Emerging Technologies
in the context of “security”

Table of contents

1 Overview

On 12 December 2003, the European Council adopted a European security strategy “A secure Europe in a Better World. This document provides the framework for European concerted activity in the field of security and, more specifically, 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 effectively undertake action in the field of security, was emphasised by a series of recent events caused by terrorist activity as in Madrid and London or by natural disaster as the Tsunami.

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 Programme (ESRP).

Of particular relevance for preparing the content of this ESRP are the so-called road-mapping activities that the European Commission has contracted under the first call of the PASR. The road-mapping activities (SeNTRE and ESSRT) will make a comprehensive strategic analysis of where research activities should focus in priority.

2 Socio-economic challenges

2.1 Definition for security

COM(2004) 72 final 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, citizens’ concerns, including the protection against terrorist threats, and the adaptation of governance structures to effectively deal with these matters.”

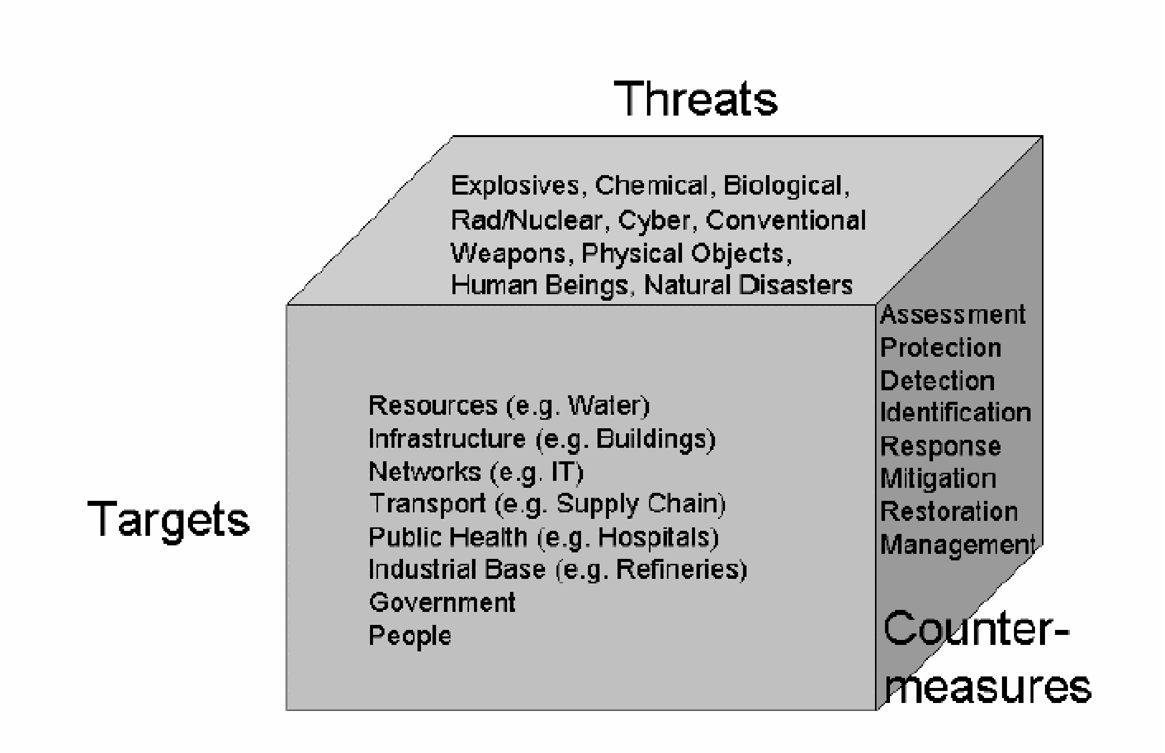
Since this definition is rather vague and tends to limit the focus of security to terrorism and anti-terrorism, it is suggested to adopt for the purpose of this report a definition which broadens this scope, to also include organized crime such as illicit trafficking, illegal immigration, smuggling, etc. as well as the need for enhanced capabilities to cope with natural threats such as flooding, forest fires, etc.

The CEN BT/WG 161 on Protection and Security of the Citizen 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, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made).***

2.2 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.


Threats
Explosives, Chemical, Biological, Rad/Nuclear, Cyber, Conventional Weapons, Physical Objects, Human Beings, Natural Disasters
Targets
Resources (e.g. Water)
Infrastructure (e.g. Buildings)
Networks (e.g. IT)
Transport (e.g. Supply Chain)
Public Health (e.g. Hospitals)
Industrial Base (e.g. Refineries)
Government
People
Assessment
Protection
Detection
Identification
Response
Mitigation
Restoration
Management
Counter-measures

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 listed in the security model above:

- *Resources* cover the quality of water, soil and air and include natural energy resources and the food supply chain, including plants and animals.
- *Infrastructures* address buildings 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 considers the finance system.
- *Information, Computers and Communication* includes computer information systems, information sharing systems and communication networks, public (broadcasting) as well as emergency communications. It also addresses 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, ambulance, police)
- *Industrial Base* considers refineries, power plants, gas tanks, chemical plants, etc. and any structure that produces potentially hazardous material. It pays specific attention to nuclear processing facilities and the defence supply chain.

- *Government* (all levels) addresses command and control functions, intelligence/information services and continuity of operations
- *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. Targets can be classified into several categories as listed in the security model above:

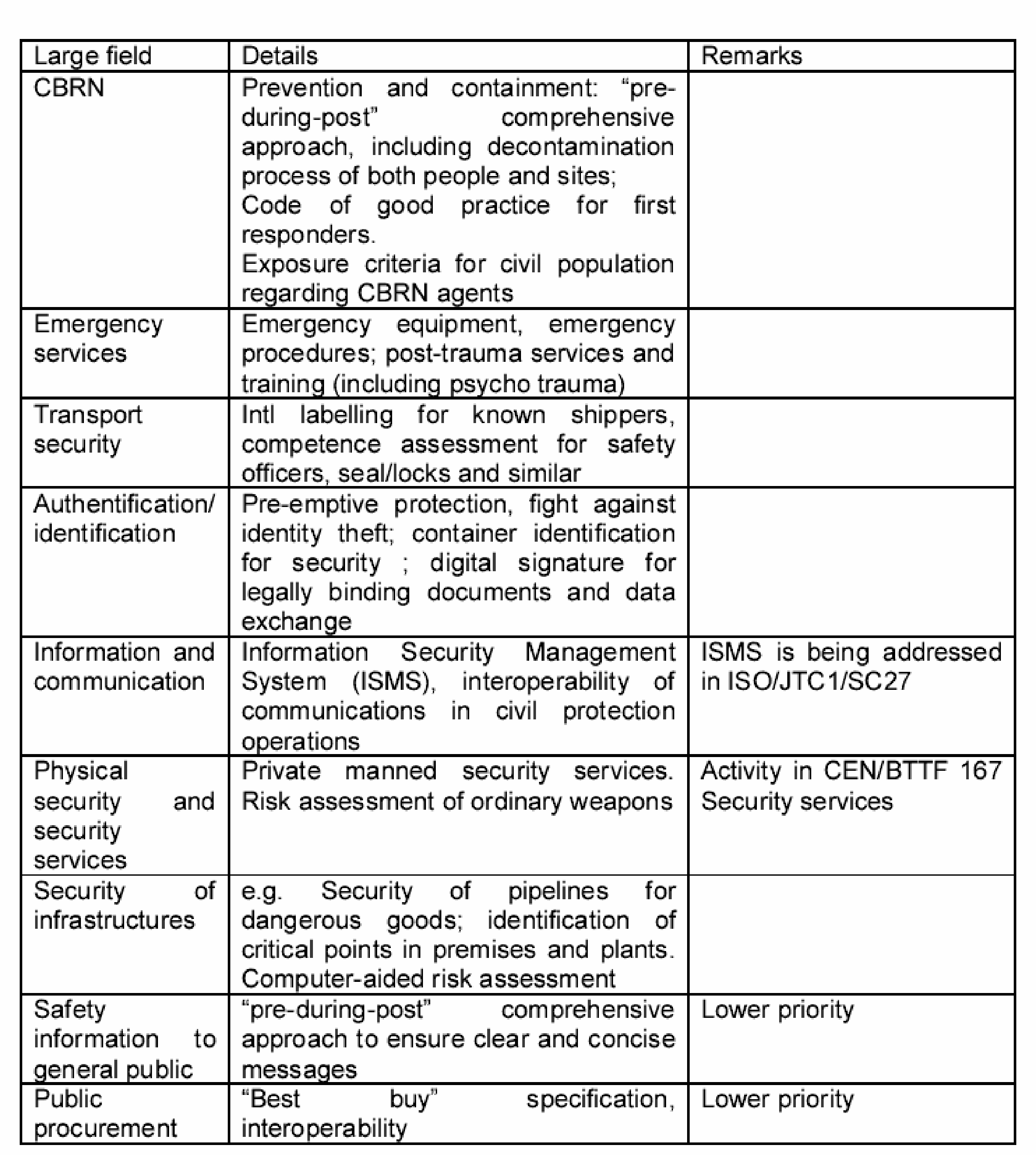
- *Explosives*
- *Chemical agents*
- *Biological agents*
- *Radiological/nuclear material*
- *Cyber* includes somputer viruses, denial of service, hacking, spoofing, identity theft, etc.
- *Conventional weapons* covers a.o. handguns, knifes, etc.
- *Ordinary physical objects used for attacks* cover the use of an object or a vehicle, such as a plane or a truck, as a weapon (e.g. plane attack on the Twin-Towers, 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 listed in the security model above:

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

2.3 Standards for security

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

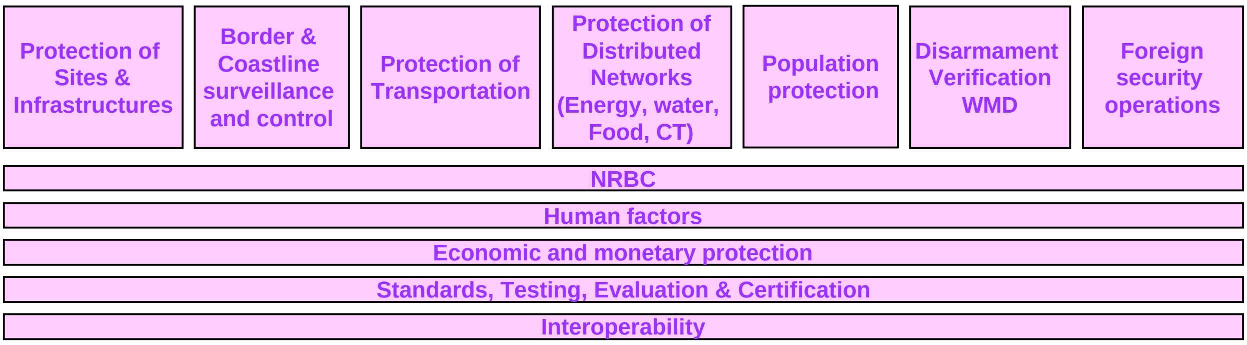


Large field	Details	Remarks
CBRN	Prevention and containment: "pre-during-post" comprehensive approach, including decontamination process of both people and sites; Code of good practice for first responders. Exposure criteria for civil population regarding CBRN agents	
Emergency services	Emergency equipment, emergency procedures; post-trauma services and training (including psycho trauma)	
Transport security	Intl labelling for known shippers, competence assessment for safety officers, seal/locks and similar	
Authentification/ 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 System (ISMS), interoperability of communications in civil protection operations	ISMS is being addressed in ISO/JTC1/SC27
Physical security and security services	Private manned security services. Risk assessment of ordinary weapons	Activity in CEN/BTTF 167 Security 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

2.4 Missions for security

Building on the targets, threats and countermeasures, a comprehensive approach can be developed, which identifies the security and security-related activities, missions and competences necessary to cope with the protection, sustainability and management of what is perceived to be a secure environment. This approach consists of seven vertical and five horizontal missions as illustrated in the table below.

COMPREHENSIVE SECURITY MISSIONS



Protection of Sites & Infrastructures

Border & Coastline surveillance and control

Protection of Transportation

Protection of Distributed Networks (Energy, water, Food, CT)

Population protection

Disarmament Verification WMD

Foreign security operations

NRBC

Human factors

Economic and monetary protection

Standards, Testing, Evaluation & Certification

Interoperability

The *protection of sites and infrastructures* covers the protection of public infrastructures, government buildings, public utilities, harbours, airports, (railway)stations and will also address the protection of hazardous sites such as chemical factories, nuclear powerplants, etc.

The *surveillance and control of borders and coastline* includes the surveillance and control of the blue and green borders as well as the surveillance of the airspace. It will consider issues such as illicit trafficking (a.o. arms, drugs), illegal immigration, counterfeit, etc.

The *protection of transportation* addresses the protection of land, sea and air vehicles as well as the supporting infrastructures, including pollution. The transport will be considered as possible target, but also in its role as possible weapon.

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

The *protection of the population* looks at people, be it as individuals or in groups. This topic covers a wide variety of aspects, ranging from specific vulnerabilities to human behaviour in crisis situations. Specific 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.

The *mission on disarmament verification – Weapons of Mass destruction* will consider capabilities needed for marking and tracing and will also include enhanced surveillance of sites.

The *foreign security operations* will cover the civil aspects of humanitarian operations, civil 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 the vertical missions in an adequate and comprehensive way. These horizontal missions are:

- *NRBC (prevention, detection, protection and decontamination)*
- *Human factors*

- *Economic and monitory protection*
- *Standards, testing, evaluation and certification*
- *Interoperability*

3 SWOTS analysis

3.1 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, e.g. world-class sensors of all types, top of the art network enabling capabilities (NEC), etc.

This section will give an overview on what these strong capabilities are and/or would need to be developed to. In order to structure this overview, this section will for each of the security missions and sub-missions identified in section 2.4., give an indication of useful support measures, describe the required support technologies or tools and give examples of useful integration/validation. The value of simulation and training tools will be illustrated in a few examples.

3.1.1 Protection of Sites and Infrastructure

3.1.1.1 Protection of Sites

Support measures

- Mapping of the 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

- Sensors:
    - Micro technologies for Sensors (surveillance, NRBC detection and tracing, …)
    - Advanced low cost smart, embedded (incl BC), smart sensors and novel techniques for discrete surveillance
    - Smart camera
    - Unattended Sensors and automated tracking across a field
    - Distributed « network 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 / although interoperable communications (video conferencing, mobile phone, WiFi) : Personal nomade information and communications system with augmented reality (“video, communications on a Palm”)
- Protection of networks against harsh environment (including directed energy weapons, laser, HPM…)
- Pattern recognition: extracting information from poor quality images/artificial intelligence systems
- Non cooperative access control

    - Check points (person and object signature - image, X-rays, 3D, neutron…- , Data Bases)
    - Detection of civil partners - Localisation of civil partners
- Light materials for human & site protections

Simulation and preparedness

- Structures vulnerability prediction after explosions and structural solutions
- Network centric of existing sensors (forest of sensors)
- Secured Wireless Broadband data links (for forest of sensors)
- Data fusion
- interoperability
- Personal nomade SIC with augmented reality
- Sensors simulation
- Survivability of components & equipment
- Advanced human behaviour modelling and simulation:
    - Prediction of mass behaviour (with immersion…)
    - Simulation 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 the choices, assist the design of procedures and assess the performances
- Simulator for training (methods and tools for aided decision making before and during operations)
- Sensor/data processing and fusion demonstrator (to get the « Hazard Global Picture » from Satellite data to micro-UAVs and sniffers at a check point…) for Surveillance / Detection / Verification…

3.1.1.2 Public Infrastructures and public building protection

Support measure

- Mapping of important European civil facilities (metro- and train stations, large sport stadiums, banks, government buildings, hospitals, …), related risk and threat assessment, prioritisation versus affordability

Support technologies or tools

- Surveillance and recognition systems
- New materials (glasses…)
- NRBC detection and protection, in particular air pollution and intoxication
    - Low cost C sensors
    - B sensors
- Population warning systems
- Evacuation and consequence management concepts

3.1.1.3 Protection of Public Utilities

Support measures

- Mapping of European infrastructures for food, water, agriculture, energy (electrical, gas and oil, dams), telecommunication, etc. and related risk and threat assessment

Support technologies or tools

- Simulations (chaos theories…)
- Protection of water supply (unusual and biological threat detection)
- Contamination and intoxication of agriculture (water beddings, rivers, soil, air,…), Crop and animal viruses
- Food testing and control
- Protection of energy plants and telecommunication networks (Surveillance, backup (reserve) energy systems,…)
- BC sensors for confined public rooms
- Light materials for human protection

Integration/validation

- Micro unmanned Aircraft Vehicle (micro-AV) demonstrator with miniaturized BC or surveillance sensors
- Personal nomade C2 with augmented reality

3.1.1.4 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, …)

Support technologies or tools

- BC long range sensors
- EM protection
- Simulations (chaos theories…)
- Impact analysis concepts and impact reduction
- Population warning systems
- Evacuation and consequence management concepts
- Decontamination techniques, first aid and protection kits
- Survivability of components & equipments
- Structures vulnerability prediction after explosions and structural solutions
- Protection and Survivability of systems against DEW (laser, HPM)

Integration/validation

- Electronic noise
- MAV demonstrator for surveillance
- Self-protected containers (explosion resistant…), with chemical sensor on a chip

3.1.1.5 Protection of Harbour

Support measures

- Specific studies for utilisation of defence technologies (affordability)

- Protection of off-shore installations (oil- and wind farms)
- “secure harbour” (Feasibility study, state-of-the-art assessment, scenario analysis, system definition)

Support technologies or tools

- Wide-scale multi-sensor surveillance
  - Radar systems
  - Optical detectors, optronics, night vision
  - Satellites
- Defence technology input for
  - “swimmer”-protection systems
  - acoustic surveillance systems (for illegal craft)
- IR/optical surveillance
- Underwater Unmanned Vehicle (UUVs)
- Smart naval shelters (with chips, anti-explosive light structure)

3.1.1.6 Protection of airports

Support measures

- Specific studies for utilisation of defence technologies (affordability)
- Protection of off-shore installations (Oil and Wind-farms)
- « Secure harbour » (Feasibility study, state-of-the-art assessment, scenario analysis, system definition)

Support technologies or tools

- Wide-scale of multi-sensor surveillance, supported by satellite systems, etc
- Secure communication systems
- Tunnel of truth (trusted traveller in correlation with verified luggage, etc)
- Secure interoperability with visa data bases and other tools necessary for support to integrated border management

Integration/validation

- smart container,
- integrated controlled door,
- hardening against electronic noise,
- micro-UAV demonstrator for surveillance, etc

3.1.2 Integrated Border Management

3.1.2.1 Border Surveillance

Support measures

- Real time border surveillance , command and control (including intelligence)
- Access Control : managing Entry and Exit to « Schengen zone »

Support technologies or tools

- Observation/detection

    - Sensors attended and unattended (early warning, ground, balloons,…, from land Radar to Video surveillance to Sniffers, quiet sensors)
    - Optronic sensors : short and long range, surface and airborne, night vision
    - Remote detection through sensors (Lasers, UAVs,…)
    - Microsystems / nanotechnologies…
    - Small disposable auto-configuring network of sensors
    - Distributed « forest of sensors », on the ground, in the air or in the Space
    - New materials as sensors: react to variations of the environment (change colour…), electromagnetic defences, seismic sensors, infrared watchers,.
- Communication and radio communication
    - Secured/although interoperable mobile phone, WiFi, Broad-band (video/global picture, multi-sensors), Distributed (between 100000 sensors… (like mobile phones or PMR …) or Satellites), protected (encryption), very fast spectrum scanning and analysis (data, voices), GSM monitoring
- Identification including biometry, rapid detection (wearable NRBC badge, forged passport)
- Access control systems
    - Cooperative and Non-cooperative (camera on a computer…), automatic pre-authorisation (clearance levels, fast-track..), abstracting salient points from raw data.
- Detection at Check points (person and object signature): image, millimetre-wave, X-rays, 3D, neutron…), Data Bases
- Information exchanges and interoperable databases to achieve a global assessment

Integration/validation

- Border surveillance demonstrator including at least one check point
- Micro UAV demonstrator for border control

3.1.2.2 Illegal immigration control

Support technologies or tools

- Border statistical surveillance (identification of paths, …)
- Unattended sensors
- Inter-connected and integrated visa/immigration facilities control systems
- Biometry
    - Permanent and unpermanent : face recognition, thermal cartography, digital fingerprints, iris/retina , handshape, earshape
    - Behaviour : voice, handwriting, signature,
    - False reject ratio, and false acceptance ratio, decision level.

Integration/validation

- Check point demonstrator
- Optical or Biological verification with reconnaissance sensors systems

3.1.2.3 Coastline and borderline protection

Support measures

- Definition of affordable system to perform coastline surveillance missions (covering missions like vessel traffic (sea route), search and rescue, assistance to ships, pollution, fire fighting, illegal immigration, smuggling of drugs in peacetime as well as terrorist landings and attack in "crisis to war" time), in a dedicated region (including harbours which constitute HVT's (High Value Target)), trade off studies (effectiveness, detection rate, adaptability, modularity, ...)

Support technologies or tools

- radars (surface and airborne threats): airborne imaging radar (SAR and ISAR) mobile/transportable coastal radars
- Networking surveillance assets (static and dynamic sites)
- Image data processing, broad-band, data fusion
- Sensors including EO active (Laser) 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 station including mobile …)

3.1.2.4 Illicit trafficking (drugs, weapons, ammunition, explosives)

Support measures

- Marking and tracing methodology

Support technology/tools

- NRBC detectors at checkpoints
- Labs on a chip
- Identification and tracing of intermediary products
- Chemical sensors
- Compact sensors with tuneable laser diodes for mixture of explosives detection
- Smart labels
- Ruggedised marking
- Secret marking

Integration/validation

- Worldwide Network-Database availability (Standardisation / Legal / Political acceptable)

3.1.3 Distributed networks protection

3.1.3.1 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, processing
  - Outside Europe: through air including UAVs/spaceborne observation (radar mainly)
- Water distribution
  - Dam surveillance
  - From satellites to micro sensors in water supply
  - Protection of water supply (unusual and biological threat detection)
  - Air/Water cleaning and filtering systems

Integration/validation

- EM low cost hardened communication civil networks

3.1.3.2 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 data mining)
  - Early detection from few statistical events
  - Non-co-operative 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/electro-magnetically difficult scenarios
- Precise location of standard communication systems for non-co-operative 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

3.1.4 Protection of transportation

3.1.4.1 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 (cf Galileo)
    - Fleet managment
    - Mobile resources integrated management
- Containers
    - positioning and tracking
    - self protected (explosure resistant…) container, with sensors on a chip
    - Protection and Survivability of systems against DEW (laser, HPM)
- Security at terminals, warehouses and distribution centres of critical goods (Wireless video surveillance and Opto surveillance)
- Protection of automated systems, information technology and documentation procedures for operational command and control centres
- Protection of rail and road infrastructure, railway protection and detection of missing parts

Integration/validation

- Fleet management demonstrator
- Smart container demonstrator

3.1.4.2 Protection of sea transportation

Support technologies or tools

- Navigation and tracking (even non-cooperative by data collection)
- Critical sea/coast areas regular survey (space and airborne) to discriminate false signals when crisis
- Mine sensing
- Anti-hijacking protection
- Pollution modelling and simulations (specific toxines / chemicals,…, NRBC)
- Pollution disaster prevention and management equipment
- self protected containers (explosure resistant…), with chemical sensors on a chip
- Structures vulnerability prediction after explosions and structural solutions
- Protection against harsh EM environments
- Protection and Survivability of systems against DEW (laser, HPM)

Integration/validation

- Naval container demonstrator

3.1.4.3 Underwater threats (incl. sea mines)

Support measures

- Transferable from underwater warfare technologies

Support technologies or tools

- Remote mine sensing (fly over detection)
  - EM solutions
  - opto-electronic solutions with lasers
- Swimmer delivery vehicle
- Bottom crawlers
- Underwater swimmer detection sonars
- New low cost sensor technologies for underwater magnetic and acoustic arrays for passive threat detection and development of new transducer technologies for active threat detection.
- Innovative Signal Processing for the detection of small objects in high reverberating environment.
- Innovative Classification and Data Fusion process of the acoustic/magnetic detected threats based on a new Artificial Intelligence methodology
- Advanced Low Energy Radar with high resolution and interception of small moving targets in clutter associated by low transmitted power peak power, in order to be not hazardous for people.
- IR active imager with eye-safe capability and modular integration of the EO sensor independently from the site morphology

3.1.4.4 Protection of air transportation

Support technologies/tools

- Light materials for aircraft protection (light armour plates etc)
- Protection of SIC against harsh environment
- Broadband Communication
- Electronic noise detector

Simulation

- Sensors simulation
- Survivability of components & equipments
- Aircraft structures vulnerability prediction after explosions and structural solutions
- Protection and Survivability of systems against DEW (laser, HPM)

Integration/validation

- BC detection systems for airports
- Fuselage with NG structure, explosion resistant (after vulnerability prediction & protection against explosions) (applicable also to helicopters for evacuation or humanitarian operations)
- Aircraft self protected container
- Demonstrators of containers (with chips) surveillance systems
- Civil aircraft protection from terrorists threats such as Manpads or Laser blinding: decoys and Infra-red /Counter Measures

- Hardened canopies and glass walls (against lasers, HPM)

3.1.4.5 Less Than Lethal Weapons-inside aircraft adapted

Support information

- Risk assessment of LTLW effect in closed spaces
- Risk in (or to generate) depressurisation situation

Support technologies/tools

- Marking devices
- Miniaturization
- MFP stopping barriers
- Dazzling laser torche
- Painful lasers
- High power directed acoustics
- LTL grenade launcher
- Long Term LTLW effects – Antidote
- Aircraft Save Technologies
- Simulation
- Secure communication with Land
- Mini robots

Integration/validation

- Crew / Cabin personnel training and Users education

3.1.4.6 Protection of legal transportation of hazardous, critical goods

Support information

- Marking and tracing methodologies / case studies

Support technology/tools

- Secured containers
- Integrated positioning/localisation/data transmission kits
- Detectors on containers
- Secret marking
- Packaging standardisation
- Light materials against explosion and chemical attack
- Tracing liability

Integration/validation

- Worldwide Network-Database availability (Standardisation / Legal / Political acceptable)
- Electronic noise detector demonstrator
- Secured container demonstrator

3.1.5 Protection of people

3.1.5.1 Protection of population

Support measures

- Risk assessment in public and urban areas

Support technology or tools

- Training / simulations (Virtual or augmented reality)
- Modelling
  - Real data collection
  - Phenomena (propagation, effects…)
  - Population behaviour
  - Individual behaviour / response to threat (effective / physical and perceived)
- Personal security
  - Protection against viruses / biological agents / radioactivity
  - Vaccines / immunology studies
  - Specific materials / composite materials / specific Air Intake Filters…
- Low cost BC sensors & alarm systems
- Perception of security (sociological aspects)
- Surveillance and recognition in Urban environment
- Population warning systems

Integration/validation

- Interoperable crisis Command Control Communications (C3) Demonstrator (« security lab »), for scenarios elaboration and emergency forces training
- Personal nomade information and communications system with augmented reality ("video, communications on a Palm")

3.1.5.2 Law enforcement

Support information

- Technico-operational risk assessment of an unauthorized use of fire arms or LTLW in Law Enforcement
- Assessment of Progressive reply in proportion of 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)

Support technologies/tools

- Biometry,
- Micro pyrotechnology,
- Microsystems,
- Physiological effects,

Integration/validation

- Architectural concept
- Tactical-operational efficiency

- Legal- Liability- Training simulation

3.1.5.3 Protection of emergency and other services

Support measures

- Case studies

Support technology or tools

- Training / simulations (Virtual or augmented reality)
- Combined operations with Robots, UAVs, etc…
- Visualisations/localization/ maps/ access to databases etc. on mobile terminals
- Secured communications
- Logistics : Optimised interventions
- Personnel physical protection (miniaturized detectors, …)
- Decontamination techniques
- Knowledge Management, store and index the experience gained for further improvements
- Modelling updating
- Law enforcement equipment compatibility with first responders
- Damage assessment
- Automatic mapping

Integration/validation

- Crisis management simulator

3.1.6 Security Policy

3.1.6.1 Global risk assessment

Support measures

- Analysis of the data available (Constraints, limitations, access,…)
- Models and methodologies for proactive evaluation, risk assessment and early warning
  - For preventing acts of terrorism
  - For monitoring global stability

Support technologies or tools

- Evaluation and risk assessment models and databases
- Grid computing
- Advanced heterogeneous data mining / browsing on sensitive information
- Multivariable analysis
- Actionable intelligence for preventing acts of terrorism
- Behaviour analysis for safety and security
  - Uncertainty handling, optimisation methods
  - Belief systems
- Risk assessment for potential terrorism targets
  - Cultural databases
  - Universal translators

Integration/validation

- Specific Open Source Browser (« security Google »)

3.1.6.2 Humanitarian aid (Petersberg tasks)

Support measures

- Definition of a European crisis analysis management capability

Support technology/ or tools

- For all missions :
  - Observation, monitoring and supervision, through spaceborne, airborne, Humint, etc… data acquisition, collection, processing (data mining, data fusion, modelling, …)
  - Secured communications/positioning (anti-jamming, space-based comms, …)
  - Advanced “security” C4ISR including mobile and deployable (possible article 169)
  - Logistics support : advanced tools including simulations and training
- Humanitarian and evacuation operations :
  - Transport/medical helicopters logistics and protection
  - Mobile medical facilities including telemedicine

Integration/validation

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

3.1.6.3 Counter-proliferation - Armament/disarmament verification

Support measures

- Ballistic Threat Assessment and Forecast

Support technology or tools

- Databases and intelligence :
  - Identification of unique/traceable components moves/purchases
  - Chips on critical containers
  - Sensitive sites and « tracks » detection
  - « Labs on a chip »
  - « Verification kits including remote access to databases»
- Support to nuclear waste/ power plants/ nuclear submarine « cleaning »: i.e with Russia and Ukraine
  - Vegetation/environment monitoring
  - Status monitoring
- Illicit trafficking :

    - Border surveillance control (paths, roads,…) by airborne, spaceborne, cameras
    - Low cost detectors – Marking and tracing of arms and ammunition

Integration - validation

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

3.1.6.4 Crisis management systems including Mobile Deployable HQ

Support measures

- Available data sources, links, etc… in the EU
- Candidate architectures

Support technology or tools

- Rapid deployment/mobility/sustainability
- Multimedia / multisource integration on video wall
- Interaction
- Immersion
- Hyper realistic render
- multi user architecture : data management & 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 evidences…, real time …)
- Human factors (stress,…) in the decision process
- Behaviour under stress (especially in mobile environments…)
- EM hardening for deployable systems

Integration/validation

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

3.1.7 Horizontal missions

3.1.7.1 NRBC detection, protection and decontamination

Support measures

- Modelisation for threat evaluation and impact assessment
- Equipment assistance definition

Support technology or tools

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

        - Nuclear detector based on deployable sensors for:
            - close-up detection of γ ray dose rate and γ radio nucleid
            - radioactive contamination monitoring
    - Protection of the population
        - NRBC filters, air lock systems, …
        - Specific materials, composite materials, …
        - Personal protection against viruses, biological agents, radioactivity, …
        - Vaccines, antidotes, immunology studies
    - Decontamination techniques
        - Specific showers
        - New active materials, paintings, …

Integration/validation

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

3.1.7.2 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 & 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, resistant in a harsh environment,
    - 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
- Nomade Information and Communication system with augmented reality on a Palm
- Network of personal nomade computers and CIS

3.2 Weaknesses

3.2.1 Need to further develop specific technological competences

The recent terrorist events and large-scale disasters show that, despite the very good European in-house science, research and technology competences, they do not suffice to adequately and efficiently prevent these horrible events from happening and to protect human beings and their properties and assets against the catastrophic effects of them.

In order to enhance competence and overall capability to respond more adequately, significant progress needs to be made in further developing the individual and combined technologies identified under section 3.1.

3.2.2 Need for an integrated approach

Modern security missions and civil crisis management require concepts that are:

- Responsive and adaptable, so that they can respond to changing needs of 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 across all levels they can operate in integrated operations involving all relevant national and international services
- Broad, so that they are able to operate over 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 at all times access to information and enabling the user to search and exchange information that has been collected by all sources internal and external to the field.
- 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, etc… and when necessary military services to support operations

The EU has today 25 Member States, each of the Member States with different systems in place, with different protocols, with different decision procedures, etc… Moreover, security is a multi-service activity, involving stakeholders from a variety of domains. E.g. Border control and management involve border guards, law enforcement, customs, illegal immigration offices, etc. For such a fragmented and heterogeneous environment a doctrinal one-for-all integrated concept may not be the best approach. It is suggested to follow and develop the concept of network enabling capabilities (NEC) which are much more concerned with evolving capability 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 level. Technical interoperability concerns the technical aspects related to the interconnection of different systems and equipments, so that information exchange between these different systems and equipments becomes technically possible. Interoperability of data deals with incompatibility of data and datasets and looks at the process of data-mining and data-fusion with the objective to achieve that the right information reaches the right person at the right location at the right time, so that this person can take the right decision and/or undertake the right action (so-called “seamless sharing of information”.

However the largest challenges of interoperability are at the human operational level. Problems need to be overcome that mainly result from multi-agency, multi-service, multi-cultural communication and collaboration, in particular

- Different cognitive processes and behaviours
- Different ways of capturing, sharing and re-using knowledge (learning from experience)
- Different organisational structures and decision processes
- Different understanding of impact and costs
- Different team situation awareness and shared situation awareness
- Different Reporting procedures
- Need for cross-agency standardisation and protocols

3.2.3 Need for a multi-modal approach

One step further in the process towards a full integration is the so-called process of converging technologies. This process combines and builds on the synergies and cross-fertilisations 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 at a high pace of development and examples of pay-off may include revolutionary changes in healthcare, highly effective communication techniques, improving individual and group creativity, perfecting man-machine interfaces, etc.

For clarification purposes, the potential of converging technologies is illustrated by means of a practical example, i.e. education and training.

The objective is to create a virtual-reality training environment, which is tailored to the individual’s learning modes, which uses the contexts stimulating the individual and which reduces any embarrassment over mistakes. The information exchange with the computer can be fully interactive (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 accurateness and retention.

Information technology must develop the software to enable far more rapid information processing and display. Since e.g emergency training or integrated border management must include teaming relationships, the software must ultimately accommodate interaction amongst 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 modes (oral, visual, tactile). They respond to different motivators and different contexts. Human memory and decision processes depend on biochemical processes. A better understanding of these processes may lead to enhanced states of accurateness and retention.

3.2.4 Need for new test, evaluation and certification procedures

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

3.3 Opportunities

3.3.1 Capability-based research

Security is a very 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 people, custom services, etc are confronted with. In this understanding, science, research and technological development for security, has another dimension. Science, research and technological development for security is *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
- Technology not to offer stand-alone solutions, but solutions to be embedded in the operational chain
- Technology to offer complex and integrated solutions, but remain user friendly and easy-to-operate
- Technology to enhance the security level, but not infringe on privacy and liberty of the individual
- Technology to intensify the control, but not to increase the level of false alarms or the length of the procedure
- …

Capability-based research is not a completely new concept. Whilst it may be a new approach for the civil research programmes 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 very wide spread of the user community, resulting in a large variety of user needs and required capabilities. So, although the military domain provides a good starting point, it is necessary to adapt it significantly to adequately address the specificity of the security sector.

3.3.2 New technological advances

Section 3.1 provides a good overview of what type of technological evolutions could significantly enhance the overall competence to respond more adequately the new security challenges.

In summary, a.o. the following technology areas need to be further developed at the level of individual technologies:

3.3.2.1 Sensor and radar technologies

The area of sensor and radar technologies covers the challenges related to the development of new and advanced sensors covering the full frequency spectrum, i.e. RF sensor technologies, micro- and millimetre 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, in particular 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 receiver and transmitter, digital real-time processing and programming, processing algorithms and control, the electro-magnetic environment, etc.

3.3.2.2 Communication technologies

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

3.3.2.3 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 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-co-operative IFF techniques, non-co-operative penetration of suspect e-systems, jamming and anti-jamming technologies, etc

3.3.2.4 Materials technologies

The area of materials covers the development of new light and strong materials, coatings, etc., including light materials for human protection, light materials for site protection, self-protective and explosive resistant material technology, NRBC protective material technology, etc.

The area also looks into opto-electronic material technology and structural materials/structural effects analysis, considering e.g. optical fibre material technology, UV/IR detector material technology, non-linear optical material technology, ceramics and glass technology, composite materials technology, etc.

Also to be considered in this context, are the further developments in the areas of energetic materials and plasma technology, covering issues such as (micro-)pyrotechnology, explosive detection techniques, etc.

3.3.2.5 Human sciences

The area of human sciences addresses the aspects of human behaviour analysis and modelling and in particular considers individual behaviour, population behaviour, prediction of mass behaviour, human information processing, team work, organisations and cultures, training (individual and team) and training techniques, collective training, human performance enhancement, task analysis modelling, etc.

The area also covers human factors, including human survivability, protection and stress effects, stress and human performance modelling, fatigue and human performance modelling, human factors in manufacturing, uncertainty handling and belief systems, human factors in the decision process, etc.

3.3.2.6 Social sciences

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

3.3.2.7 Biotechnology

The area of biotechnology addresses the further development of biological technologies, covering technologies related to biomaterials and nanofabrication, bio-compatible materials

Biomedical technologies are also considered, in particular rapid analysis of biological agents and of human susceptibility to diseases and toxicants, rapid diagnosis of infectious disease, telemedicine (diagnosis and surgery), novel anti-virals, antibiotics, vaccines, and drug development, etc.

In addition, the area covers agri/food-biotechnologies, including contamination and intoxication of agriculture (water beddings, rivers, soil, air, etc.), crop and animal viruses, food testing and control techniques, water testing and purification techniques, etc. and addresses techniques for decontamination.

3.3.3 Integration of systems, data and services

As already stated in section 3.2.2, although advances in individual technologies are very much needed, modern security missions and civil crisis management require urgently a strong focus on integrated concepts, and this at the level of systems, data and services.

Section 3.1 provides a good overview of what type of technological evolutions could significantly enhance the overall competence to respond more adequately the new security challenges.

In summary, a.o. the following technology areas need to be further developed at the level of integrated approaches:

3.3.3.1 Sensor and radar technologies

The area of sensor and radar technologies includes the challenges related to the integration of different sensor technologies in sensors that would allow sensing for detecting different types of substances (biological, chemical and-or other agents/materials) simultaneously using different scanning and sensing techniques. This part includes concepts such as forest of sensors, network centric of existing sensors, wide-scale long-range multi-sensor surveillance, autonomous, automated, compact, mobile and reconfigurable sensors, sensors on a chip, innovative techniques for discrete surveillance, sensor-related imaging and mapping techniques, low cost concepts (affordability), etc.

3.3.3.2 Communication technologies

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

3.3.3.3 Information society technologies

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

3.3.3.4 Integrated systems technology

The area of integrated systems technology considers integrated systems design, integration of equipment, interoperability, reliability and maintainability of systems, system health monitoring concepts, etc. Specific attention will need to be paid to the certification of these systems, since current test, evaluation and certification methods are not adapted to test, evaluate and certify complex integrated systems. This issue relates to the problem identified in section 3.2.4 and will be further addressed in section 3.3.4.

3.3.3.5 Simulation

The area of simulation addresses equipment simulation techniques, covering issues such as structures vulnerability prediction after exposures and structural solutions, network centric of existing sensors, sensor simulation, video-tag-biometric co-operation, survivability of components and equipment, virtual and augmented reality, equipment training, etc.

It also considers scenario and decision simulation techniques, in particular advanced human behaviour modelling and simulation, simulation for decision making, mission simulation, evacuation and consequence management techniques, chaos theories, impact analysis concepts and impact reduction, pollution modelling, structures vulnerability prediction, etc.

3.3.3.6 Human sciences

The area of human sciences covers inter-organisational co-ordination and communication, including co-ordination in accordance with the organisation structures, their roles and means, crisis communications towards external parties (media, press, governmental agencies, etc.), potential stakeholders and general public, joint control room, etc

It also addresses human interoperability, which includes the need for a better understanding of the specificities and characterstics of individual services, including their decision process and operational environment and covers the development of a common approach towards joint operations.

3.3.4 New concepts for testing, evaluation and certification

As described in section 3.2.4, the integration of systems has a large impact on the current way of testing, evaluation and certification. New test and evaluation tools will need to be explored, in particular the use of simulation in the testing, evaluation and also at the (pre-) certification level.

E.g. a key aspect in 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 characterise the variety in landscape/environment/ geographical conditions of the European green and blue border crossing points/areas.
- All generic data criteria that characterise the possible climatic situations

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

3.4 Threats

3.4.1 Systems technologies versus enabling technologies

The risk of capability-based research and an integrated approach is the over-emphasis of systems technologies and consequently, the lack of focus on enabling or underpinning technologies and basic research.

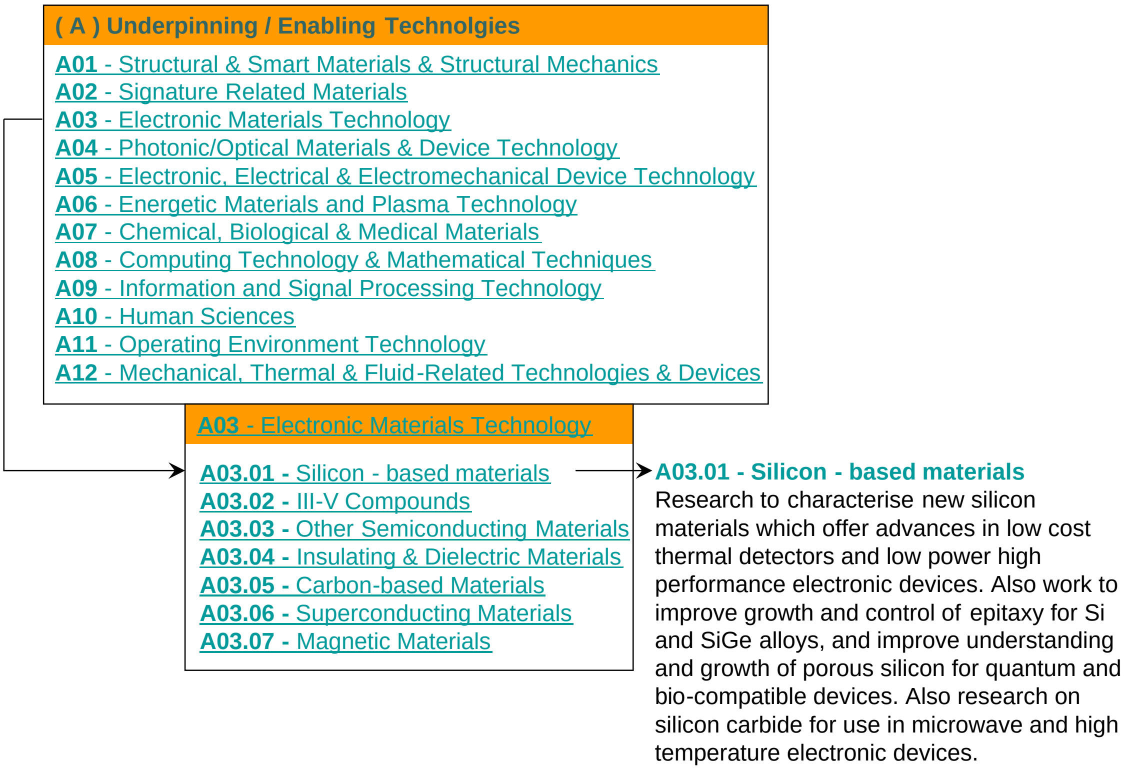
This threat of over-emphasising system technology is not only real for security-related research activities. It also constitutes a very relevant problem in defence-related research activities and even for the last evolutions in civil-related research activities.

E.g. the concept of Integrated Projects (FPVI): *Integrated Projects are based on a "programme approach" 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 to achieve ambitious objectives (objective-driven research).*[1]

Although their research activities may cover the whole research spectrum from basic to applied research, the tendency is for these IP to evolve from objective-driven research into system-driven research, in particular in those IP where demonstration activities are part of the project.

[1] European Commission – Classification of the FP6 Instruments – Detailed description.

Enabling or underpinning technologies are those technologies that are fundamental and necessary for the building of systems. The UK MOD taxonomy identifies the underpinning / enabling technologies to be:



(A) Underpinning / Enabling Technolgies

A01 - Structural & Smart Materials & Structural Mechanics
A02 - Signature Related Materials
A03 - Electronic Materials Technology
A04 - Photonic/Optical Materials & Device Technology
A05 - Electronic, Electrical & Electromechanical Device Technology
A06 - Energetic Materials and Plasma Technology
A07 - Chemical, Biological & Medical Materials
A08 - Computing Technology & Mathematical Techniques
A09 - Information and Signal Processing Technology
A10 - Human Sciences
A11 - Operating Environment Technology
A12 - Mechanical, Thermal & Fluid-Related Technologies & Devices

A03 - Electronic Materials Technology

A03.01 - Silicon - based materials
A03.02 - III-V Compounds
A03.03 - Other Semiconducting Materials
A03.04 - Insulating & Dielectric Materials
A03.05 - Carbon-based Materials
A03.06 - Superconducting Materials
A03.07 - Magnetic Materials

A03.01 - Silicon - based materials
Research to characterise new silicon materials which offer advances in low cost thermal detectors and low power high performance electronic devices. Also work to improve growth and control of epitaxy for Si and SiGe alloys, and improve understanding and growth of porous silicon for quantum and bio-compatible devices. Also research on silicon carbide for use in microwave and high temperature electronic devices.

3.4.2 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 the individual. 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 will be a thin line of balance between security, liberty and justice and this thin 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 telecoms companies and internet 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 held. Worthwhile to note is that a recent proposal on this from UK and France faced much opposition from telecoms companies and the European Parliament since it was considered to be infringing on privacy. There will now be a Commission proposal for a directive.

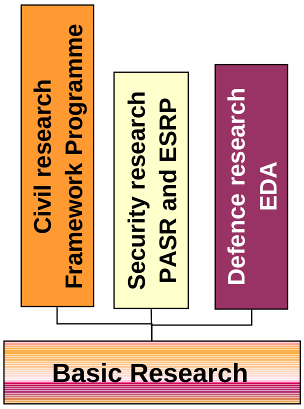
Privacy issues are also very popular in the domain of biometrics. Biometrics are techniques being used as a secure way of identifying an individual in a variety of applications worldwide. Biometrics are being used to improve security, such as making sure that only authorized people have access to facilities and information to prevent theft or to prevent 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 or a face or a voice. The information is then stored and later matched to verify the identity of people.

If biometrics are addressed, immediately the public's willingness to use biometrics needs to be considered as well and a number of relevant questions: which data are stored, where are these data stored, who as access to these data, what can the data be used for, etc?

3.5 Solutions

3.5.1 A "common" dedicated programme for basic research

In order to address the problem of increased need for prioritising capability- and system-oriented research, it is suggested to consider the establishment of a European basic research programme, from which the application- and system-oriented research programmes (FP, PASR, ESRP and defence research) could pull the relevant enabling technologies, as illustrated in the figure below.



Such an approach would allow to paying specific attention to enabling/underpinning technologies, examples of which have been described in section 3.4.

It is necessary though, in this context, to address the funding mechanisms for this programme. In basic research there should be sufficient opportunity to explore new technological areas, including technologies that may result in large application opportunities, but as well technologies with a high risk potential or very little visibility on what the application opportunities could be in the (distant) future. A funding mechanism which requires a (50%) participation in funding will not encourage the latter type of research and will hence leave major technology capability gaps.

3.5.2 Technology-watch and monitoring

Technological watch or technology monitoring is recognized to be a crucial activity for achieving and maintaining competitive positions in a rapidly evolving business environment. It serves the purpose of identification and assessment of 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 watch process/mechanism for the civil, security and defence community.

4 Cross-cutting issues

Security-related research is capability-based and mission-oriented. Its key research focuses relate to integrated different technologies, interoperability and converging technologies. All other key technology reports are of high relevance to the security-related report: bio-technology, nano-technology, research in the services sector, complexity and systemics, social sciences and humanities, cognitive science, agri-food and environmental technologies, energy technologies, ICT technologies, manufacturing technologies and transport-related research activities, as individual technologies but even more so as integrated.

5 Conclusions and recommendations

Science, research and technological development for security is ***capability-based research***. It is undertaken to support and facilitate the day-to-day work of people involved in security-related activities.

Although the European industry and research community has excellent skills to support and further develop their contribution to addressing the day-to-day security problems, the recent terrorist events and large-scale disasters show that these skills do not suffice to adequately and efficiently prevent these horrible events from happening and to protect human beings and their properties and assets against the catastrophic effects of them. In order to enhance competence and 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 require urgently 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 capability 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 capability. In NEC, the key word is interoperability and this at the level of respectively services (***human interoperability***), systems (***technical interoperability***) and information (***data interoperability***). ***Converging technologies*** are a key area to be explored.

The integration of systems has a large impact on the current way of testing, evaluation and certification. ***New test, evaluation and certification tools*** will need to be explored, in particular the use of simulation in the testing, evaluation and also at the (pre-) certification level.

In order to address the risk of capability-based research and an integrated approach to over-emphasise systems technologies and thereby not pay sufficient attention to enabling or underpinning technologies and basic research, it is recommended to consider the establishment of ***European basic research programme***, from which the application- and system-oriented research programmes (FP, PASR, ESRP and defence research) could pull the relevant enabling technologies. New funding-mechanisms 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 watch process/mechanism*** for the civil, security and defence community.