Security Research

Protecting Europe's homeland and its future

European Commission
Enterprise and Industry

SEVENTH FRAMEWORK PROGRAMME

Acronyms used in this publication

CBRNE – Chemical, biological, radiological, nuclear, explosive

CCTV – Closed circuit television

CEN – European Committee for Standardisation

CENELEC – European Committee for Electrotechnical Standardisation

DG-ENTR – Directorate-General for Enterprise and Industry

ETSI – European Telecommunications Standards Institute

EU – European Union

FP7 – EU's 2007-13 Seventh Framework Research Programme

NGO – Non-governmental organisation

SCADA – Supervisory control and data acquisition

SMEs – Small and medium sized enterprises

A great deal of information on the European Union is available on the internet.
It can be accessed through the Europa server (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2011

ISBN 978-92-79-20949-9
doi:10.2769/29014

Printed in Belgium, 2011

Cover picture: © Konstantin Sutyagin/fotolia

Printed on processed chlorine-free recycled paper (PCF)

Foreword

© EC

These are turbulent times for the international community as it grapples with a convergence of economic, political and natural disaster challenges. Preventing and dealing with instability and the unknown – be it man-made or natural – but bouncing back from any adverse effects is the raison d'être of the EU's Security Research Programme.

Now well into the second half of its seven-year (2007-13) life, much of the programme's pragmatic emphasis is shifting to user-driven applications and large-scale projects. The latter will demonstrate "system-of-systems" capabilities designed to protect complex structures and societal functions such as wide-area public spaces and events, critical infrastructure in energy and communications or real-time surveillance of Europe's extensive coastline. Protecting against attacks on multi-mode transport points, where buses, trams and trains may converge under a shopping mall, is but one example of the complexity facing Europe's civil security planners. Indeed, that is the goal of one of its new demonstration projects.

Other medium and smaller-sized Security Research projects will continue to research the best ways to support other civil security objectives. These include the EU's fight against organised crime such as financial fraud, securing its ports, harbours and airports or knitting together Europe's first-responder communities across borders by boosting their ability to exchange data seamlessly and quickly. Such common "situational awareness" – the product of integrated detection and communications technologies – cuts across many Security Research projects, from border management to protection against chemical or biological threats.

Common to all Security Research capability objectives, however, is the EU's obligation to ensure that security technologies are thoroughly based on democratic values and rights of the citizen. So too is the obligation to get value for money, which is why each project is closely scrutinised to ensure there is no duplication of efforts at national level.

Two key strands running through the programme are equipment interoperability and the promotion of common technical references and industrial standards. Both are designed to promote a pan-European market in civil security goods and services, thus stimulating job creation, economic growth and a firm place for European players in the burgeoning global market for civil security goods and services.

The Security Research programme is already pursuing some of these goals such as the development of dual-use capabilities that offer spin-offs from civil security into defence applications. More industrial initiatives will be proposed in 2012.

By the time it draws to a close at the end of 2013, the Security Research programme will have supported approximately 250 innovative research projects involving more than 2,500 participating entities from all walks of European society, business and research. It has been a ground-breaking effort to draw all these actors together towards a common goal. As the fruits of Security Research now move into the real world, we can be proud of the achievements attained so far – and those that will unfold in the future.

ANTONIO TAJANI

Vice-President of the European Commission
Commissioner for Enterprise and Industry

Antonio Tajani

Table of contents

© majeczka/shutterstock

Introduction

Few would dispute that our society is safer and more secure than in the days of our grandparents but, as first-responders everywhere know, we should never take that for granted. Europe's security is constantly being tested by new threats and problems. To keep these at bay, we must remain collectively vigilant and prepared. This lies at the heart of the EU's Security Research programme.

Having just moved beyond its mid-term point, the programme – worth EUR 1.4 billion during 2007-13 – represents a broad and rich agenda of scientific work and industrial cooperation. At its core are hundreds of R&D projects of every size that are producing innovation in all areas of civil security, from border management to disaster relief and protection of critical infrastructures.

This effort is anchored by:

- close interaction with societal groups and advisory experts on the ethical aspects of Security Research such as privacy and the protection of personal data
- regular consultations with civil security stakeholders and especially end-users to gather their ideas and feedback on the programme's research goals
- key industrial policy initiatives by the Commission to promote technical interoperability between the 27 EU nations for a common civil security market and thus economic growth and job creation

The crux of the programme, however, remains its civil security R&D effort, which cuts across a huge array of civil security technologies and capabilities – each strongly underpinned by respect for Europe's democratic values.

The Security Research programme is aligned to the EU's four main security missions. These are:

- **Security of the citizen** (civil protection, bio-security, protection against crime and terrorism, etc.)
- **Security of infrastructures and utilities** (protecting critical infrastructure in transport, energy, computer networks and other service sectors)
- **Intelligent surveillance and border security** (development and deployment of equipment, tools and methods to protect Europe's land and sea borders)
- **Restoring security & safety in case of crisis** (provision of technologies, communications and planning tools for civil, humanitarian and rescue tasks)

These are supplemented by three "cross-cutting" missions, based on:

- Improving the **integration, interconnectivity and interoperability** of security systems
- Analysis of the **socio-economic, political, cultural and ethical** aspects of security
- **Coordinating and structuring** civil security activities across the 27 EU nations and the associated countries

Mission 1

Security of the Citizen

Protecting Europe's citizenry against harm is a daunting challenge since the threats – and possible targets – are potentially vast. These threats range from the mundane such as economic corruption to the highly complex such as organised crime or chemical, biological and radiological attacks.

Research in these areas is largely focused on technology solutions to improve civil protection or bio-security, for example, while minimising the possibilities for crime or malevolent acts. Much of the research emphasis is placed on threat awareness and detection, identification and authentication techniques, prevention and preparedness or threat neutralisation and post-incident resiliency.

Pre-emptive detection of bombs or bomb-making facilities via multiple sensor networks in urban environments is an important objective, for example. It calls for "intelligent" networks that function with clear controls and rapid, if not automatic, methods of threat traceability.

Certain commercially available chemicals, for example, have the potential to be turned into weapons. This calls for techniques that can analyse their supply-chain origins. This also applies to Europe's food-supply chain, which is susceptible not only to deliberate threats but to naturally occurring ones such as diseases or inadvertent infections.

Another aspect of citizen security is to prevent corruption, fraud and financial crime, which calls for the development of advanced forensic toolboxes. These bring together the best practices, methodologies and technical standards to reconstruct crime scenes, improve the interpretation of evidence and strengthen prosecution. A number of projects aim to make such tools applicable and available to all EU Member States.

Many of these threats stem from organised crime, so considerable research is going into the development of new data extraction techniques and transformation tools to support operational and policy knowledge management about organised crime and its political impact.

Indeed, the detection-identification-authentication research approach protects the citizen in many ways. Economic crime can be countered via tools that guard against money laundering and terrorist financing. Or they can help prevent dangerous counterfeit medicines by filtering them out of the marketplace, while enabling public authorities to trace how criminal gangs operate in this sector.

© Monika Wisniewska/123rf

PLANTFOODSEC

Protecting Europe's food chain against health threats

Europe's agro-food sectors depend not only on tightly inter-linked production and distribution networks but on a high level of public confidence that products are safe to eat. It only takes one safety oversight – or threat – to bring the whole system quickly to a halt. Rapid-fire detection, surveillance and counter-measure action is central to keeping our food chains safe and healthy.

Protecting this complex "farm-to-fork" production chain from inadvertent or deliberately manipulated pathogens and pests is the crux of the research project known as "PlantFoodSec" (Plant and Food BioSecurity).

Launched in February 2011 with EU support of EUR 6 million, PlantFoodSec is a five-year project whose goal is to create a virtual international "centre of competence" by knitting together networks of experts to strengthen bio-security training and research in Europe.

As bio-security is a relatively new field in Europe, PlantFoodSec's 13-strong research consortium also includes researchers from the United States and Israel, where food production threats have been studied for longer. PlantFoodSec will also build on the research results of previous EU projects that have studied various aspects of bio-security.

The project's main research objectives are to:

- improve disease surveillance and detection systems via tighter international cooperation among laboratories to prevent the use or spread of deliberately-introduced pathogens into the farm-to-fork production chain
- assess forensic techniques regarding pathogens on plants to enhance prevention, response or recovery from food-borne illnesses
- build a strong "culture of awareness" about bio-security issues across all sectors of agriculture and food production

PlantFoodSec's main end-users will be national and EU-level authorities responsible for plant health – and ultimately that of the European consumer. It will thus help ensure that Europe's dinner table continues to remain safe.

>> www.plantfoodsec.eu

Mission 2

Security of Infrastructure & Utilities: protecting society’s critical functions

”Critical infrastructure” refers to any asset or system that is vital to the maintenance of society such as the provision of energy, transport or health services. Increasingly these are linked not only within but across the 27 Member States (and neighbouring countries), meaning their disruption would pose a major threat to the EU and its 500 million citizens. Strengthening the security of critical infrastructure is a natural focus for Security Research, which involves the analysis and reinforcement of these systems’ interdependence.

Energy sites are a good example as they could be the target of either deliberate acts – terrorism, sabotage or criminal activity – or haphazard ones such as accidents, natural disasters or negligence. Certain projects are researching the tools needed to identify vulnerabilities along Europe’s energy grids and energy plants, and how to protect them against the cascading effects of a disruptive incident.

Critical infrastructure also refers to the resilience of public spaces such as transport terminals or shopping malls. Research here focuses on the planning, redesign and reengineering needed to protect urban environments against attacks or accidents. Part of the challenge is to integrate “smart” surveillance and information systems with improved sensor technology to build up local situation awareness that allows operators to take rapid decisions to protect their infrastructure against an incident or to recover quickly if there is one.

The many paths to Security Research

The scale of any SR project falls into one of three broad categories:

- Capability projects: single technology efforts
- Integration projects: groups of related technologies or capabilities
- Demonstration projects: system-of-systems equipment and capabilities

Where a typical Capability project might have a budget of EUR 3 million or less, Demonstration projects get co-funding from the EU that can be as high as EUR 20 million or more to test and exercise advanced security systems and concepts whose cost might be too high for an individual Member State to shoulder.

ESCORTS

Scoping out SCADA in Europe

Most modern industrial processes – from chemical manufacturing to electricity production – are controlled by software known as "supervisory control and data acquisition" or SCADA. He who controls SCADA controls the process.

Today networked computers lie at the heart of critical SCADA systems on which society relies: power grids, oil and gas infrastructures, water supply networks, etc. Some of these may be using outdated or older-generation software that is vulnerable to attacks. A good illustration was the notorious but unsuccessful attack in 2010 by the "Stuxnet" worm that targeted the SCADA systems of Iran's nuclear research facilities.

The potential consequences of such an attack could be huge, as an attack could do any of the following: inhibit a system's operation, corrupt or expose its private data or compromise the safety of personnel or the public at large by causing accidents such as blackouts, oil spills or the release of pollutants.

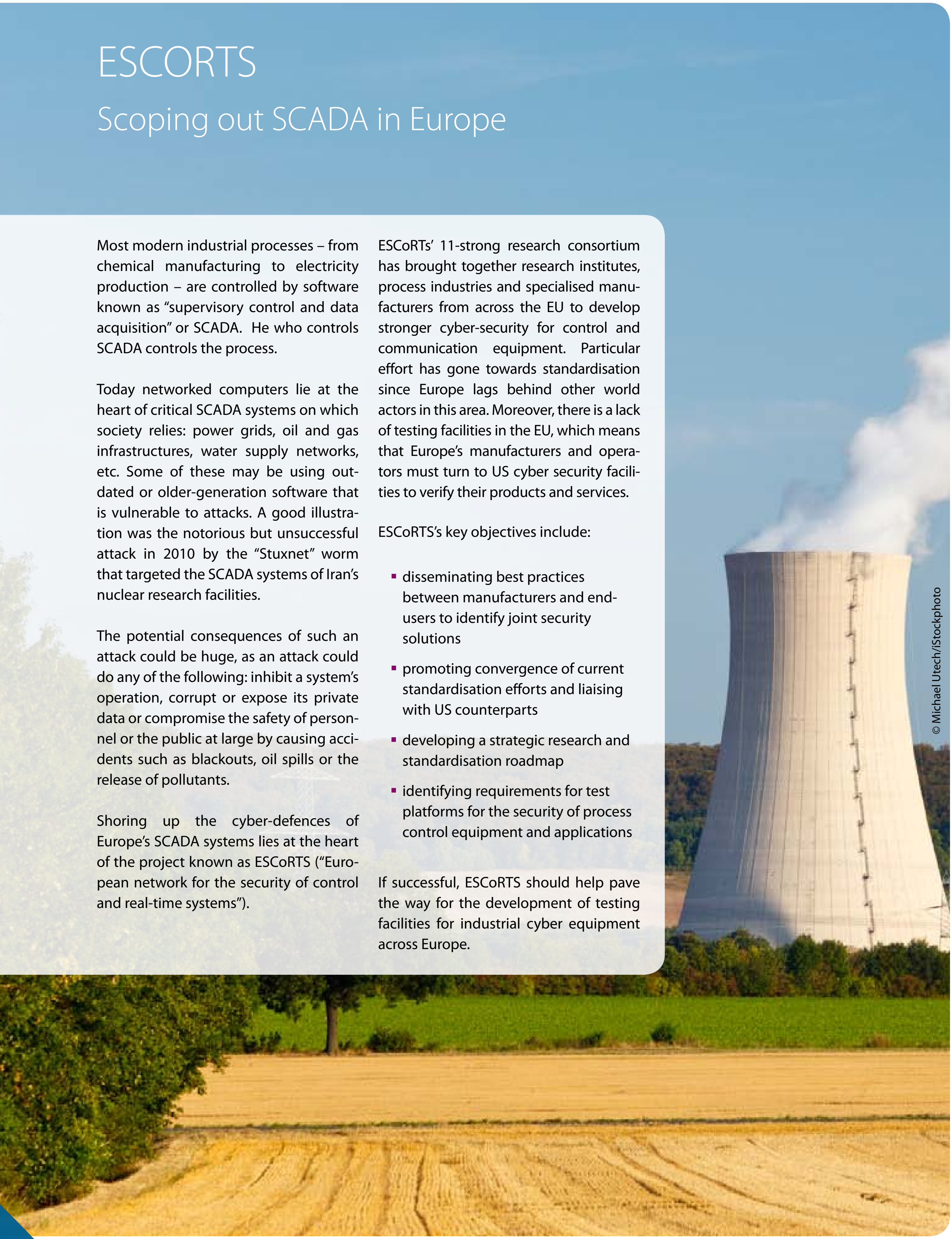
Shoring up the cyber-defences of Europe's SCADA systems lies at the heart of the project known as ESCoRTS ("European network for the security of control and real-time systems").

ESCoRTs' 11-strong research consortium has brought together research institutes, process industries and specialised manufacturers from across the EU to develop stronger cyber-security for control and communication equipment. Particular effort has gone towards standardisation since Europe lags behind other world actors in this area. Moreover, there is a lack of testing facilities in the EU, which means that Europe's manufacturers and operators must turn to US cyber security facilities to verify their products and services.

ESCoRTS's key objectives include:

- disseminating best practices between manufacturers and end-users to identify joint security solutions
- promoting convergence of current standardisation efforts and liaising with US counterparts
- developing a strategic research and standardisation roadmap
- identifying requirements for test platforms for the security of process control equipment and applications

If successful, ESCoRTS should help pave the way for the development of testing facilities for industrial cyber equipment across Europe.



© Michael Utech/iStockphoto

Mission 3

Border Management: intelligent surveillance of our frontiers

Border management means preventing illicit activities such as smuggling goods and people while facilitating the legitimate needs of citizens and businesses. This presents an immense challenge to Europe with its extensive land and sea borders.

Across Europe's land borders illegal crossings are often made on foot, taking advantage of difficult or hard-to-survey terrain. As for our maritime borders, the threats and risks concern both security and safety. Here, the detection and tracking of small craft of all types is of particular concern. But it's not just about water or land frontiers: airspace is also a common route for smuggling and other illegal activities.

Meeting such challenges implies a strong reliance on risk analysis, intelligent surveillance and border security capabilities: i.e. the technologies, equipment, tools and methods that effectively and affordably protect Europe's frontiers and thus its internal security.

Most risk and foresight scenarios in Europe agree that border management will remain a long-term critical capability in view of our region's ever-rising international movements of people and material. This demands better efficiency at border crossing, which requires technologies that are user-friendly, reliable in difficult operational conditions, widely deployable – and interoperable between Europe's border authorities.

Not incidentally, the Security Research programme places heavy emphasis on all of these requirements. Indeed, as it enters its final two years the 2007-13 programme's first large-scale Demonstration project (see below) will show Europe's end-user communities how system-of-systems border management capabilities can be seamlessly applied to actual operational needs along Europe's land and littoral frontiers.

UNIONE EUROPEA
Acquisto di quattro Motovedette d'altura
Acquire 4 offshore patrol vessels
...to dall U.E. nell'ambito del Fondo per le Frontiere Esterne
2007-2013
Annuale 2007 – Azione 2.2.7
...ale 2008 – Azione 2.2.4)
GUARDIA COSTIERA

Guardia costiera boat classe 300 © Frontex

PERSEUS

Common awareness for maritime security

The Security Research programme's first system-of-systems Demonstration project, worth more than EUR 40 million, was launched in February 2011. With a tight deadline of 2015, it will demonstrate a common operational picture for EU countries to monitor threats and anomalies around their littoral borders.

Known as PERSEUS ("Protection of European seas and borders through the intelligent use of surveillance"), all aspects of the 54-month project are vast: its size, number of players and technological goals. And given the 90,000 km of coastline and 891 designated sea border crossing points within EU-27, its potential scope of application is vast too.

PERSEUS aims to fuse together surveillance and detection data from a wide diversity of national and regional platforms to produce a useable common picture and distribute it in an affordable and user-friendly way to public end-users involved directly or indirectly in maritime security. It will tie together ground, aerial and sea-based platforms, including maritime patrol aircraft and ships, unmanned aerial vehicles and vehicle-mounted sensor stations.

The project will focus on irregular migration and crime-related activity such as trafficking, smuggling or terrorist acts. Its work will be validated via two live demonstrations involving five specific exercises, with initial emphasis on drug trafficking and irregular migration. The first live demonstration will take place in the western Mediterranean and its Atlantic approaches in 2013, with the second covering the eastern Mediterranean in 2014 – both will integrate data from national maritime control centres in these regions.

Ultimately, PERSEUS has implications for higher policy since its work will directly feed into the EU's wider initiative to manage its common external land and sea borders known as EUROSUR (European external border surveillance system).

Fact File: PERSEUS

- **Total budget**: EUR 43.6 million
- **EU share**: EUR 27.85 million
- **Duration**: 54 months (Feb 2011 – July 2015)
- **Size of consortium**: 28 members
- **Consortium profile**: 13 public-sector players; 15 private ones
- **Project coordinator**: Spain's INDRA
- **Transatlantic aspect**: includes NATO and Boeing's Spanish R&D facilities

The security sector and Europe's economy

Given the diversity of today's natural and man-made threats to highly advanced societies, the security industry is destined to play an increasing role in Europe's economy. DG-ENTR's support for technological innovation in the security industry will protect Europe's citizens, while helping consolidate this newly emerging sector to reinforce economic growth and competitiveness.

The Commission motivates the EU's entrepreneurs and researchers in the sector in a number of ways. The Security Research programme supports systematic R&D networking across Europe's scientific communities to accelerate the exchange of ideas, best practices and interoperable standards. The goal is to avoid duplication of effort and encourage the best technological ideas to come forward.

All research topics – whether technology-based or grounded in socio-economic analysis – are ultimately geared to the future needs of the demand side, i.e. security of end-users. In this way each project brings together those who need innovative capabilities – public authorities – with those who can provide them: Europe's industrial and scientific communities.

DG-ENTR ensures that the programme's door stays wide open to those with new ideas and the ability to innovate quickly such as Europe's independent entrepreneurs and SMEs (small and medium-sized enterprises). Its budgetary support for SME participation in its projects is well above the EU's minimum requirement of 15 percent, for example.

The Security Research programme also has a wider economic dimension by laying the groundwork for the sector's future growth.

According to an independent study carried out for the Commission in December 2009, "Study on the competitiveness of the EU security industry", the value of Europe's security market in 2008 was around EUR 36 billion in the equipment sub-sectors of aviation, maritime and border security, critical infrastructure protection, counter-terrorist intelligence capabilities and first-responder demands. Add in the value of Europe's security personnel services and the sector's turnover rises to an estimated value of EUR 50 billion.

The study also indicated that, while Europe's security sector is a young one and still hampered by a highly fragmented demand side, it has considerable potential for growth.

© rtem/shutterstock

© Tan Kian Khoon/fotolia

Stakeholder dialogue and end-user needs

Civil security embraces the widest diversity of stakeholders, from policy-makers, researchers and technology providers to public end-users and, ultimately, society at large. EU policy requires their guidance to help set objectives and determine how the fruits of civil Security Research will be developed and deployed. Indeed, research policy must continually align itself with the needs of stakeholders to remain relevant and to ensure coherence with European values.

At the level of the European Commission, relevant expertise on Security Research is provided by the Security Advisory Group of public and private sector experts, with a committee of official representatives from the 27 Member States and associated countries overseeing the programme's implementation. The latter are particularly responsible for assisting the Commission in shaping the programme's annual technology goals.

To reinforce research at the operational levels, there must be regular debate, exchanges of ideas and experience and reviews of lessons learned. At the higher policy level, inter-institutional dialogue across Europe about Security Research requires stronger cooperation, coordination and governance.

Conferences and workshops are an effective way to overcome these policy and technological divisions. DG-ENTR increasingly relies on workshops, for example, to test the effectiveness of current research and to sound out stakeholders about future R&D goals and industrial policy initiatives.

Recent workshops sponsored by the Commission have focused on the ethical and society aspects of civil Security Research, air transport security and the capabilities needed to detect and prevent CBRNE threats. Forthcoming workshops will focus on industry standards, technical and other policy issues to promote interoperability and a more coherent marketplace for civil security products and services.

Bridging the dual-use gap

Many Security Research objectives aim for improved capabilities such as detection and surveillance, which lend themselves to both civil security and defence applications. Yet these "dual-use" technologies have traditionally been developed in isolation from one another, leading to wasteful duplication of efforts. In this context, the programme already has a significant track record of cooperation and coordination with the corresponding research actions managed by the *European Defence Agency*, in the context of the so-called "European Framework Cooperation".

Mission 4

Crisis Management & Resiliency

Crisis management is a core responsibility of modern societies. When disaster strikes – whether accidental, natural or man-made – governments must ensure as swift a return to normal life as possible, while limiting damage and restoring calm. As events have shown in recent years, policy and technology should also enable citizens to contribute effectively to recovery efforts.

The operational principles of crisis management are largely independent of the type of incident itself; from a management point of view, all crisis situations operate according to similar processes. This opens the door to interoperable procedures and to so-called dual-use technologies that can be exploited by both civil and military first-responders to cope with security incidents, hostile operating conditions and the provision of aid, or to mitigate the cascading effects of security incidents.

Certain Security Research projects are developing the techniques to detect, identify and contain the dispersal of CBRNE (chemical, biological, radiological, nuclear, explosive) materials or the spreading effects of an industrial accident in order to limit their consequences. Others are studying the best ways to restore basic services such as energy, water or communications and to ensure that society and the economy – whether at local, national or regional levels – can respond and recover quickly, whatever the threat.

Indeed, the multi-dimensional aspect of many crisis situations calls for new technologies that deliver situational awareness to decision-makers, organisations and first-responders simultaneously. This requires new sensors and systems that quickly produce accurate information for command and control centres so that first-responders can effectively handle the situation and restore lost services.

The technical demonstration of integrated and scalable crisis management capabilities for decision-makers, whether inside or beyond Europe, is among the main objectives of the programme.

© De Visu/shutterstock

SECURENV

Evaluating the security aspects of environmental accidents

Environmental security is a growing factor for the EU's development and policy concerns. Our environment is vulnerable to human negligence yet the potential consequences of environment-related threats are becoming more difficult to anticipate, as industrial accidents and natural disasters have repeatedly shown in recent years.

The project known as SECURENV ("Assessment of environmental accidents from a security perspective") aims to generate a better understanding of the complex interplay between environmental disasters and their impact on security.

SECURENV's overall objective is to expand Europe's knowledge base in order to ensure the security of its natural environment. One indication of the importance of this work is that its funding, though relatively modest, is entirely financed by the programme's budget.

The project will analyse major industrial and environmental accidents from a security perspective, using foresight methods and scenario-building techniques that give end-users a better understanding of future environmental risks. Natural phenomena such as fires and floods, industrial accidents such as chemical or biological incidents as well as other threats will be investigated.

SECURENV's work packages entail:

- a review of past environmental incidents and the effects of human actions
- creation of databases with relevant information for end-users
- identification of new and emerging threats to the environment and of the technological challenges that might accompany them
- development of scenarios based on future environmental risks and a foresight methodology to investigate policy options

The project aims to provide insight and advice to security policy-makers, relevant research programme managers and security researchers. As such, SECURENV will help shape the planning and design of future Security Research objectives and actions.

Fact File: SECURENV

- **Total cost**: EUR 851,245
- **EU share:** EUR 851,245
- **Date started**: 01/04/2009
- **Duration:** 24 months
- **Participating nations:** Hungary, Sweden, Germany

>> ***www.securenv.eu***

Mission 5

Interoperability & Interconnectivity

Security end-user organisations face a plethora of technical, operational and human interoperability issues – not only across their own national territory but especially when they have to interact with international counterparts.

Europe alone is a patchwork of languages, laws, diverse cultures and habits that can change abruptly across borders. Even when similar technology is deployed, it is not always compatible across borders. Such differences give rise to vulnerabilities that criminal and terrorist groups can exploit. New forms of criminal financial activity such as money laundering, which have grown to huge proportions in Europe, need a coherent multinational response from public authorities.

Clearly, in an increasingly interconnected world, assets, capabilities and operational procedures must be shared to react quickly to threats and crises to save lives and minimise negative impacts on the economy.

Seamless approach

A coherent and seamless approach to security within and across Europe's borders is therefore essential. Ideally, this should be based on convergence of policies and investment strategies at all levels, though that will take time. Most urgent is to achieve interoperability at the operational level, from equipment to training.

To generate a more cohesive response to threats across the union, Security Research projects are assessing and prioritising those areas where interoperability at the equipment and system levels must be achieved. Innovative technological and training solutions are being developed, for example, to ensure that rescue workers from different nations can work together effectively and exchange information rapidly.

To get there, R&D is focused on boosting security systems' integration, interconnectivity and interoperability. Individual projects in this area cover such topics as standardisation of training curricula, improved communication systems for emergency response crews or hand-held devices for detecting people in collapsed buildings – things that can be deployed across the continent. And as the information is gathered for civil research purposes, guarantees are being built into these systems to protect data confidentiality and the traceability of transactions to ensure respect for privacy.

© Dmitry Yashkin/shutterstock

VIRTUOSO

Boosting border awareness

Just as the PERSEUS project will extend the interoperability of maritime surveillance around Europe's littoral borders, the project VIRTUOSO ("Versatile information toolkit for end-users oriented open sources exploitation") aims to boost border security operational awareness regarding strategic threats and risks in general.

A three-year project launched in May 2010, the keystone to VIRTUOSO's work will be its development of an "open-source information exploitation" toolbox for European authorities working in border security.

This toolbox will extend the security "distance" of Europe's common frontier by allowing border agencies and national authorities to anticipate, identify and respond to strategic threats in a timely manner. What kind of threats are we talking about? They include terrorism, illegal migration, piracy, illicit drug trading and the trafficking of people and counterfeit or stolen goods.

VIRTUOSO's researchers have big ambitions for their information toolbox and see it as the kernel for an eventual pan-European technological platform to collect, analyse and distribute open-source information to border authorities across all 27 EU nations and beyond. The toolbox would also include methods of crisis management response in the event of a "rupture" scenario.

The project places high importance on the involvement of end-users, and its work will evolve incrementally according to their specific requirements. During its lifetime VIRTUOSO will develop three successive versions of its open-source toolbox. The first will demonstrate the toolbox's design and potential for end-users. The second will integrate a limited selection of operational functions, while the third and final version will incorporate all operational functions that end-users need.

Real-time results

In the end VIRTUOSO's toolbox platform will aggregate information from the internet, broadcast media and other sources in real-time and filter it – using text mining and other decision-support technologies – to produce situational awareness and early-warning alerts for end-users. Moreover, the core platform's software will be made freely available to Europe's border security community.

>> http://www.virtuoso.eu/

Mission 6

Security & Society Governance & User Feedback

This cross-cutting mission is especially important. It affects all areas of Security Research and their ethical and societal dimensions because it points to the need to combine security innovation and market growth with Europe's democratic values and freedom of the individual.

How to detect signs of radicalisation in the general population? How to distinguish 'abnormal' behaviour from 'normal' behaviour in public places that might lead to an attack against society? These are difficult and controversial questions whose translation into R&D or operational policy is never easy or obvious for decision-makers.

That is why the Commission turns regularly to advisory and citizens' groups for guidance and the evaluation of research proposals. The research concept of "privacy by design", where security products and services are engineered from the start to protect personal data, is one embodiment of this idea.

Moreover, a sizeable portion of all projects is focused on the ethical, legal and economic aspects of research to identify potential problems as early as possible. One good example is the project known as DETECTER ("Detection technologies, terrorism, ethics and human rights").

DETECTER's express goal is to analyse current security and detection technologies for the risks they may pose to ethics and human rights. "We bring together the technology developers and law enforcement agencies with ethical and legal experts to review these issues," says Tom Sorell, Ethics professor at the University of Birmingham and DETECTER's coordinator.

His project colleague, Martin Scheinin, who teaches international law at the European University Institute in Florence, said DETECTER's main focus is on human rights aspects. 'We look at human rights treaties and their interpretation in practice. We consider what is prohibited by international law and what kind of requirements need to be in place.'

Scheinin and team have now completed a systematic overview of the legal arguments used by international governments when suspending aspects of human rights law in so-called 'emergency' situations. "This requires a three-stage test, with any restriction having a clear legal basis, a legitimate aim and necessity in a democratic society," says Scheinin.

DETECTER's researchers are now applying this test to different generic detection technologies such as body scanners to assess their relative harm from a human rights perspective.

Fact File: DETECTER

- **EU contribution**: EUR 1,869,684
- **Total cost**: EUR 2,424,416
- **Starting date**: 1 December 2008
- **Duration**: 36 months
- **Coordinator**: University of Birmingham, UK

>> www.detecter.bham.ac.uk

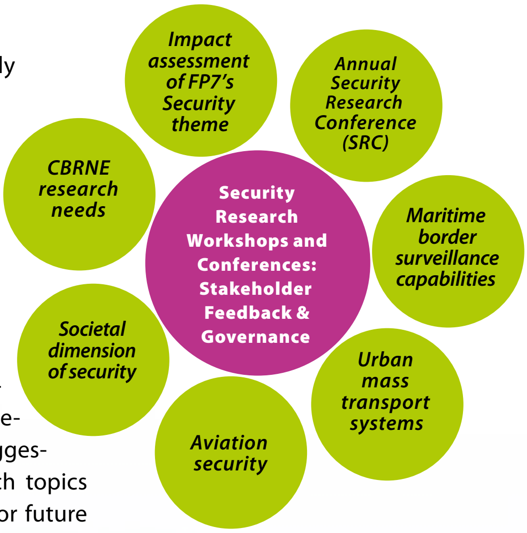
DETECTER

Vetting security technologies for ethics

The Security Research programme continually aligns itself with the needs of policy, operational end-users, industry and – above all – society at large. This is based on regular consultations with policy-makers and societal groups, as well as on the exchange of ideas and lessons learned with Europe's scientific community and technology providers.

Matching the goals of research projects with the needs of end-users is a primary objective in this regard, and workshops are an effective way to do that. DG-ENTR increasingly relies on workshops to stimulate stakeholder dialogue and thus shape not only its R&D goals, but related industrial policy initiatives. DG-ENTR's annual three-day Security Research Conferences (SRC) do the same thing but on a wider scale, for example.

Each workshop deliberately brings together a diversity of stakeholders who normally do not mix with each other such as researchers and end-user authorities in a given domain, industry and civil society groups, policy-makers and NGOs. These dialogue-rich events function as a sounding board for the Commission to review the effectiveness of R&D so far, collect suggestions for new Security Research topics and, crucially, test the waters for future policy initiatives.



Security Research Workshops and Conferences: Stakeholder Feedback & Governance

Impact assessment of FP7's Security theme

Annual Security Research Conference (SRC)

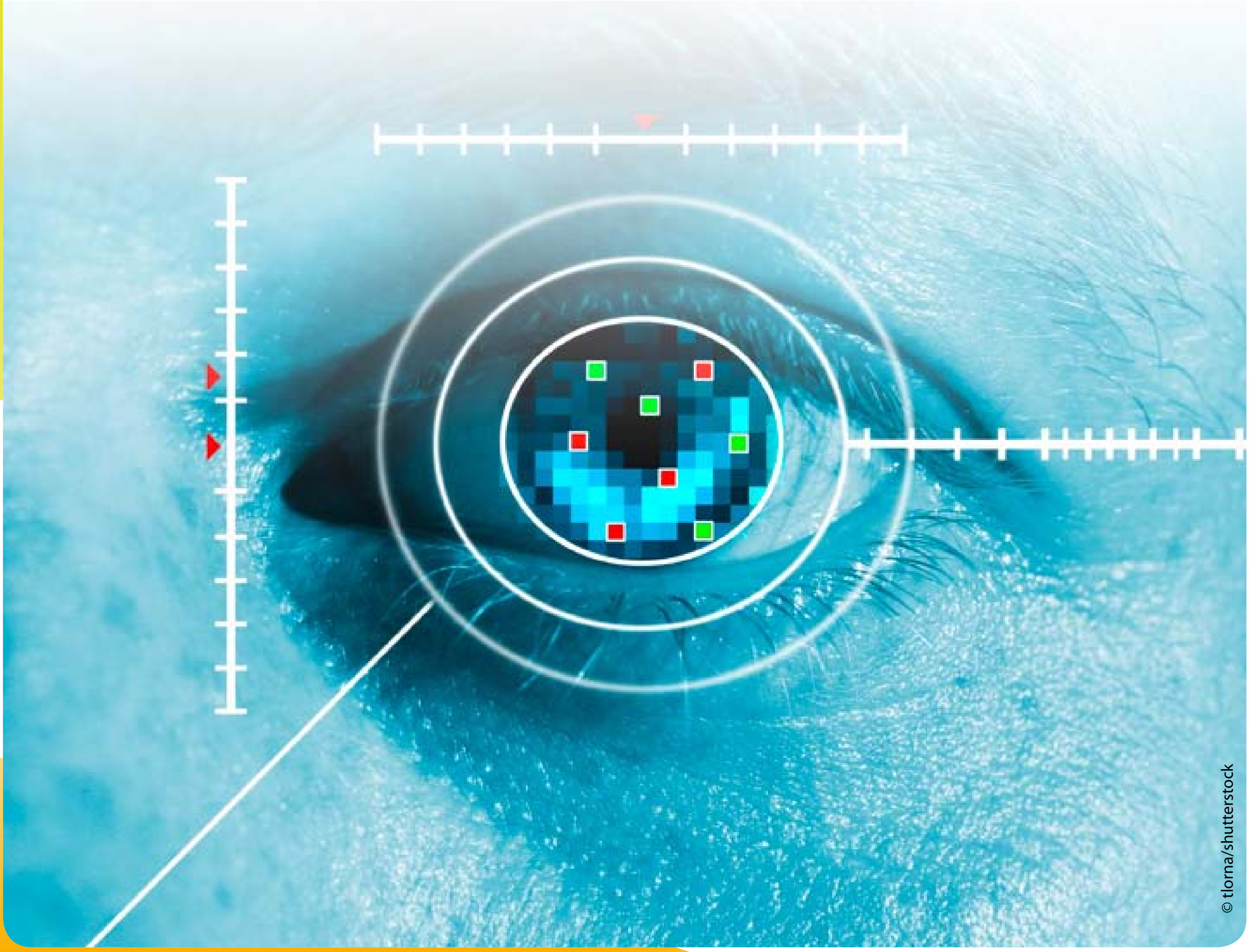
Maritime border surveillance capabilities

Urban mass transport systems

Aviation security

Societal dimension of security

CBRNE research needs



© tloma/shutterstock

Mission 7

Coordination & Structuring

Just as Europe's security market is fragmented, so too is its research community. Though considerable progress has been made in recent years to break down the cross-border barriers to scientific coordination and collaboration, greater effort is still needed.

That is why the Security Research programme sets aside funding for research coordination and structuring activities, as well as for training. Indeed, dedicated training actions in this research domain are still rare in Europe, which needs centres of excellence to facilitate networking, the exchange of ideas and the formation of joint approaches to R&D.

Security Research coordination and structure projects carry out one or more of these activities. Some aim to organise international research between experts regarding specific technical goals. Others strive to foster long-lasting cooperation between regions or countries beyond the lifetime of a given project, while others are using the internet to create permanent reference sites and materials for a given research topic.

These projects can branch out in many directions to include, for example, assessment of supporting facilities such as field laboratories and test centres – and how to make them interoperable across borders. Other structuring and coordination projects aim to develop technological synergies between civil, security and defence research or to better align the demand and supply sides of new technologies.

Forecasting Europe's long-term Security Research needs, or doing risk analysis of emerging technologies to identify relevant civil security applications for the future, are also the aim of such projects. Indeed, the analysis of emerging technologies to identify future applications or research needs is a good example of how two cross-cutting missions can complement each other's work, with one focused on technology research structuring and the other on its ethical implications.

In sum, coordination and structuring projects are laying the long-term foundations for a more coherent approach to civil Security Research at local, regional and pan-European levels.

EUSECON

The cost impacts of security

EU Security Research is not just about the development of technologies and capabilities or their ethical and societal aspects. Often overlooked are the cost aspects of security – whether direct such as budgetary or economic, or indirect ones like avoided costs associated with one security policy or another.

The economics of security is a new and relatively under-analysed field of research in Europe. The EU-funded project known as EUSECON ("A new agenda for European security economics") is helping reverse this trend by studying the cost-benefit calculations of security policies in all their various guises.

Now entering its fourth and final year, EUSECON has generated useful data in several areas such as the economics of CCTV monitoring or CBRNE preparedness, for example. With a total budget of EUR 3 million (of which the EU contributes 80 percent), the project is led by Germany's Institute of Economic Research (DIW) in Berlin.

The project's main output has been an extensive series of working papers. In general, these highlight the gaps in existing knowledge about the cost of terrorism and organised crime across the 27 Member States. They also suggest stronger methodologies for carrying out cost-benefit calculations about EU security polices and counter-measures.

EUSECON's economic analysis flows from its seven work packages, which include:

- a comparison of current investment in CBRNE policies against estimates of the likelihood and potential severity of attacks
- an overview of money-laundering economics due to organised crime in Europe and world wide
- analysis of Europe's security technology market vis-à-vis that of the US market

About 50 papers have been published so far, and nearly 60 will have been issued by the time the project concludes in February 2012, thus providing better economic and budgetary benchmarks for Europe's policy-makers to allocate their resources.

© Andrey Prokhorov/iStockphoto

Industrial policy and the future

Europe's security sector is a highly segmented one. Not only does the supplier base lie splintered across many industrial sub-sectors, but the demand side percolates down through a huge diversity of end-user authorities, from local to European, with very little coordination across borders.

DG-ENTR has identified those areas where action is most needed. These entail efforts to:

- overcome the market's fragmentation
- strengthen the industrial base
- increase harmonisation of equipment and operations
- provide incentives to promote interoperability between the 27 Member States

Creating pan-EU industrial standards in targeted capability areas, for example, would help ensure that the security technologies of regional and national authorities are compatible across Europe's borders. Emergency broadcast networks, border surveillance systems and disaster response equipment are three obvious functions where this is needed.

One way to do this could be to align the technology preferences of end-users via "pre-operational validation" and possibly also "pre-commercial procurement". Here public authorities would act as the launch customer for private-sector innovation over a limited period of time. In return, they would have the right to exploit the supplier's research and test the technologies, after which normal market conditions would prevail. The main idea behind such schemes is that they could collectively build critical mass on the *demand* side across EU-27 while stimulating innovation and economies of scale on the *supply* side of Europe's security sector.

These are just some of many ideas now under consideration, however.

How to support development of cost-saving "dual-use" technologies, where civil-oriented research could give rise to military applications, is a future policy goal, for example. So is the strengthening of regulatory and equipment certification procedures. This includes ways to accelerate the definition of industrial standards for security sub-sectors by Europe's three standards-setting institutions (known as CEN, CENELEC and ETSI).

Speeding up the research-to-market cycle is important, too. One possibility for the future is to create "fast-track" approval of R&D funding by the EU for high-priority technologies and capabilities.

Finally, future Security Research policy must take into account those security technology areas where European industry is dependent on supplies from non-EU regions — be it due to restrictive intellectual property rights or technology transfer barriers arising from classified export restrictions. These need to be identified so that alternative technology solutions can be developed and so that EU-produced security equipment can be used, sold or deployed worldwide to Europe's advantage without hindrance.

© Konstantin Sutyagin/fotolia

For additional information, please get in touch with:

European Commission: Directorate-General for Enterprise and Industry

General website:

- ***http://ec.europa.eu/enterprise/policies/security/***

Security R&D programme:

- ***http://cordis.europa.eu/fp7/security/***

European Commission

Security Research
Protecting Europe's homeland and its future

2011 – 20pp. – 29.7X21 cm
ISBN 978-92-79-20949-9
doi:10.2769/29014

NB-32-11-838-EN-C

Publications Office

ISBN 978-92-79-20949-9

9 789279 209499