciti@nextlimit.com
Website:
www.nextlimit.com

Project objectives

The SAFECITI project proposes the creation of a simulation system for police intelligence analysts to predict the behaviour of crowds in urban environments under specific threats or stresses (e.g. turmoil, violence, panic, catastrophes or terrorism) to train officers and develop better safety plans and tactic operations.

This platform will be designed both as a simulation platform for training purposes and as a predictive tool for operational use. The platform will include performance measurement tools based on safety goals (people and infrastructure damage) to measure the skills of the analyst. All the simulations will be stored in a database to work as a historic repository but also, more interestingly, as a large set of useful data to be re-analyzed by artificial intelligence algorithms to create predictive models. The main goal of this predictive model will be the creation of a virtual analyst that is able to recommend actions based on the enriched analysis of hundreds or thousands of simulations.

Description of the work

The development of the simulation platform involves several technological challenges that will be covered in the work plan:

» Requirements and specifications: definition of the specifications mainly driven by end user requirements; serious game technology selection; requisite verification methodology;

» Interactive graphical platform, interfaces and control system: development of the main control system, integration of all the modules in the interactive platform; user interfaces; scene setup; interactive workflow, control and network modules;

» Graphics components: 3D models for human representation, static and dynamic versions, 3D vehicles and graphics optimization;

» Generation of urban environment: development of urban generation module (as the project aims to simulate realistic environments);

» Advanced crowd simulation: design and development of the crowd simulation engine that initializes and updates the entities, their behaviours and their actions on the environment;

» Database module and predictive model: development of database components and predictive models, which provide a very powerful tool for expanding the framework of the project beyond classic e-learning;

» System validation: validation of the system. Field expertise by the Spanish national police department will help to validate and test the system.

Expected results

SAFECITI will not only improve the training methodologies and performance measurement of the analysts, but will create an innovative profile for new-generation analysts who will be trained in a first stage and operate the system later during their whole operational life, thus helping to enrich the system with new simulations and validation cases. These new analysts will be able to project new operational plans in advance by simulating "what-if" cases in complex scenarios, and anticipating threats.

The main expected impacts of SAFECITI are:

- improvements in the safety of citizens against different threats;
- threat anticipation and adequate response through planning;
- development of next-generation intelligence analysts;
- technologies and services for new SMEs' business development.

PARTNERS	COUNTRY
Next Limit S.L. (NL)	Spain
Griffin Softfware SRL (GR)	Romania
Golaem S.A. (GO)	France
ESRI R&D Center Zurich AG (ESRI)	Switzerland
Politecnico di Torino (POLITO)	Italy
Ministerio del Interior (MIR-DGP)	Spain

LIST OF PROJECTS

LIST OF PROJECTS

NOTES

NOTES

NOTES

European Commission

Luxembourg: Publications Office of the European Union, 2016

2016 — 636 pp. — 21 cm x 29.7 cm

ISBN 978-92-79-56875-6
doi:10.2837/796260

DR-02-16-187-EN-N

Security Research Projects
under the 7th Framework Programme for Research

EU Research for a Secure Society

Further information available at:
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/industry-for-security/index_en.htm

Publications Office