Emerging Technologies in the Context of "Security" *

Overview

On 12 December 2003, the European Council adopted a European security strategy, entitled "A Secure Europe in a Better World." This document provides the framework for concerted European activity in the field of security and, more specifically, in activities to anticipate and cope more effectively and efficiently with new security threats such as terrorism, proliferation of weapons of mass destruction, failed states, regional conflicts, and organized crime.

The need to undertake effective action in the area of security was emphasized by a series of recent terrorist events, such as the bombings in Madrid and London, or by natural disasters, such as the tsunami in Asia in 2004. The European research community responded to this need. In March 2004, the European Commission launched its Preparatory Action on Security Research (PASR), and the Group of Personalities advocated in its report "Research for a Secure Europe" the creation of a European Security Research Program (ESRP).

Of particular relevance for the preparation of the content of this ESRP are the so-called road-mapping activities that the European Commission has contracted under the first phase of PASR. These activities—known as SeNTRE and ESSRT—will undertake a comprehensive strategic analysis of where research activities should be focused, and where they could have the greatest impact.

Socioeconomic Challenges

Definition of Security

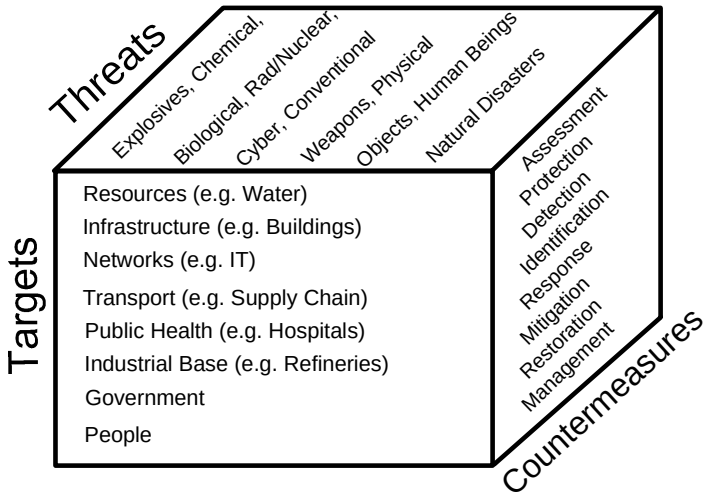
Commission Communication COM(2004) 72 defines security to be "an evolving concept" that "represents many challenges to the EU-25 that impact on a wide range of existing and emerging EU policies [and] citizens' concerns, including the protection against terrorist threats, and the adaptation of governance structures to effectively deal with these matters." Since this definition is rather vague, and tends to limit the focus of "security" to matters of terrorism and anti-terrorism, for the purposes of this report we propose a definition that broadens this scope to also include organized criminal activity—such as illicit trafficking, illegal immigration, smuggling, etc.—as well as the need for enhanced capabilities to cope with natural threats such as floods, forest fires, etc.

The CEN BT/WG 161 on Protection and Security of the Citizen, from the European Committee for Standardization, adopted the following definition in January 2005:

> Security is the condition (perceived or confirmed) of an individual, a community, an organization, a societal institution, a state, and their assets (such as goods, infra-

* This report was issued by the Institute for the Protection and Security of the Citizen, Sensors, Radar Technologies, and Cybersecurity Unit of the European Union (Head of Unit: Alois J. Sieber).

structure), to be protected against danger or threats such as criminal activity, terrorism, or other deliberate or hostile acts, disasters (natural and man-made).



Model for Security

The underlying structure to this definition is illustrated in the security model below, which was introduced by the ISO Advisory Group on Security in 2004 (ISO/TMB AGS N 46, dated 2005-01-06) and adopted by the CEN BT/WG 161. The model provides a framework to classify aspects of security in three dimensions: targets, threats, and countermeasures.

Targets are the entities, including people, things, and processes, that are vulnerable to threats and that need to be secured. Targets can be classified into several categories, as displayed in the diagram of this security model above:

- Resources include the quality of water, soil, and air, as well as natural energy resources and the food supply chain, including plants and animals.
- Infrastructures address buildings and structures of all types, including water reservoirs, and cover distributed networks such as water supply systems and energy distribution networks (e.g. gas and oil pipelines). It also includes a nation's finance system.
- Information, computers, and communication include computer information systems, information-sharing systems and communication networks, and public (broadcasting) as well as emergency communications. It also covers the postal services.
- Transportation covers air, land, and sea transportation networks and vehicles. It also considers the transport supply chain, including container transport.

- Public health/safety includes all aspects of the public health care system and the emergency services (e.g., fire brigades, ambulance, police).
- The industrial base considers refineries, power plants, gas tanks, chemical plants, etc., as well as any structure that produces potentially hazardous material. It pays specific attention to nuclear processing facilities and the defense supply chain.
- Government (all levels) addresses command and control functions, intelligence/ information services, and continuity of operations.
- The category of people include all individuals, including their properties but also their rights, ethics, etc.

Threats are the means by which targets may be subjected to attack and harmed. Threats can be classified into several categories, as identified in the model above:

- Explosives
- Chemical agents
- Biological agents
- Radiological/nuclear material
- Cyber threats include computer viruses, denial of service attacks, hacking, spoofing, identity theft, etc.
- Conventional weapons covers, among others, handguns, knives, etc.
- Ordinary physical objects used for attacks cover the use of an object or a vehicle, such as a plane or a truck, as a weapon (as in the attacks on the World Trade Center and Pentagon)
- Human beings include terrorist groups, criminals, etc.
- Natural disasters cover earthquakes, fires, floods, storms, etc.

Countermeasures are the systems, methods, and tools used to prevent or respond to threats against targets. Countermeasures can be classified into several categories, as shown in the diagram of the security model:

- Assessment
- Protection
- Detection
- Identification
- Response
- Mitigation
- Restoration
- Management.

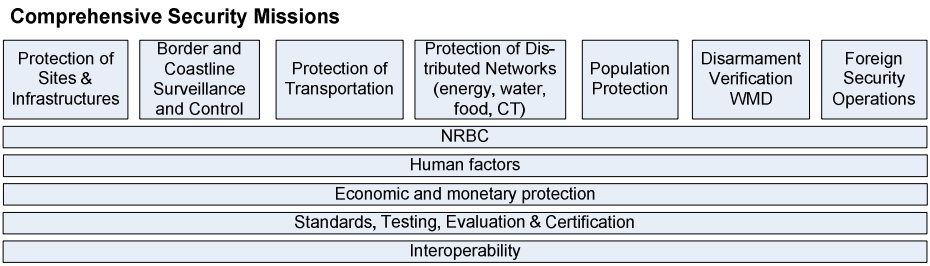
Standards for Security

Both ISO/TMB AGS N 46 and CEN BT/WG 161 launched systematic inventories of the capability needs of security stakeholders, with the goal of identifying their usage of security standards and the concerns they face in the area of security. The inventory is an ongoing process, and must be regularly updated. However, a tendency is reflected in the table below:

Large field	Details	Remarks
CBRN	Prevention and containment: "pre-during-post" comprehensive approach, including de-contamination process of both people and sites; Code of good practice for first responders; Exposure criteria for civil population regarding CBRN agents	
Emergency services	Emergency equipment, emergency procedures; post-trauma services and training (including psycho trauma)	
Transport security	Intl labeling for known shippers, competence assessment for safety officers, seal/locks and similar	
Authentication/ identification	Pre-emptive protection, fight against identity theft; container identification for security; digital signature for legally binding documents and data exchange	
Information and communication	Information Security Management Systems (ISMS), interoperability of communications in civil protection operations	ISMS is being addressed in ISO/ JTC1/ SC27
Physical security and securiy services	Private manned security services. Risk assessment of ordinary weapons	Activity in CEN/BTTF 167 Secuirty services
Security of infrastructures	e.g. Security of pipelines for dangerous goods; identification of critical points in premises and plants. Computer-aided risk assessment	
Safety information to general public	"pre-during-post" comprehensive approach to ensure clear and concise messages	Lower priority
Public procurement	"Best buy" specification, interoperability	Lower priority

Missions for Security

Building on the identification of targets, threats, and countermeasures, a comprehensive approach can be developed that identifies the security and security-related activities, missions, and competencies necessary to cope with the protection, maintenance, and management of what is perceived to be a secure environment. This approach consists of seven vertical and five horizontal missions, as identified on the next figure.



The protection of *sites and infrastructures* covers the protection of public infrastructure, government buildings, public utilities, harbors, airports, and railway stations; it will also address the protection of hazardous sites such as chemical factories, nuclear power plants, etc.

The surveillance and control of *borders and coastline* includes the surveillance and control of a nation's blue and green borders, as well as the surveillance of its airspace. It will consider issues such as illicit trafficking in arms, people, and narcotics; illegal immigration; counterfeiting; etc.

The protection of *transportation* addresses the protection of land, sea, and air vehicles as well as their supporting infrastructures. This category also considers environmental pollution as well. Transportation vehicles will be considered as possible targets, but also in their role as possible weapons.

The protection of *distributed networks* covers networks that are spread over large geographical areas, such as energy supply networks (oil, gas, electricity) and the food and water supply chains. It also includes the protection of information and communication networks as well as their data.

The protection of the *population* is concerned with people, whether as individuals or in groups. This topic covers a wide variety of aspects, ranging from specific vulnerabilities to human behavior in crisis situations. Particular attention will be paid to those people that have a crucial role in the prevention and/or management of incidents, crises, or disasters, such as emergency forces, first responders, and law enforcement personnel.

The mission relating to *disarmament verification/weapons of mass destruction* will consider the capabilities needed for marking and tracing materials from dismantled nuclear, chemical, and biological weapons, and will also include enhanced surveillance of storage sites.

The area of *foreign security operations* will cover the civilian aspects of humanitarian operations, civilian crisis management support for crises in areas outside the EU, and evacuation operations.

The five horizontal missions are relevant for all seven vertical missions. They need to be addressed systematically under each of the seven vertical missions, since they concern specific aspects of the capabilities needed to carry out each of the vertical missions in a comprehensive manner. These horizontal missions are:

- NRBC (prevention, detection, protection, and decontamination)

- Human factors
- Economic and monetary protection
- Standards, testing, evaluation, and certification
- Interoperability.

SWOTS Analysis

Strengths

The European industrial and research community has excellent skills to support and further develop their contribution to addressing the day-to-day security problems facing Europe. These competencies include, for example, the development and production of world-class sensors of all types, and the creation of state-of-the-art network enabling capabilities (NEC).

This section will give an overview of where these capabilities stand today, or to what point they would need to be developed in order to meet the security needs of the EU. In order to structure this overview, this section will give an indication of useful support measures for each of the security missions and sub-missions identified in the previous section, describing the required support technologies or tools and giving examples of useful integration/validation. The value of simulation and training tools will be illustrated through the use of a few examples.

Protection of Sites

Support measures

- Mapping of critical sites, including the assessment of the environment, the current situation, and the potential risks
- Systems architecture, including backup procedures and solutions in case of disaster (emergency action plan).

Support technologies or tools

- Micro technologies for sensors (surveillance, NRBC detection and tracing, etc.)
- Advanced low-cost, smart, embedded smart sensors and novel techniques for covert surveillance
- Smart cameras
- Unattended sensors and automated tracking mechanisms
- Distributed “networks” of sensors on the ground, in the air, or in space
- Network security and data integrity between distributed sensors
- Secured wireless broadband data links for secured distributed computing
- Secured (but interoperable) communications, including video conferencing, mobile phone services, and wireless networks

- Personal information and communications systems (i.e., ability to receive video on a PDA)
- Protection of networks against environmental threats or attacks (including directed energy weapons)
- Pattern recognition capabilities, to allow for extraction of information from poor quality images
- Non-cooperative access control
- Check points, using signatures, image recognition systems, X-ray devices, and biometric scanning, all linked to relevant databases
- Detection and localization of civil partners
- Lightweight materials for protection of human and infrastructure targets.

Simulation and preparedness

- Predictions of the vulnerability of structures after explosions and other events; development of structural solutions
- Networking of existing sensors (forest of sensors)
- Secured wireless broadband data links (for forest of sensors)
- Data fusion
- Interoperability
- Personal mobile SIC with augmented reality
- Sensors simulation
- Survivability of components and equipment
- Advanced human behavior modeling and simulation, including: prediction of mass behavior; simulations for decision-making
- Video-tag-biometric cooperation.

Integration/validation

- Advanced video surveillance demonstrator (detection, tracking, reconnaissance, identification with fixed and mobile cameras)
- Global simulation tool to facilitate choices, assist in the design of procedures, and assess the performance of different options
- Simulator for training in methods and tools (to improve decision making before and during operations)
- Sensor/data processing and fusion demonstrator (to get a picture of the global threat environment from sources as diverse as satellite data to micro-UAVs and sniffers at border checkpoints) for surveillance, detection, and verification.

Protection of Public Infrastructures

Support measures

- Mapping of important European civil facilities, including transit and train stations, sport stadiums, banks, government buildings, and hospitals
- Risk and threat assessments, including analysis of priority versus affordability.

Support technologies or tools

- Surveillance and recognition systems
- New materials
- NRBC detection and protection, particularly air quality monitoring
- Low-cost chemical agent sensors
- Biological agent sensors
- Population warning systems
- Evacuation and consequence management plans.

Protection of Public Utilities

Support measures

- Mapping of European infrastructures for food, water, agriculture, energy (electrical, gas and oil, hydroelectric), and telecommunication installations, and related risk and threat assessments.

Support technologies or tools

- Simulations
- Protection of water supply (pollution, chemical, and biological threat detection)
- Testing for contamination of agriculture (watersheds, rivers, soil, etc.), including monitoring for crop and animal viruses
- Food testing and control
- Protection of energy plants and telecommunication networks, including surveillance and backup energy systems
- Biological and chemical agent sensors for confined public spaces
- Lightweight materials for protection of human targets.

Integration/validation

- Small unmanned aircraft demonstrator with miniaturized biological/chemical or surveillance sensors
- Portable C2 modules with augmented reality.

Protection of Hazardous Sites

Support measures

- Build and maintain a comprehensive assessment of European infrastructures with catastrophic potential (nuclear power plants, chemical facilities, pipelines, ports, etc.).

Support technologies or tools

- Biological/chemical long-range sensors
- EM protection
- Simulations
- Impact analysis and reduction plans
- Population warning systems
- Evacuation and consequence management plans
- Decontamination techniques, first-aid and protection kits
- Survivability of components and equipment
- Predictions of structure vulnerability after explosions, and development of structural solutions
- Protection and survivability of systems against directed energy weapons.

Integration/validation

- Electronic noise
- MAV demonstrator for surveillance
- Self-protected, blast-resistant containers, with chemical sensors.

Protection of Harbor Sites

Support measures

- Specialized studies for the utilization of defense technologies
- Protection of off-shore energy installations
- Development of a "secure harbor" concept (feasibility study, state-of-the-art assessment, scenario analysis, system definition).

Support technologies or tools

- Wide-scale multi-sensor surveillance: radar systems; optical detectors; night vision; satellites
- Defense technology input for:
  - Diver protection systems
  - Acoustic surveillance systems
  - IR/optical surveillance
  - Underwater unmanned vehicles (UUVs)
  - Smart naval shelters (lightweight, blast-resistant structures).

Protection of Airports

Support measures

- Specialized studies for utilization of defense technologies

Support technologies or tools

- Wide-scale use of multi-sensor surveillance, supported by satellite systems
- Secure communication systems
- "Tunnel of truth" (trusted traveler in correlation with verified luggage, etc.)
- Secure interoperability with visa databases and other tools necessary for providing support to integrated border management efforts.

Integration/validation

- Smart container methodologies
- Integrated controlled doors
- Hardening of cockpits against electronic noise
- Micro-UAV demonstrator for surveillance.

Integrated Border Management

Support measures

- Real-time border surveillance, command, and control (including intelligence)
- Access control—managing entry and exit to the "Schengen zone."

Support technologies or tools

- Observation and detection systems, including attended and unattended sensors (early warning, ground, balloons, land radar, video surveillance, sniffers, quiet sensors)
- Optronic sensors: short and long range, surface and airborne, night vision
- Remote detection through sensors
- Microsystems and nanotechnologies
- Small disposable auto-configuring network of sensors
- Distributed "forest of sensors"— on the ground, in the air, or in space
- New materials for use in sensors, able to react to variations in the environment
- Electromagnetic defenses, seismic sensors, and infrared watchers
- Communication systems
- Secured (but interoperable) mobile phone, wireless, and broadband networks (video, multi-sensor input)
- Distributed network with encryption, very fast spectrum scanning and analysis (data, voice), GSM monitoring
- Identification, including biometric data, rapid detection of forged credentials and travel documents
- Access control systems

- Cooperative and non-cooperative automatic pre-authorization systems (clearance levels, fast-track approval), abstracting salient points from raw data
- Detection at checkpoints (signatures, image, X-rays, biometric information), linked to databases
- Information exchanges and interoperable databases to achieve a global assessment.

Integration/validation

- Border surveillance demonstrator, including at least one checkpoint
- Micro UAV demonstrator for border control.

Illegal immigration control

Support technologies or tools

- Border statistical surveillance (identification of routes)
- Unattended sensors
- Inter-connected and integrated visa/immigration facilities control systems
- Biometric data collection
- Permanent and temporary systems for facial recognition, thermal cartography, digital fingerprints, iris/retina scans, hand shape, ear shape
- Behavior: voice, handwriting, signature
- False reject ratio, and false acceptance ratio, decision level.

Integration/validation

- Checkpoint demonstrator
- Optical or biometric verification, with reconnaissance sensor systems.

Coast and Border Protection

Support measures

- Definition of affordable system to perform coastline surveillance missions (including monitoring vessel traffic at sea, search and rescue operations, providing assistance to ships, pollution, fire-fighting, interdiction of illegal immigrants and drug smuggling, halting terrorist landings and attacks in crisis and wartime) in a dedicated region (including high-value target harbors)
- Feasibility and trade-off studies (effectiveness, detection rate, adaptability, modularity).

Support technologies or tools

- Radar systems for surface and airborne threats: airborne imaging radar (SAR and ISAR), mobile/transportable coastal radars
- Networking surveillance assets (static and dynamic sites)

- Image data processing, broadband, data fusion
- Sensors, both active and passive
- Integration of equipment
- Autonomy
- Robust flight control systems
- Certification of systems (UAVs' inclusion in civil air traffic management).

Integration/validation

- Advanced coastline surveillance feasibility demonstrator, using various means (UAVs, maritime patrol aircraft, helicopters, satcomms, ground stations).

Illicit Trafficking (Drugs, Weapons, Ammunition, Explosives)

Support measures

- Tagging and tracing methodologies.

Support technologies or tools

- NRBC detectors at checkpoints
- Chip-based detectors
- Identification and tracing of intermediary products
- Chemical sensors
- Compact sensors with tuneable laser diodes for detecting mixtures of explosives
- Smart labels
- Durable marking
- Secret marking.

Integration/validation

- Worldwide network/database availability (standardized, legal, politically acceptable).

Protection of Distribution and Supply Networks

Support measures

- IEM risk assessment for telecommunications networks.

Support technologies or tools

- IEM protection
- Oil/gas network surveillance
- Inside Europe: miniaturized sensors, data collection and processing
- Outside Europe: airborne and space-based surveillance and observation, including UAVs and radar

- Water distribution
- Dam surveillance
- Monitoring devices, from satellites to micro sensors in water supply
- Protection of water supply (detection of biological and other unusual threats)
- Air/water cleaning and filtering systems.

Integration/validation

- EM low-cost hardened communication civil networks.

Information and Information Systems Protection

Support measures

- Intelligence gathering
- Adaptive and passive algorithms for data/image/signal processing.

Support technologies or tools

- Effective defensive and offensive EW/IW techniques, measures, and countermeasures
- Cyber security, including cyber deterrence
- Cryptology and key management
- Attack prevention and identification
- Web intelligence (large-scale data mining)
- Early detection (based on small numbers of events)
- Non-cooperative IFF techniques
- Database protection and contextual search
- Network and protocol-independent secured communications
- Secured robust multi-mode communication systems
- Mobile re-configurable communications
- Broadband access to mobile users in dynamic situations or electro-magnetically difficult scenarios
- Precise location of standard communication systems for non-cooperative users
- Non-cooperative penetration of suspect e-systems
- Jamming and anti-jamming technologies
- Small form factor display systems.

Integration/validation

- Information warfare demonstrator
- EM Hardened C3 demonstrator.

Protection of Land Transportation

Support measures

- Mapping of critical zones in rail and road infrastructure (highway connections, bridges, tunnels, etc.) and related risk and threat assessment.

Support technologies or tools

- Positioning/tracking applications (e.g., Galileo)
- Fleet management
- Mobile resources integrated management
- Containers
- Positioning and tracking
- Self-protected (blast resistant) containers, with chip-based sensors
- Protection and survivability of systems against directed energy weapons
- Security at terminals, warehouses, and distribution centers for critical goods (wireless video surveillance and optical surveillance)
- Protection of automated systems, information technology, and documentation procedures for operational command and control centers
- Protection of rail and road infrastructure, including rail cars; detection of missing parts.

Integration/validation

- Fleet management demonstrator
- Smart container demonstrator.

Protection of Sea Transportation

Support technologies or tools

- Navigation and tracking (even of non-cooperative entities, by data collection)
- Regular surveys of critical sea/coastal areas (both space-based and airborne) to allow for elimination of false signals in times of crisis
- Mine detection
- Anti-hijacking protection
- Pollution modeling and simulations (specific toxins/chemicals, NRBC)
- Pollution disaster prevention and management equipment
- Self-protected containers (blast resistant), with chip-based chemical sensors
- Predictions of structural vulnerability after explosions, and identification of structural solutions
- Protection against harsh EM environments

- Protection and survivability of systems against directed energy weapons.

Integration/validation

- Naval container demonstrator.

Underwater Threats (including mines)

Support measures

- Transferable from underwater warfare technologies.

Support technologies or tools

- Remote mine sensing (aerial detection)
- EM solutions
- Optronic solutions with lasers
- Diver delivery vehicle
- Bottom crawlers
- Underwater diver-detection sonars
- New low-cost sensor technologies for underwater magnetic detection, and acoustic arrays for passive threat detection
- Development of new transducer technologies for active threat detection
- Innovative signal processing for the detection of small objects in high reverberating environments
- Innovative classification and data fusion processes for the acoustic/magnetic detected threats, based on a new artificial intelligence methodology
- Advanced low-energy radar with high resolution for interception of small moving targets in clutter, featuring low transmitted peak power, in order to not be hazardous for people
- IR active imager with eye-safe capability and modular integration of the EO sensor independently from the site morphology.

Protection of Air Transportation

Support technologies or tools

- Lightweight materials for aircraft protection (light armor plates, etc.)
- Protection of SIC against harsh environment
- Broadband communication
- Electronic noise detector.

Simulation

- Sensors simulation
- Survivability of components and equipment

- Predictions of vulnerability of aircraft structures after explosions, and identification of structural solutions
- Protection and survivability of systems against directed energy weapons.

Integration/validation

- Biological and chemical detection systems for airports
- Fuselage with NG structure, explosion resistant (after vulnerability prediction and protection against explosions)—applicable also to helicopters used in evacuation or humanitarian operations
- Self-protected aircraft containers
- Demonstrators of containers' (with chips) surveillance systems
- Civil aircraft protection from terrorists threats, such as Manpads or laser blinding; use of decoys and infrared and other countermeasures
- Hardened canopies and glass walls (against lasers, HPM).

Protection Against Less-Than-Lethal Weapons (adapted for the aircraft environment)

Support information

- Risk assessment of effects of LTLW in closed spaces
- Possibility and risk of depressurization situation.

Support technologies or tools

- Marking devices
- Miniaturization
- MFP stopping barriers
- Dazzling laser flashlights
- Painful lasers
- High-power directed acoustics
- Long-term LTLW effects
- Aircraft "save" technologies
- Simulation
- Secure communication with ground
- Mini robots.

Integration/validation

- Training for crew and cabin personnel, and user education.

Protection of Legal Transportation of Hazardous or Critical Goods

Support information

- Marking and tracing methodologies and case studies.

Support technologies or tools

- Secured containers
- Integrated positioning/localization/data transmission kits
- Detectors on containers
- Secret marking
- Packaging standardization
- Lightweight materials for protection against explosion and chemical attack
- Tracing liability.

Integration/validation

- Worldwide network/database availability (standardized, legal, politically acceptable)
- Electronic noise detector demonstrator
- Secured container demonstrator.

Protection of Population

Support measures

- Risk assessment in public and urban areas.

Support technology or tools

- Training and simulations (virtual or augmented reality)
- Modeling
- Real-time data collection
- Studies of risk phenomena (propagation, effects)
- Population behavior
- Individual behavior and responses to threats (effective/physical and perceived)
- Protection against viruses, biological agents, and radioactivity
- Vaccines and immunology studies
- Specialized materials, composite materials, and air intake filters
- Low-cost biological and chemical sensors and alarm systems
- Perception of security (sociological aspects)
- Surveillance and recognition in urban environments
- Population warning systems.

Integration/validation

- Interoperable crisis command, control, and communications (C3) demonstrator ("security lab"), for scenarios elaboration and emergency forces training

- Personal mobile information and communications system with augmented reality.

Law Enforcement

Support information

- Technical-operational risk assessment of unauthorized use of firearms or LTLW in law enforcement operations
- Assessment of progressive responses in proportion to the threat
- Crowd control: preparation; initial phase (stopping vehicles); transition phase (identification of group leaders); negotiation (marking of leaders); crisis (extraction of leaders); use of corrective means; specific C3 solutions.

Support technologies/tools

- Biometric data
- Micro pyrotechnics
- Microsystems
- Physiological effects.

Integration/validation

- Architectural concepts
- Tactical-operational efficiency
- Legal/liability training simulation.

Protection of Emergency and Other Services

Support measures

- Case studies.

Support technologies or tools

- Training/simulations (virtual or augmented reality)
- Combined operations with robots, UAVs, etc.
- Visualizations/localization/maps/access to databases on mobile terminals
- Secured communications
- Logistics: optimized interventions
- Physical protection of personnel (e.g., miniaturized detectors)
- Decontamination techniques
- Knowledge management methodologies, to store and index the experience gained for further improvements
- Updating of models
- Compatibility of law enforcement equipment with that of first responders
- Damage assessment

- Automatic mapping.

Integration/validation

- Crisis management simulator.

Security Policy—Global Risk Assessment

Support measures

- Analysis of available data (constraints, limitations, access)
- Models and methodologies for proactive evaluation, risk assessment, and early warning to prevent acts of terrorism and monitor global stability.

Support technologies or tools

- Evaluation and risk assessment models and databases
- Grid computing
- Advanced heterogeneous data mining/browsing for sensitive information
- Multivariable analysis
- Actionable intelligence for preventing acts of terrorism
- Behavior analysis for safety and security
- Methods for handling uncertain situations and optimizing responses
- Study of belief systems
- Risk assessment for potential terrorism targets
- Cultural databases
- Universal translators.

Integration/validation

- Specialized open source browser ("Security Google").

Humanitarian Aid (Petersberg Tasks)

Support measures

- Definition of a European crisis analysis and management capability.

Support technologies or tools

- For all missions:
  - Observation, monitoring, and supervision, through space-based, airborne, human intelligence, and other methods
  - Data acquisition, collection, and processing (data mining, data fusion, modeling)
  - Secured communications/positioning (anti-jamming, space-based communications)

  - Advanced "security" C4ISR, including mobile and deployable modes (possible article 169)
  - Logistics support: advanced tools, including simulations and training
- Humanitarian and evacuation operations:
  - Logistics and protection for transport/medical helicopters
  - Mobile medical facilities, including telemedicine.

Integration/validation

- Crisis management platform demonstrator, including logistics, C3, planning, etc. (deployable)
- Fuselage with new generation composite structure, explosion resistant (after vulnerability prediction and study of protection against explosions); also applicable to helicopters for evacuation or humanitarian operations
- High-performance, low-cost targeting for helicopters (for evacuation operations)
- Low-cost reliable land-mine detection system.

Counter-proliferation: Armament/Disarmament Verification

Support measures

- Ballistic threat assessment and forecast.

Support technologies or tools

- Databases and intelligence
- Identification of movements and purchases of unique/traceable components
- Chips on critical containers
- Detection mechanisms at sensitive sites and along sensitive routes
- Chip-based detectors
- Verification kits, including remote access to databases
- Support to nuclear waste storage sites, power plants, and nuclear submarine "cleaning" efforts (e.g., with Russia and Ukraine)
- Environmental monitoring
- Status monitoring
- Illicit trafficking:
  - Border surveillance control, including surveillance of critical routes, by airborne and space-based devices, cameras, etc.
  - Low-cost detectors—marking and tracing of arms and ammunition.

Integration/validation

- Demonstrators of containers (with chips) and surveillance systems (marking and tracing).

Crisis Management Systems (including mobile deployable HQ)

Support measures

- Available data sources and links in the EU
- Candidate architectures.

Support technologies or tools

- Rapid deployment, mobility, and sustainability
- Multimedia/multi-source integration on video wall
- Interaction
- Immersion
- Hyper-realistic rendering
- Multi-user architecture: data management and configuration
- Scenario preparation: artificial intelligence, imaginary system simulation
- Results analysis: knowledge management, visual display
- Multi-modal interfaces: vocal, mobile PC, wireless, PDA
- Data fusion ("data on demand")
- Grid computing/real-time access
- Data mining (clustering, automatic notification, real-time analysis)
- Human factors (e.g., stress) in the decision-making process
- Behavior under stress (especially in mobile environments)
- EM hardening for deployable systems.

Integration/validation

- Crisis analysis center simulator/training/logistics (security lab)
- Mobile deployable HQ.

NRBC Detection, Protection, and Decontamination

Support measures

- Modeling for threat evaluation and impact assessment
- Equipment assistance definition.

Support technologies or tools

- Detection
- Remote and local warning systems, including miniaturized detectors
- Wide-scale surveillance and identification devices (hyperspectral imager, IR 8-12μ, laser induced fluorescence, neutron, etc.)
- Terahertz laser sensors for biological agent detection

- Nuclear detector based on deployable sensors for: close-up detection of gamma-ray dose rate and gamma radio nucleids; radioactive contamination monitoring
- Protection of the population:
  - NRBC filters and air lock systems
  - Specialized composite materials
  - Individual protection against viruses, biological agents, and radioactivity
  - Vaccines, antidotes, and immunology studies
  - Decontamination techniques
  - Specialized showers
  - New active materials and coatings.

Integration/validation

- Integrated NRBC detection/protection system for public facilities (airports, railway stations).

System Integrated Operations ("Network Centric Ops")

Support information

- Assessment of the existing civil and military systems in the EU
- Interoperability of civil/security communications systems
- System architecture study based on mission requirements ("system of systems").

Support technology/tools

- Increased situation awareness and decision-support aids:
  - Smart and mobile sensor networks
  - Secure and reliable communications to and from platforms (spectrum control, communication interception), including reinforcement of communications in a local area, and resistant systems for use in harsh environments
  - Data and information fusion techniques
  - "Data on demand"—grid computing/real-time access
  - Distributed information processing
- Interoperability of components, including secured communications
- Integrated modular systems (integratable, interoperable, adaptable, scalable)
- Call centers.

Integration/validation

- Demonstrator for a common information infrastructure architecture
- Mobile information and communication system with augmented reality on a PDA
- Network of personal mobile computers and CIS.

Weaknesses

Need to Further Develop Specialized Technological Competencies

The recent terrorist events and large-scale disasters show that, despite the very high level of European in-house science, research, and technology competencies, they are not sufficient to adequately and efficiently prevent these horrible events from happening, nor to protect human beings and their property against the catastrophic effects of such events. In order to enhance skill levels and overall capability to respond more adequately, significant progress needs to be made in further developing the individual and combined technologies identified in the previous section of this essay.

Need for an Integrated Approach

Modern security missions and civilian crisis management efforts require concepts that are:

- Responsive and adaptable, so that they can respond to changing circumstances within the operational situation and so that they can be adapted and redirected based on the learning experience in the field
- Solid and robust, so that they remain effective throughout the operation
- Interoperable, so that they can operate across all levels in integrated operations involving all relevant national and international services
- Broad, so that they are able to operate across a wide range of situations.

In order to achieve this, it is necessary at all times to have a full overview of what is happening in the field. Therefore, capabilities need to be developed with a strong focus on:

- Full information availability, providing the user access to information at all times and enabling the user to search and exchange information that has been collected by all sources internal and external to the field of operations
- Situation awareness, providing a shared understanding and interpretation of a situation, the mission planning, the potential sources of action, etc.
- Flexible and modular systems, enabling assets to rapidly reconfigure to meet changing mission needs
- Integrated network support, allowing the use and integration of public service capabilities, NGOs, industry (and, when necessary, military services) to support operations.

The European Union today has twenty-five member states. Each of these states has different systems in place, with different protocols and different decision procedures, different equipment, etc. Moreover, security is a multi-service activity, involving stakeholders from a variety of domains. For example, border control and management efforts involve border guards, law enforcement, customs, illegal immigration officers, and a number of other agencies. For such a fragmented and heterogeneous environment, a doctrinaire, one-size-fits-all integrated concept may not be the best approach. It

is suggested instead to follow and develop the concept of network enabling capabilities (NEC), which are more concerned with evolving capabilities by bringing together decision-makers, sensors and other systems, and enabling them to pool their information by "networking" in order to achieve an enhanced capability. In NEC, the key word is *interoperability*.

An integrated approach requires interoperability at technical, data, and human levels. Technical interoperability concerns the technical aspects related to the interconnection of different systems and equipment, so that information exchange between these different systems and equipment becomes technically possible. Interoperability of data deals with the incompatibility of data and datasets and looks at the process of data-mining and data fusion, with the objective to ensure that the right information reaches the right person in the right location at the right time, so that this person can make the right decision and/or undertake the right action (known as "seamless sharing of information").

However, the greatest challenges of interoperability are at the human operational level. Problems need to be overcome that mainly result from multi-agency, multi-service, and multicultural communication and collaboration. Some key areas are:

- Different cognitive processes and behaviors
- Different ways of capturing, sharing, and re-using knowledge (learning from experience)
- Different organizational structures and decision processes
- Different understanding of impacts and costs
- Differences in team situation awareness and shared situation awareness
- Different reporting procedures
- Need for cross-agency standardization and protocols.

Need for a Multi-modal Approach

One additional step in the process toward full integration is the so-called process of converging technologies. This process combines and builds on the synergies and cross-fertilization of four different technology areas:

- Nanoscience and nanotechnology
- Biotechnology and biomedicine
- Information processing, including advanced computing and communications
- Cognitive science, including cognitive neuroscience.

Each of the above technologies is characterized by a high pace of development. Examples of benefits may include revolutionary changes in health care, highly effective communication techniques, improving individual and group creativity, perfecting man-machine interfaces, etc. For purposes of clarification, the potential of converging technologies is illustrated by means of a practical example: education and training.

The objective is to create a virtual-reality training environment that is tailored to the individual's learning modes. This allows training programs to use contexts that are most stimulating to individual learners; another benefit is that it reduces any embarrassment over mistakes. The information exchange with the computer can be fully interactive, including speech, vision, and motion.

In the above example, nano-devices will be essential to store the variety of necessary information or imagery and to process that information for real-time interaction. Biotechnology will be important to provide feedback on the individual's state of accuracy and retention. Information technology must develop the software to enable far more rapid information processing and display. Since cases such as emergency training or integrated border management rely on team relationships, the software must ultimately accommodate interaction among multiple parties. Innovations are also needed to enable augmented-reality manuals, whereby individuals might have real-time display of information for repair and maintenance actions.

Effective learning must start with an understanding of the cognitive process. People have different learning styles and modes: oral, visual, tactile. They respond to different motivations and different contexts. Human memory and decision processes depend on biochemical processes. A better understanding of these processes may lead to enhanced states of accuracy and retention.

Need for New Testing, Evaluation, and Certification Procedures

The integration of systems has a large impact on the current method of testing, evaluation, and certification. It is not sufficient to test, evaluate, and certify the stand-alone equipment individually; rather, it is essential for the integrated systems to be tested, evaluated, and certified as well on the quality of the interaction of this stand-alone equipment in the integrated environment. It will be physically impossible to test for the most adequate and appropriate combinations of integrations of systems, but new testing and evaluation tools will need to be explored.

Opportunities

Capability-based Research

Security is a highly complex environment, with a large variety of scenarios, missions/tasks, stakeholders, and user interests. Each of the specific missions requires the capabilities to deal effectively and efficiently with the day-to-day problems border guards, emergency responders, customs services, and others must face. In this view, science, research, and technological development for security takes on another dimension. Science, research, and technological development for security are primarily forms of capability-based research. It is undertaken to support and facilitate the day-to-day work of people involved in security-related activities. In practical terms, issues need to be addressed such as:

- Technology not to replace human action, but to complement and support it
- Technology not to offer stand-alone solutions, but solutions to be embedded in the operational chain

- Technology to offer complex and integrated solutions, but at the same time to remain user-friendly and easy to operate
- Technology to enhance the level of security, but not infringe on privacy and individual civil liberties
- Technology to increase the level of control in the area of security, but not to increase the number of false alarms or the length of operations.

Capability-based research is not a completely new concept. While it may be a new approach for the civilian research program community, there is significant expertise in the military domain. But it has to be borne in mind that the security environment is very different from the military environment. The largest difference is the great diversity of the user community, resulting in a large variety of user needs and required capabilities. So, although the experience of the military domain provides a good starting point, it is necessary to adapt it significantly to adequately address the specificity of the security sector.

New Technological Advances

Previous sections of this essay have provided overview of what type of technological evolutions could significantly enhance the overall level of competence to respond more adequately the new security challenges. In summary, the technology areas discussed below (among others) need to be further developed at the level of individual technologies.

Sensor and radar technologies. The area of sensor and radar technologies covers the challenges related to the development of new and advanced sensors across the full frequency spectrum—e.g., RF sensor technologies, micro- and millimeter wave sensor technologies, nanotechnologies for sensors, electro-magnetic sensor technologies, electro-optical devices and optronics, laser technologies, IR sensor technologies, UV/visible wave sensor technologies, thermal sensor technologies, NRBC sensor technologies, biological and chemical threat detection technologies, acoustic sensor technologies, terahertz technology, etc. The area also addresses advanced developments in radar technology, including technologies related to the design of receivers and transmitters, digital real-time processing and programming, processing algorithms and control, and the electro-magnetic environment.

Communication technologies. The area of communication technologies covers concepts for secured communication, including network and protocol-independent secured communications, multi-mode secured communications, reconfigurable communications, mobile secured communications, innovative technologies related to the protection of communication networks against harsh environmental conditions, etc.

Information society technologies. The area of information society technologies covers concepts for information and data systems, including pattern recognition, innovative data collection, data classification and data fusion techniques, knowledge management, innovative data and signal processing, grid computing, web intelligence (large-scale data mining), contextual search techniques, actionable intelligence, etc. It also addresses issues related to information warfare, such as cyber security (including

cyber deterrence), cryptology and key management, early detection techniques, non-cooperative IFF techniques, non-cooperative penetration of suspect e-systems, jamming and anti-jamming technologies, etc.

Materials technology. The area of materials technology covers the development of new lightweight and strong materials, coatings, etc., including lightweight materials for human protection and site protection, self-protective and blast-resistant material technology, NRBC protective material technology, etc. The area also looks into opto-electronic material technology and structural materials/structural effects analysis, considering, for example, fiber optic material technology, UV/IR detector material technology, non-linear optical material technology, ceramics and glass technology, and composite materials technology. Also to be considered in this context are further developments in the areas of energetic materials and plasma technology, covering issues such as (micro-)pyrotechnology, explosive detection techniques, etc.

Human sciences. The area of human sciences addresses the aspects of human behavior analysis and modeling, and in particular considers individual behavior, population behavior, prediction of mass behavior, human information processing, teamwork, organizational culture, training (individual and team) and training techniques, collective training, human performance enhancement, task analysis modeling, etc. The area also covers human factors, including human survivability, protection and stress effects, stress and human performance modeling, fatigue and human performance modeling, human factors in manufacturing, uncertainty handling and belief systems, human factors in the decision process, etc.

Social sciences. The area of social sciences covers political and policy developments (national, regional, and international), multi-culturalism and diversity, ethics and human rights, environmental and social issues, welfare and sustainability, religious orientation, societal role of research, etc.

Biotechnology. The area of biotechnology addresses the further development of biological technologies, covering technologies related to biomaterials and nanofabrication, bio-compatible materials, and genetic engineering. Biomedical technologies are also included, in particular rapid analysis of biological agents and of human susceptibility to diseases and toxins; rapid diagnosis of infectious diseases; telemedicine (diagnosis and surgery); development of new anti-viral treatments, antibiotics, vaccines, and drugs, etc. In addition, the area covers agricultural and food-biotechnologies, including mechanisms to combat contamination of agricultural resources (water beddings, rivers, soil, air, etc.), crop and animal viruses, food testing and control techniques, and water testing and purification techniques, as well as addressing techniques for decontamination.

Integration of Systems, Data, and Services

As already stated above, although there is a great need for advances in individual technologies, modern security missions and civil crisis management efforts urgently require a strong focus on integrated concepts, and this at the level of systems, data, and services. Earlier sections of this essay provided an overview of what type of technological evolutions could significantly enhance Europe's overall competence to respond more

adequately the new security challenges. In summary, the following technology areas (among others) need to be further developed at the level of integrated approaches.

Sensor and radar technologies. The area of sensor and radar technologies includes the challenges related to the integration of different technologies in sensors that would allow for the detection of different types of substances (biological, chemical, and other agents and materials), simultaneously using different scanning and sensing techniques. This aspect includes concepts such as "forests" of sensors; network-centric rearrangements of existing sensors; wide-scale, long-range multi-sensor surveillance; autonomous, automated, compact, mobile, and reconfigurable sensors; chip-based sensors; innovative techniques for covert surveillance; sensor-related imaging and mapping techniques; and low-cost concepts (affordability).

Communication technologies. The area of communication technologies addresses technologies in support of interoperable communication, such as secured communications, wireless broadband datalinks, broadband access for mobile users in dynamic situations or electro-magnetically challenging scenarios, population warning techniques, etc.

Information society technologies. The area of information society technologies covers information networks and architectures, including the development of concepts such as secure wireless broadband datalinks for distributed computing, network security and data integrity between distributed sensors, information exchanges and interoperable databases, etc.

Integrated systems technology. The area of integrated systems technology considers integrated systems design; integration of equipment systems; interoperability, reliability, and maintenance of systems; system health monitoring concepts, etc. Specific attention will need to be paid to the certification of these systems, since current testing, evaluation, and certification methods are not adapted to test, evaluate, and certify complex integrated systems. This issue relates to the problems identified above, and will be further addressed in the following section of this essay.

Simulation. The area of simulation addresses equipment simulation techniques, covering issues such as structures vulnerability prediction after explosions and the identification of structural solutions; network-centric deployments of existing sensors; sensor simulation; video-biometric cooperation; survivability of components and equipment; virtual and augmented reality; equipment training, etc. It also considers scenario and decision simulation techniques, in particular advanced human behavior modeling and simulation, simulations for decision making, mission simulation, evacuation and consequence management techniques, chaos theories, impact analysis concepts and impact reduction, pollution modeling, structures vulnerability prediction, etc.

Human sciences. The area of human sciences covers inter-organizational coordination and communication, including coordination in accordance with the organizations' structures, their roles, and means; crisis communications with external parties (media, press, governmental agencies, etc.), potential stakeholders, and the general public; establishment of joint control rooms; etc. It also addresses human interoperability, which includes the need for a better understanding of the specificities and characteristics of

individual services, including their decision processes and operational environments. It covers the development of a common approach to joint operations.

New Concepts for Testing, Evaluation, and Certification

As described above, the integration of systems has a significant impact on current methods of testing, evaluation, and certification. New testing and evaluation tools will need to be explored, in particular the use of simulations in testing and evaluation, and also at the pre-certification level. For example, a key aspect of integrated border management is the monitoring of green border lines between control posts. In practical terms, it might be difficult to assess the performance of tools for border monitoring in all possible environmental situations in all possible climatic situations. Therefore, it is proposed to use simulators instead. Such a simulator would need to comprise and integrate:

- All generic data criteria that characterize the variety in landscape/ environment/ geographical conditions of European green and blue border crossing points/areas
- All generic data criteria that characterize the possible climatic conditions in these locales.

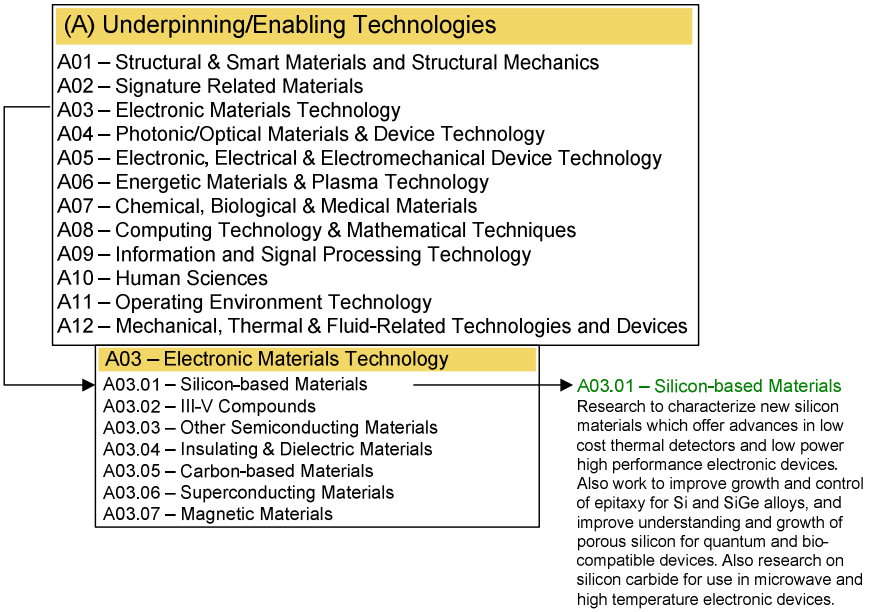
These data will have to be integrated in order to provide an adequate platform to test and evaluate systems according to the technical specifications and characteristics of the integrated systems in a simulation environment.

Threats

Systems Technologies versus Enabling Technologies

The risk of capability-based research and an integrated approach is an over-emphasis on systems technologies, and a consequent lack of focus on enabling or underpinning technologies and basic research. This threat of over-emphasizing system technology is not only real for security-related research activities; it also constitutes a very relevant problem in defense-related research activities, and even for the most recent evolutions in civilian research activities. One example is the concept of integrated projects (FPVI). Integrated projects are based on a "program approach" to dealing with different issues. They are usually composed of various components covering research, demonstration, training, etc. They are expected to assemble the necessary critical mass of activities, expertise, and resources in order to achieve ambitious objectives (thus they are also known as objective-driven research).

Although their research activities may cover the entire research spectrum from basic to applied research, the tendency is for these integrated projects to evolve from objective-driven research into system-driven research, in particular in those integrated projects where demonstration activities are part of the project. Enabling or underpinning technologies are those technologies that are fundamental and necessary for the building of systems. The U.K. MoD's taxonomy identifies the underpinning/enabling technologies as follows:



Security versus Legal and Ethical Principles

One of the key "political" issues to be addressed in the context of the ESRP will be how to enhance security without infringing on the privacy or liberty of individuals. It is not the intention of the ESRP to create a "Big Brother" environment, but it should operate within a framework of balance between security, justice, and liberty.

There is, however, a fine line between security, liberty, and justice, and this line is subject to fluctuation depending on the political situation and social environment. The recent recommendations of the European Council following the terrorist attacks in London supported the principle of data retention. This principle requires telecom companies and Internet service providers to keep details of phone and web communications for at least a year. The content of calls and e-mails would not be kept, but details of the sender, recipient, time, duration, and location would be retained. It is worthwhile to note that a recent proposal on this from the United Kingdom and France faced much opposition from telecom companies and the European Parliament, since it was considered to infringe on individual privacy. There will now be a Commission proposal for a directive related to this issue.

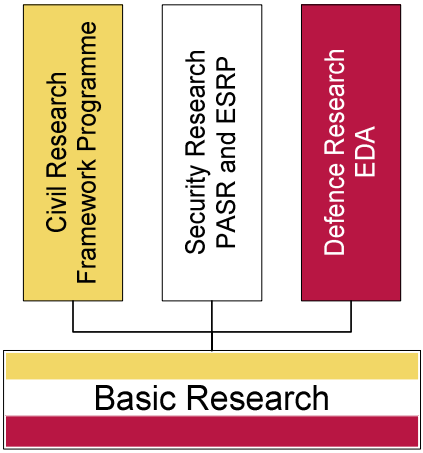
Privacy issues are also gaining prominence in the domain of biometrics. Biometrics are techniques being used as a secure way of identifying an individual through a variety of applications worldwide. Biometric data are being used to improve security, such as making sure that only authorized people have access to sensitive facilities, and using biometric information to prevent theft or fraud (such as identity theft and credit card fraud). They are also a way to identify people who might be wanted by law enforcement authorities. Most biometric approaches work by extracting information from a

picture or recording of, for example, a fingerprint, face, or voice. The information is then stored and later matched to verify the identity of individuals. If biometric methods are to be used, immediately the public's willingness to rely on biometric data needs to be considered, as well as a number of relevant questions: which data are stored, where are these data stored, who has access to these data, what can the data be used for?

Solutions

A "Common" Dedicated Program for Basic Research

In order to address the problem of the increased need for prioritizing between capability- and system-oriented research, it is suggested to consider the establishment of a European basic research program, from which the application- and system-oriented research programs (FP, PASR, ESRP, and defense research) could draw the relevant enabling technologies, as illustrated in the figure below.



Such an approach would allow specific attention to be paid to enabling/ underpinning technologies, examples of which have been described above. It is necessary, though, in this context, to address the funding mechanisms for this program. In basic research, there should be sufficient opportunities to explore new technological areas, including technologies that may result in broad application opportunities, but also technologies with a high risk potential or with few clear opportunities for application opportunities in the distant future. A funding mechanism that requires a 50 percent participation in funding will not encourage the latter type of research, and will thus leave major technology capability gaps.

Technology Monitoring

Technology monitoring is recognized as a crucial activity for achieving and maintaining competitive positions in a rapidly evolving business environment. It serves the purpose of identifying and assessing technological advances critical to competitiveness

and innovation, and of detecting changes and discontinuities in existing technologies. In this context, it would be worthwhile to start a debate around a common technology monitoring process/mechanism for the civil, security, and defense communities.

Cross-Cutting Issues

Security-related research is capability-based and mission-oriented. Its key research focuses relate to integrating different technologies, interoperability, and the impacts of converging technologies. All other key technology sectors are of high relevance to the security-related field: bio-technology, nano-technology, research in the services sector, complexity and systems theory, social sciences and humanities, cognitive science, agricultural and environmental technologies, energy technologies, ICT technologies, manufacturing technologies, and transport-related research activities. Each of these fields of research is important in its own right as an individual technological area, but they take on even greater importance as they are integrated.

Conclusions and Recommendations

Science, research, and technological development in the field of security are primarily capability-based. It is undertaken to support and facilitate the day-to-day work of people involved in security-related activities. Although the European industrial and research community has excellent skills to support and further develop their contribution to addressing the day-to-day problems of security, the recent terrorist events and large-scale disasters show that these skills are not sufficient to adequately and efficiently prevent these horrible events from happening, or to protect human beings and their assets against the catastrophic effects of them. In order to enhance competence and the overall capability to respond more adequately, significant progress needs to be made in further developing a wide range of technologies.

Although advances in individual technologies are very much needed, modern security missions and civil crisis management efforts urgently require a strong focus on integrated concepts. It is suggested to follow and develop the concept of network enabling capabilities (NEC), which are much more concerned with evolving capabilities by bringing together decision makers, sensors, and other equipment/systems, and enabling them to pool their information by "networking" in order to achieve an enhanced level of capability. In NEC, the key word is *interoperability*, and this at the level of services (human interoperability), systems (technical interoperability), and information (data interoperability). Converging technologies are also a key area to be explored. The integration of systems has a large impact on the current methods of testing, evaluation, and certification. New testing, evaluation, and certification tools will need to be explored, in particular the use of simulation in testing and evaluation, and at the pre-certification level.

In order to address the risks that capability-based research and an integrated approach may over-emphasize systems technologies and thereby not pay sufficient attention to enabling or underpinning technologies and basic research, it is recommended to consider the establishment of a European basic research program, from which the ap-

plication- and system-oriented research programs (FP, PASR, ESRP, and defense research) could draw the relevant enabling technologies. New funding mechanisms to support this research will need to be explored. With the purpose of identifying and assessing technological advances critical to competitiveness and innovation, and of detecting changes and discontinuities in existing technologies, it is recommended to start a debate around a common technology monitoring process/mechanism for the civil, security, and defense communities.