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

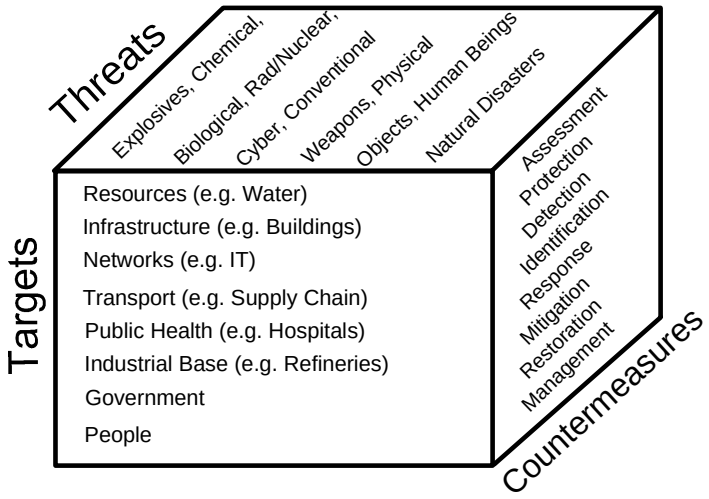
Commission Communication COM(2004) 72 defines security to be "an evolving concept" that "represents many challenges to the EU-25 that impact on a wide range of existing and emerging EU policies [and] citizens' concerns, including the protection against terrorist threats, and the adaptation of governance 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.

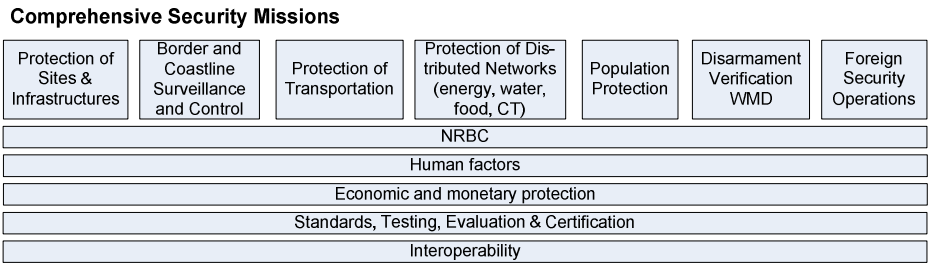
Standards for Security

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.

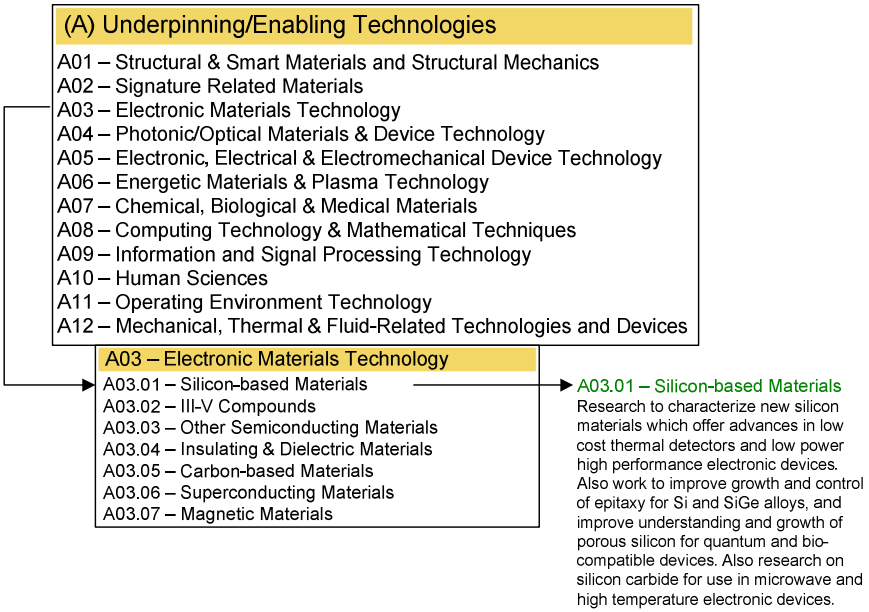
These data will have to be integrated in order to provide an adequate platform to test and evaluate systems according to the technical specifications and characteristics of the integrated systems in a simulation environment.

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.

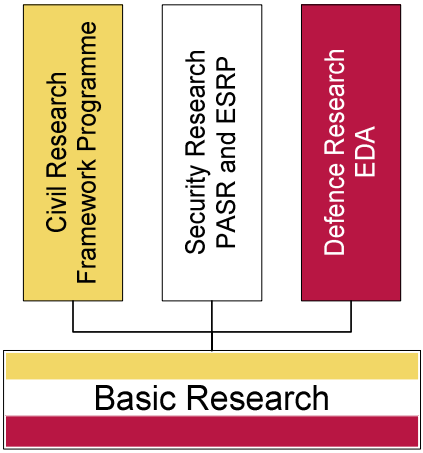
Privacy issues are also gaining prominence in the domain of biometrics. Biometrics are techniques being used as a secure way of identifying an individual through a variety of applications worldwide. Biometric data are being used to improve security, such as making sure that only authorized people have 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.

Border Security and Unmanned Aerial Vehicles

Jason Blazakis *

Summary

The use of Unmanned Aerial Vehicles (UAVs) to improve border security is a technique that has gained the attention of Congress. This report examines the strengths and limitations of deploying UAVs along the United States' borders and related issues for Congress. This report is not intended to provide in-depth information regarding the technical or military capabilities of UAVs, but rather to discuss their application in maintaining border security.

Background

Border security has long been recognized as a priority by the U.S. Congress. The northern border separating the mainland United States and Canada is 4,121 miles long, and consists of 430 official and unofficial ports of entry.[1] The expansive nature of the border and the possibility of entry through unpopulated regions make the border difficult to patrol. In July 2003, U.S. Customs and Border Protection (CBP) Commissioner Robert Bonner announced that an additional 375 border patrol agents would be reassigned to the U.S. border with Canada. This increase brought the number of agents deployed on this border to 1,000.[2] Commissioner Bonner also noted that CBP's border agents had "the front line responsibility for detecting terrorists and terrorist weapons."[3]

The southern border separating the United States and Mexico is 2,062 miles long, and consists of thirty ports of entry and "innumerable unofficial crossings."[4] In contrast to the United States' northern border, however, as of January 2003, more than 10,000 border patrol agents were stationed on the southern border. Despite this larger presence, covering a much shorter border, illegal border crossings and significant drug smuggling activities occur frequently.

In addition to being patrolled by border patrol agents, the borders are monitored and protected by video cameras, ground sensors, physical barriers, land vehicles, and manned aircraft. The diverse nature of U.S. border defense strategies is challenged by an equally diverse array of threats, ranging from terrorists to drug smugglers, arms dealers, and human traffickers. Past difficulties in securing the nation's borders, com-

---

* Jason Blazakis is an Analyst in Social Legislation in the Domestic Social Policy Division of the Congressional Research Service at the Library of Congress in Washington, D.C.

1 See *CIA World Factbook*, at www.cia.gov/cia/publications/factbook/geos/ca.html#Geo.

2 U.S. Customs and Border Protection, Office of the Commissioner, "CBP Assigns Additional Border Patrol Agents to Increase Northern Border Security," press release, 2 July 2003.

3 Ibid.

4 U.S. Congress, House Committee on Government Reform, *Federal Law Enforcement at the Borders and Ports of Entry: Challenges and Solutions*, 107th Congress, 2nd sess., H.Rept. 107294 (July 2002), 19.

bined with fears that terrorists could exploit existing security vulnerabilities by surreptitiously crossing the borders, has prompted Congress to call on the Department of Homeland Security (DHS) to examine the potential use of Unmanned Aerial Vehicles (UAVs).

UAVs are also known as drones, or remotely piloted vehicles (RPVs).[5] The Department of Defense defines a UAV as a powered aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry lethal or nonlethal payloads.[6] UAVs have played important roles in recent conflicts in Bosnia, Kosovo, Afghanistan, Pakistan, and both Gulf Wars.[7] Historically, UAVs have been utilized in various military settings outside of U.S. borders. For example, during Vietnam and the recent crises in the Balkans, UAVs provided real-time reconnaissance, surveillance, target acquisition, search and rescue services, and battle damage assessments.

UAV technology has also been applied domestically. The NASA-sponsored Environmental Research Aircraft and Sensor Technology (ERAST) program has produced civilian UAVs to monitor pollution and measure ozone levels.[8] Academic institutions have also been active in exploring civilian uses for UAVs. The Massachusetts Institute of Technology (MIT) is involved in developing Global Positioning Systems (GPS) and video camera guidance systems for locating and identifying toxic substances.[9] The Department of Energy has also announced that it will test UAVs outfitted with radiation sensors to detect potential nuclear reactor accidents.[10]

On 12 November 2003, Congress agreed to the Department of Defense (DoD) Authorization Conference Report (H.R. 1588), which became P.L. 108-354 on 24 November 2003. Section 1034 of the DoD Authorization Act requires the president to issue a report "on the use of unmanned aerial vehicles for support of homeland security missions." UAVs were recently tested for potential domestic application on the U.S.-Mexican border. UAV demonstrations conducted by various commercial companies at Fort Huachuca and Gila Bend, Arizona on behalf of the Department of Homeland Se-

---

5 It is important to note the distinction between drones and RPVs. Both drones and RPVs are pilotless, but drones are programmed for autonomous flight, whereas a ground control operator controls the flight pattern of an RPV.

6 United States Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: U.S. Department of Defense, April 2001), 557.

7 For a discussion regarding the military application of UAVs, see Elizabeth Bone and Christopher Bolkcom, *Unmanned Aerial Vehicles: Background and Issues for Congress*, CRS Report RL31872 (Washington, D.C.: Congressional Research Service, Library of Congress, 2003). For use of this technology by the Navy, see Ronald O'Rourke, *Unmanned Vehicles for U.S. Naval Forces: Background and Issues for Congress*, CRS Report RS21294 (Washington, D.C.: Congressional Research Service, Library of Congress, 2005).

8 More information regarding ERAST can be located at www.erast.com.

9 Hugh McDaid and David Oliver, *Smart Weapons* (New York: Barnes and Nobles Books, 1997), 9.

10 Jefferson Morris, "GoldenEye UAV to perform flight demo for DOE," *Aerospace Daily* (5 December 2003).

curity's Customs and Border Protection (CBP) Bureau have prompted various questions regarding their potential use within the United States. Shortly after the Arizona UAV demonstrations, DHS acknowledged that one model of UAV, the Predator B, would be used in Operation Safeguard, an experimental law enforcement program that will conduct missions along the U.S.-Mexican border.[11] P.L. 108-90, on appropriations for the Department of Homeland Security, provides USD 35.2 million to establish a Northern Border Airwing, of which USD 12.8 million will be available for aircraft procurement. In earmarking these funds, Congress supported functional and organizational air and marine interdiction (AMI) and modernization efforts. Congress also assigned the DHS Under-secretary of Border and Transportation Security to devise a report outlining operational plans by which the Air and Marine Operations Center (AMOC) would eliminate surveillance gaps affecting the northern border and western United States.

Benefits and Limitations of UAVs

One potential benefit of UAVs is that they could fill a void in current border surveillance. In particular, the unique technical capabilities of UAVs could improve coverage along remote sections of the United States' borders. Electro-optical identification technology is advanced enough that it can identify a potentially hostile target the size of a milk carton from an altitude of 60,000 feet.[12] UAVs can also provide precise and real-time imagery to a ground control operator, who would then disseminate that information so that informed decisions regarding the deployment of border patrol agents on the ground can be made quickly.

Another benefit of the UAV system is what is known as its loiter capabilities. The Predator B used in Operation Safeguard can fly for more than thirty hours without having to refuel.[13] The UAV's ability to loiter for prolonged periods of time has important operational advantages over manned aircraft. The longer flight times of UAVs mean that they are able to provide sustained coverage over a previously exposed area, which may improve border security.

UAVs are less expensive than other manned aircraft used on the borders. The unit cost of UAVs varies widely. The Shadow UAV costs USD 350,000, while the Predator costs USD 4.5 million.[14] In contrast, the unit cost of a P-3 manned aircraft used by U.S. Immigration and Customs Enforcement is USD 36 million. Black Hawk helicopters, which are frequently used on border patrol missions, cost USD 8.6 million per

[11] The Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) evaluated the Predator B used during Operation Safeguard, which began on 29 October 2003 and ended on 12 November 2003. Representatives from the General Atomics Corporation remotely piloted the Predator B during simulated night and daytime border demonstrations.

[12] Peter Hardin, "Eyes in the Skies," *Richmond Times-Dispatch* (30 October 2003), F1.

[13] For additional information regarding the Predator B's technical capabilities, see the General Atomics website at www.uav.com/products/predator_b_er.html.

[14] See Bone and Bolkcom, *Unmanned Aerial Vehicles*.

unit. However, the benefits of the Black Hawk's relative low unit cost are diminished by its lack of endurance. Black Hawks have a maximum flying time of 2 hours and 18 minutes.[15] Consequently, the longer flying time of unmanned aircraft would allow them to patrol the border longer—e.g., for an entire night—while reducing the overall number of missions flown.

The range of UAVs is a significant asset when compared to either border agents on patrol or stationery surveillance equipment. If an illegal border entrant attempts to transit through dense woods or mountainous terrain, UAVs would have a greater chance of tracking the violator with thermal detection sensors than would the stationary video equipment that is often used on the borders. It is important to note, however, that rough terrain and dense foliage can degrade the images produced by a UAV's sensory equipment, and thus limit their effectiveness on certain segments of the border. Another benefit is that the extended range and endurance of UAVs may lessen the burdens on human resources at the borders. During Operation Safeguard, the prototype Predator B RPV was remotely piloted from a ground control station. The safety concerns faced by helicopter pilots on patrol are eliminated when UAVs are used.

Despite the potential benefits of using UAVs for homeland security, various problems encountered in the past may hinder UAV implementation on the border. There are concerns regarding UAVs' high accident rate. Currently, the accident rate for UAVs is 100 times higher than that of manned aircraft.[16] Because UAV technology is still evolving, there is less redundancy built into the operating systems of UAVs than of manned aircraft; until redundant systems are perfected, mishap rates are expected to remain high. Additionally, if control systems fail in a manned aircraft, a well-trained pilot is better positioned to find the source of the problem because of his/her physical proximity. If a UAV encounters a similar system failure, or if a UAV landing is attempted during difficult weather conditions, the ground control pilot is at a disadvantage, because he or she is removed from the event. Unlike a pilot on board an aircraft, the remote pilot would not be able to assess important sensory information such as wind speed, runway conditions, etc.[17]

The key goal of Operation Safeguard was to identify potential threats crossing the southern border illegally. The surveillance capabilities of UAVs equipped with only an electro-optical camera and forward looking infrared radar (FLIR) sensor have been limited in the past by poor weather conditions. Cloudy conditions and high humidity climates can distort the imagery produced by electro-optical and FLIR equipment. Although the Predator B is operating primarily in the low-humidity environment of the Southwest, the effects of extreme climatic or atmospheric conditions on its sensors reportedly can be mitigated if DHS decides to outfit the Predator B with a synthetic ap-

---

[15] Paul Jackson, *Jane's All the World's Aircraft 2003-2004* (Alexandria, VA: Jane's Information Group, 2003), 721–22.

[16] Ibid.

[17] Amy Butler, "ACC Officials to Suggest Service Establish Five Predator Squadrons," *Inside the Air Force*, 7 June 2002.

erture radar (SAR) system.[18] These radar systems can produce high-resolution imagery in inclement weather. The ability of SAR to function during adverse weather conditions sets it apart from optical or infrared systems.[19] However, its ability to track moving targets is limited. This limitation can be mitigated by augmenting SAR with moving target indicator (MTI) radar technology. Adding SAR and MTI to the Predator B's platform could significantly enhance its operational capability for border missions. By adding SAR and MTI to the UAV platform, however, the costs of using UAVs on the border would increase.

How UAVs could be integrated into civilian airspace within the United States is a fundamental question that would need to be addressed by the Federal Aviation Administration (FAA) and DHS. Integrating UAVs into civilian airspace so that they can operate safely would require not only the creation of regulatory guidelines by the FAA, but also a variety of technical developments, primarily around safety issues. Currently, the FAA is working on guidelines for integrating UAVs into the national airspace. Although there are no guidelines or regulations for incorporating UAVs into domestic airspace, the FAA has worked closely with government users of UAV technology in developing a certificate of authority (COA) so that portions of airspace can be blocked off for exploratory development or operational testing. A primary concern of the FAA is whether UAVs can operate in already crowded airspace. The challenge, according to FAA spokesman William Shumann, is "to develop vehicles that meet FAA safety requirements if they want to fly in crowded airspace."[20] Before UAVs can be introduced into domestic U.S. airspace, the FAA, DHS, and other relevant technology users will need to address collision avoidance, communication, and weather avoidance issues.[21]

Issues for Congress

Congress will likely conduct oversight of Operation Safeguard before considering wider implementation of UAV technology. Additionally, the president's report to the Congress in April 2004 on the use of UAVs for support of homeland security missions should be useful to congressional evaluations, especially with respect to the tactical, early warning, and intelligence capabilities of this technology. If implemented, would UAVs simply be used to monitor the borders for illicit activity, or would they be util-

[18] According to General Atomics, the Predator B used during Operation Safeguard was equipped with electro-optical, FLIR, and SAR systems.

[19] For further information about synthetic aperture radar (SAR), see www.sandia.gov/radar/whatis.html. The SAR system used by some Predators is called the LYNX. The LYNX system can provide photographic images of up to four-inch resolution at a maximum altitude of 40 kilometers in fair weather. For more about the LYNX system, see www.ga.com/news/lynx_sar.html.

[20] Greta Wodele, "Firms to showcase unmanned planes for Border Patrol," *National Journal's Technology Daily* (11 August 2003).

[21] In November 2003, the FAA, DoD, NASA, and six private commercial companies launched Access Five, a five-year program to address the safety and technical concerns associated with using UAVs in domestic airspace.

ized in a more sophisticated manner? In the future, could UAV imagery be used to develop intelligence products on patterns and tactics used by illegal entrants?

If Congress concurs that UAVs can fulfill an important homeland security mission, how many UAVs would be needed to patrol the borders? A robust pilot program simultaneously testing multiple UAVs on the borders might be needed in order to ascertain where, how, and whether UAVs should be deployed. Larger-scale testing would provide an opportunity to evaluate whether the technical limitations of UAVs would hinder their utility on the border. In the past, multiple UAVs piloted in close proximity to each other have experienced interference and loss of control between the UAV and the remote pilot. In many cases, such interference led to accidents. An expanded pilot program would provide an opportunity to evaluate UAVs in a more realistic operational setting. Additionally, testing multiple UAVs on the borders could help in establishing parameters under which they could successfully operate.

The use of UAV technology on the northern and southern borders of the United States could potentially act as an important force multiplier by covering previously unpatrolled areas. This comparative advantage, however, may not be so significant when terrorists, like the September 11 hijackers, can enter the country through more easily accessible official ports of entry. Another consideration is how well—and how quickly—the CBP could respond to UAV imagery. Are there enough border patrol resources to investigate all targets identified by UAVs? Would the lack of human resources render high technology like UAVs less effective?

The technical capabilities of UAVs have been tested in a military context, but serious safety and technical issues need to be addressed if the program is to be expanded domestically. Perhaps most importantly, a clearly defined role and action plan for the application of UAV technology to homeland security needs would need to be created. If DHS moves forward with efforts to use UAVs in domestic airspace, both broad and technical issues will arise for congressional consideration. For example, will UAVs be more cost-effective or technically proficient in defending the borders than tethered aerostat radars (TARS), biometrics, more sophisticated ground sensor equipment, or additional border patrol agents? Until these questions are addressed, the utility of UAVs in helping to ensure U.S. border security will remain more speculative than practical.

Generational Change: Implications for the Development of Future Military Leaders

Paul Whelan *

In the last decade, the *raison d'être* of the international military environment has experienced a transition in scope and perspective. These changes in military perspective have an impact on the way the military interacts with both the professional and non-professional world within which it operates. Employee aspirations and attributes are evolving too. Today's employees exhibit values and aspirations different from their older generational counterparts. Both of these factors conspire to paint an altered and challenging landscape for the practice of leadership and management in the military in future years.

This paper will address the future of military leadership and management within the context of generational change among its management employees. It will outline this future in the context of the new and wider purpose of the Irish Defense Force. It will present current evidence gathered from the science of organizational behavior and management, and contrast this evidence with the model of training and socialization processes that the Irish military currently applies to cadets and newly commissioned officers, or more appropriately, the military managers of the future.

The Corporate Military

S.C. Sarkesian, a scholar of organization and management, has written that "all professions are corporate in nature."[1] Sarkesian, a former U.S. Army officer, argues that all corporations employ a system of bureaucracy and adhere to specific rules and regulations. He suggests that all professions embrace certain values, ethics, and ideals in the conduct of their business that are unique to each profession. They maintain standards of performance by which they gauge progress. Professions employ and mold their members to share in the common corporate goal of achieving legitimacy of purpose. Sarkesian posits that the modern military, as a profession, is substantially similar in concept to a corporation.[2] The models of practice outlined above could equally apply to the military as they do to a profession such as law or business. However, the understood role of the international military has changed dramatically from the roles that had been defined for it in previous decades. These changes are currently reflected in the

---

* Commandant Paul Whelan is a serving officer in the Irish Defense Forces, having just completed his country's Staff Course at the Command and Staff School, The Curragh, County Kildare, Ireland, and the Masters Degree in Leadership, Management and Defense Studies through the National University of Ireland. This is an edited version of his Masters' Thesis.

1 S.C. Sarkesian, *The Professional Army Officer in a Changing Society* (Chicago: Nelson Hall Publishers, 1975), 9.

2 Ibid., 10.

international security strategies of both the United States and Europe.[3] These changes have also been acknowledged in the Irish Defense Forces: "One thing that comes up in every discussion is the transformation process that seems to be ongoing in all forces today, and the fact that as transformation is ongoing, the operational demands are increasing and becoming more diverse and complex in nature."[4]

Essentially, the modifications of military purpose have had the effect of moving the military model even closer to that of a professional corporation.[5] For military formations internationally, the possibility and probability of participation in total war has declined. Instead, the prospect of involvement in total war has been replaced by a higher likelihood of joint participation in counter-terrorism efforts, low-intensity conflicts, limited wars, high technology information warfare, and a diverse array of peace operations. This new range of missions has brought about a necessary shift in focus for today's military organization. "The emphasis on technology and scientific knowledge has transformed the military from a parochial, inbred instrument of land battle to a highly sophisticated, multi functional organization closely linked to society."[6] Aligned with these changes of purpose, the military today are working in increasingly active cooperation with an ever-widening range of other military, non-military, and professional organizations. These circles may be political, civil, corporate, or non-governmental.

The Military's New Professional

A corollary of the organizational changes that are sweeping the cultures of both the corporation and the military is the idea that "employees are changing too."[7] Today's professionals embrace different values, attributes, and aspirations for their working lives when compared to their counterparts in earlier generations. They view the world differently from the way their parents might have viewed it. From an early age, today's generation of young and aspiring employees has recognized and mentally registered the trials and traumas confronted by their parents in an era when economies, politics, employment values, and employment rules were vastly different from today's.[8] They have grown up alongside technology and innovation and, having been exposed to computer technology from a young age, they are comfortable with change and motivated by technological advancement. They are inquisitive. They are generally well-traveled. Through modern approaches to parenting, and through more open and conscientious schooling, today's generation possess a better understanding and a better acceptance of

---

3 See George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: The White House, 2002),13; and *European Security Strategy* (2002), 3.

4 Lt. Gen. J. Sreenan, transcript of speech presented to the 62nd Command and Staff Course, The Curragh, County Kildare, Ireland (24 February 2006), 1.

5 Walter F. Ulmer, Jr., "Military Leadership into the 21st Century: 'Another Bridge Too Far?'" *Parameters* (Spring 1998): 6.

6 Sarkesian, *Professional Army Officer*, 8.

7 A. Kakabadse, J. Bank, and S. Vinnicombe, *Working in Organisations, The Essential Guide for Managers in Today's Workplace*, 2nd ed. (London: Penguin, 2005), 47.

8 Catherine Loughlin and Julian Barling, "Young Workers' Work Values, Attitudes, and Behaviors," *Journal of Occupational and Organizational Psychology* 74:4 (2001): 545.

different cultures, nations, and societies.[9] They therefore possess attributes and values that distinguish them from previous generations. This generation represents the newest entrants to the workplace, and is popularly referred to as "Generation Y."[10]

Personal Perspective

Since my commissioning in early 1991, I have held varied levels of responsibility for the selection, employment, and training of military cadets. I have spent the vast majority of my career training cadets and young officers in both the academic study of flight and in the skilled discipline of military flying itself. In that time I have witnessed a tangible transition in the type of person I am educating. During my early days of instructorship, when training someone to fly, I would always imagine myself in the student's place. By doing so, and by taking due cognizance of his or her capability, personality, and attitude, I felt able to deliver more considered, relevant, and effective instruction. I became more aware of the student's possible reactions, and the fact that these reactions would probably and usually coincide with my adopted position. I therefore became more capable of providing an appropriate response or reaction to situations or problems presented by the student.

As my experience as an instructor progressed, however, I found this process increasingly difficult to apply. I felt that a disconnection was taking place between my students and myself, and that this disparity, at least to me, was based on personality.

On mature reflection, the student and I were on diverging paths. I, fixed in my methods and responses, was moving further away from the student as the years passed and the faces changed. The student's attributes, attitudes, aspirations, and outlooks were becoming increasingly different from mine. The younger students were changing, and I remained firmly fixed in my generation, and therefore wedded to my methods of instruction.

The members of this younger generation are different people. They question and challenge professional direction more frequently. They actively seek considered and honest guidance, and despair when none is forthcoming. I learned that newer employees' initial career expectations could be thwarted by meaningless direction from their superiors. I also learned that the psychological contract that exists between employer and employee requires constant and considered attention at the employment entry phase and thereafter. Active and considered employee socialization processes, or "onboarding" efforts, on behalf of the new employer can serve to successfully guide the new employee toward a clearer and more considered approach to their new career.

What Is "Generational Change"?

Generations are defined not by a formal process, but rather by demographers, popular culture, the press and media, and even by the generations themselves. The differences

---

[9] R. Zemke, C. Raines, and B. Filipczak, *Generations at Work* (New York: AMACOM, 2000), 137.

[10] Bruce Tulgan and Carolyn Martin, *Managing Generation Y: Global Citizens Born in the Late Seventies and Early Eighties* (Boston: HRD Press, Inc., 2001), xi.

in personality experienced and recognized by organizations in their managers, both young and old, are categorized as "generational." The majority of literature emanating from the discipline of organizational behavior dealing with this topic of generational change is American in origin, and thus applies its focus to a Western style of organizational behavior. While slight discrepancies exist in the identification and categorization of the various generations, delineations have nevertheless been made in the literature that delineate the various generational cohort groups for the purposes of study.

In order to enable clarity of definition, I will begin with the "Silent Generation," as the portrayal of this generation allows more clearly definitive comparisons to be drawn when examining today's generation, Generation Y. Examining the two generations that reside between these extremities allows an appreciation of the evolution of the values attributed to Generation Y.

The Silent Generation

Most analysts date the birth of members of the Silent Generation between 1925 and 1942. Despite some debate about the exact dates, virtually all authors broadly agree on the attributes and values of this cohort group, as its members were influenced by the historical and social conditions of their time. Essentially, this generation is approaching or has already concluded its working life in the professional world. Some scholars have posited that the Silent Generation was the product of families that lived through the Great Depression, and that they were influenced by the difficulties that their parents faced to treasure employment and to be loyal employees, and by their parents' generation's service in the military during the Second World War to be command-oriented in the way that they managed their employees. The Silent Generation spent their early management careers in a post-war world that rarely, if ever, questioned authority, adhered to rather rigid chains of command, and observed a system of honor, subservience, and reverence for seniority. They are disciplined in that they are willing to accept poor direction, even when they know it to be flawed, and tend to tolerate it silently. They believe resolutely in law and order and are conservative by their nature.

The Baby Boomers

The birth years of the next generational cohort, known as the Baby Boomers, are usually held to be between 1943 and 1964. Particularly in the case of the United States, this generation was born into an era of rebellion and post-war national wealth, and their views were shaped by the emergence of the counterculture in the 1960s, the Vietnam War, and the Watergate scandal, all of which served to call into question established forms of authority. These trends would be mirrored in much of Europe, as in the 1968 student uprising in Paris. For this generation, authority appeared increasingly unreliable, an object of suspicion. They were further influenced by the styles of idealism proffered by emerging leaders such as Martin Luther King, Jr. and John F. Kennedy. According to one group of scholars, this cohort group believe in growth and expansion, take great pride in themselves as professionals, are optimists, are oriented towards

teamwork, and have "pursued their own personal gratification uncompromisingly, and often at a high price to themselves and others."[11]

Generation X

The next generational cohort, which has been dubbed Generation X, was born between 1960 and 1980. This generation lacked the experience of growing up through "real" wars that the two generations discussed above experienced. Members of Generation X are described by Zemke as being self-reliant, seeking a work–life balance and placing greater importance on family. Their approach to authority is casual and sometimes skeptical. They also possess a greater level of comfort with technology, having grown up in the computer age. Personal sacrifice for professional work advancement, which was so well practiced by older generations, has relatively little appeal for members of Generation X. "In a nutshell, they distrust hierarchy. They prefer more informal arrangements. They prefer to judge on merit rather than on status. They are far less loyal to their companies."[12]

Generation Y

A fourth group is now in evidence—Generation Y, or the "Millenials," a cohort made up of those born after 1980. This group is now making its presence felt within the professional world. Members of Generation Y are relative newcomers to the workforce, but early indications are that they are highly motivated and actively seek to improve their skills and abilities. They are not averse to questioning authority and, like the members of Generation X, lack permanent affiliation or commitment to their job. Martin, et al. describe this generation as one possessed with much aplomb. They are a "generation of new confidence, upbeat and full of self-esteem," perhaps not surprising as they "grew up basking in the 'decade of the child', a time when humanistic theories of childhood psychology permeated counseling, education and parenting."[13] They state that this period of psychological parenting has taken place under the cloud of isolation brought about by absentee double-income parents, often being raised by nannies or other non-parental caregivers. Generation Y has been brought up in environments that advocate that career-minded parents pursue their professional ambitions, while their children reside within a care environment or fend for themselves, independent of sustained parental presence and interest. By way of replacement, through access to vastly more information than was available to previous cohorts, this generation learns of the world's ills through the proliferation of electronic media.

These four generational dimensions, distinct and complete, are each products of the eras in which they grew up. Their values have been shaped and oriented according to the various political, environmental, and social backdrops to which they were exposed

[11] Ron Zemke, Claire Raines, and Bob Filipczak, *Generations at Work: Managing the Clash of Veterans, Boomers, Xers, and Nexters in Your Workplace* (New York: American Management Association, 1999), 67.

[12] Jay A. Conger, *Winning 'Em Over: A New Model for Management in the Age of Persuasion* (New York: Simon & Schuster, 2001), 9.

[13] Tulgan and Martin, *Managing Generation Y*, 4.

and against which they were raised; in turn, they defend and promote these virtues throughout their working lives. Generations are delineated by major world-historical events, such as the period of the Great Depression, the World Wars, Vietnam, cultural rebellion in the 1960s, the attacks of 9/11, etc. These events redefine ideology and social behavior; they are true "paradigm shifts," in that they reshape and alter people's intellectual approaches to the world.

Questioning Authority

The subject of generational value differences is important in the context of organizational behavior, in that it raises questions about generational conflict in management, management employee permanence, socialization processes, and a host of other issues. Sarkesian, writing of the civilianization of the military profession, remarks that it has "taken on the characteristics of a civilian profession, and in doing so has opened itself not only to reassessment and criticism by its own members but also by outsiders."[14] He refers to the organizational conflict that can arise between the older, more traditionalist officer and his younger subordinate. He states: "Traditionalists have a tendency to perpetuate the heroic role of the military, while the more modern and liberal professionals feel that the military must do more than manage violence."[15] Sarkesian highlighted this internal conflict in 1975, at a time when U.S. military focus was still centered on the Cold War.

More recently, an article written by Walter F. Ulmer, Jr. for the journal *Parameters* in the United States highlighted the issue again: "A survey sponsored by the Army Command and General Staff College in 1995 found some concerns about leadership and the command climate strikingly similar to those reported in the 1970 Army War College *Study on Military Professionalism*."[16] Ulmer continues, "Many senior service college students in recent classes seem to display more than typical student skepticism about the quality of senior leaders they have observed. Anecdotes about poor leadership, particularly at the field grade and general officer levels, are too persistent to ignore."[17]

In addition to highlighting various levels of dissent regarding elements of seniority, Ulmer in his article suggests that the increase in questioning of authority is linked to organizational changes associated with the modern military. He highlights the organizational qualities required in the officer ranks of today, in addition to the traditional traits and characteristics of leadership. He also notes the civilianization of the military, and calls for more effective work in the management of organizational change.

What both Sarkesian and Ulmer present, albeit only as part of their overall work, is evidence of the increasing tendency to question the viability of leadership and authority by military juniors or subordinates in the modern era. The time of unquestionable honor and reverence for leadership, as described by Conger in his appraisal of the Si-

[14] Sarkesian, *Professional Army Officer*, 14.
[15] Ibid.
[16] Ulmer, "Military Leadership into the 21st Century," 2.
[17] Ibid.

lent Generation, has passed. The new generations (both X and Y) do not simply accept direction out of obligation, and feel justified in seeking qualification, clarification, and justification for the orders they are given.

This questioning tendency is further developed in an article by Catherine Loughlin and Julian Barling. They suggest that, "Many young workers do not attach the same status to authority as previous generations, and there is now a pervasive cynicism about leadership and leaders."[18] It could be contended that "cynicism" in this context is a little harsh. It is possible that, through questioning, conflict and contradiction may emerge in the authority figure's qualifications, which in turn may disappoint the expectations of the questioner.

Practical Implications for Organizations

Kakabadse, et al. state: "The idea of a lifelong career in one company, quite common in the past, seems increasingly remote today." Today's new employees "develop new competencies and stay with an organization only as long as they find it challenging."[19] So what acknowledgement should organizations today make in recognition of the newer generational employee?

In his research paper and case study written on the generational implications of organizational behavior for the Australian Defense Forces (ADF), Bradley Jorgensen takes a critical look at the aspects of generational change. He tests the applicability of the hypothesis that generational issues should be accounted for in the design of workplace policy for the ADF. He acknowledges the differing approach to careers taken by Generations X and Y, paying particular attention to their inquisitive nature, their independence, their loyalty, and their skills and expertise in technology. He notes "that intention to leave increases markedly in line with educational attainment."[20] He notes in particular an attribute of the newest generation, in that the Generation Y cohort "values skill development and thrives on [the socialization aspect of] mentoring/coaching" and that, "like the Generation X cohort, they are motivated to do work but seek more direction and meaning in their work. They are not afraid to question authority, and will challenge management decisions that they deem unreasonable."[21]

This particular study by Jorgenson concludes: "The claims put forward by generational writers regarding the need to manage workforce through generationally-targeted mechanisms lack the necessary rigor on which to base workforce policy decisions. Rather, academic literature appears to support the notion of individualization and tailored measures rather than bulk or generic workforce policy approaches."[22] The recommendations proffered by Jorgenson, in my opinion, offer sound and qualified judgment. However, the recommendations may have been made in the knowledge that ex-

---

[18] Loughlin and Barling, "Young Workers' Work Values, Attitudes, and Behaviors," 551–52.

[19] Kakabadse, et al., *Working in Organisations*, 46–47.

[20] Bradley Jorgensen, "Baby Boomers, Generation X, and Generation Y: Policy Implications for Defence Forces in the Modern Era," *Foresight* 5:4 (2003).

[21] Ibid., 4; Tulgan and Martin, cited in Jorgenson.

[22] Jorgenson, "Baby Boomers."

isting training, management, and socialization techniques in the ADF already calculate to a large extent for generational difference. The reference to "individualization" is important, as it raises the issue of the socialization and mentoring of employees both on and after initial employment. This is the period during which notional expectations of employment on the part of both the employer and the employee are either confirmed or undermined, and may present a valuable tool toward determining employee career dedication and career permanence.

Ulmer states that, in relation to the U.S. military, there presently are "no highly visible, heavily resourced efforts to define, inculcate and monitor the creation and sustainment of organizational climates that challenge, inspire, and motivate all ranks."[23] According to Ulmer, the practice of mentoring in the military is restricted to the annual "Officer Efficiency Report," which he finds to be insufficient. Organizational best practices in the area of "developmental feedback and monitoring," he concludes, have left the military behind.[24]

The Socialization Process

In essence, the aforementioned body of literature provides an overview of the change in the military's approach to the newer generations (X and Y) and their employment. These generational cohorts utilize a different approach to authority than their predecessors, the Silent Generation and, to a lesser extent, the Baby Boomers. Issues of generational conflict are highlighted in the wish by newer generations to constantly seek direction, qualification, and purpose from their employers. This quest, from my own experience, is conducted unashamedly and with ample merit.

One method of guiding new employees through the mist of the first stages of a new position is through the utilization of considered socialization techniques. Socialization, whether consciously or not, is a method used by the Irish Defense Forces to extend the training acquired through the Cadet School and apply this training to employment practice. While socialization within the Irish military is not currently a discretely identified process after a cadet's commissioning—that is, it is not monitored or controlled by any training or management body—it can and does form a vital component of the individual's induction into the organization. It also makes a definite and lasting impression upon the employee.

As stated at the beginning of this paper, military employees are involved now more than ever with a widening circle of military, non-military, and civilian organizations.[25] The emphasis of such contact has shifted away from one directed toward purely military objectives. This diversification of professional contact requires that military offi-

---

[23] Ulmer, "Military Leadership into the 21st Century," 6.

[24] Ibid.

[25] See Sarkesian, *Professional Army Officer*; Ulmer, "Military Leadership into the 21st Century"; and M. Vlachova and L. Halberstat, "A Casual View into the Future: Reform of Military Education in the Czech Republic," *Geneva Centre for the Democratic Control of Armed Forces*, Working Paper No. 105 (2003); at www.dcaf.ch/publications/Working_Papers/105.pdf (accessed on 2 December 2005).

cers and personnel be equipped professionally with the wider relationship skills required for such associations. Effective socialization processes through peer or superior mentoring can serve to foster and develop appreciation of the skilled requirements of diplomacy.

Through socialization, the initial expectations of the employee are tested against the reality of the job, and a tentative adjustment in attitude and behavior can then take place.[26] Initial military training falls under the category of "divestiture" in socialization terms.[27] Through divestiture, one tries to deny and/or change the identity of the newcomer. There follow, then, two methods of socialization, as proposed by Ardts, et al.:

- Institutionalized socialization and personnel instruments
- Individualized socialization and personnel instruments.

Institutionalized methods of socialization are selected "when one wants conformist newcomers that have little intention to leave the company, that are loyal and emotionally committed to the organization."[28] This is a method of formalized socialization. The method or program makes use of a mentor or role model, and aims toward the affirmation of the new employee's own identity and quality.

Individualized methods of socialization are selected "when one wants innovative newcomers, and does not want to offer them a job for life, and if one is less concerned about newcomers that are loyal and that feel emotionally attached to the organization."[29] This method does not employ a mentor to facilitate the process. It may be done on an ad hoc basis, without clearly defined steps and without a predetermined time frame.

Allowing that there is no clearly established method or framework of socialization recognized and undertaken by the Irish military after commissioning (with the exception of the AF451, the Officer's Annual Performance Appraisal), it follows that the IDF utilizes individualized socialization methods after the period of initial military training. In theory, then, the employee is allowed to construct their own understanding of the organization based on their own immediate experience, which in an organization as diverse as a nation's military can serve to undermine the previous beliefs and/or career expectations of the employee and thwart their potential for self-actualization.

Indications

The need for a high level of intellectual capability within the military will not diminish. In order to maintain and embellish both its self-image and its image with respect to society—especially while cooperation with society increases in response to a widening of the military's roles—education must be high on the military agenda. The forces of history and societal evolution have presented a new variant of generational cohort who

[26] See Kakabadse, et al., *Working in Organisations*.
[27] J. Ardts, P. Jansen, and M. van der Velde, "The Breaking in of New Employees," *Journal of Management Development* 20:2 (2001): 159–67.
[28] Ibid., 163.
[29] Ibid.

will fulfill the duties of management well into the future. However, Generations X and Y are somewhat fickle cohorts. The psychological requirement for self-improvement exhibited by these generations reflects the motivational theories of Maslow, but qualifies even further the "needs" theories of Alderfer, in that, "If a need is consistently frustrated, an individual 'regresses' to being motivated by lower-order needs that are already being fulfilled to a sufficient degree."[30]

Studies in organizational psychology and behavior have identified the aspirations and values of the new employee/managers of the future, Generation Y. They are an impressive generation. They symbolize the progressive, inquisitive qualities that qualify general evolutionary thought. They require honest and meaningful direction, and they seek it voraciously.

Generation Y's inquisitive nature, however, is amplified by a marked reluctance to simply adhere to direction and authority without question. Direction and authority must be both qualified and justified. This questioning of leadership is readily identified in youth society today, and is equally apparent within the military environment. New generations of employees, while lacking the kind of career permanence that their Silent Generation predecessors possessed, will nevertheless relish organizational systems of training and socialization that serve to satisfy the intangibility of career expectation. Effective and meaningful socialization techniques can serve to assist development processes while diminishing career apathy and unmet expectations among newer employees.

Is it possible, however, that older generations will always view younger generations as being "difficult to deal with," "argumentative," and as "having no persistence," not just in relation to their careers but to all undertakings? The quality of an even, consistent pace has always been associated with older generations, who are thought to prefer to control, manage, and maintain their affairs carefully and deliberately. The converse has always been imputed to younger generations, with the assumption being that they prefer to take risks and seize opportunities as they arise. Criticisms relating to younger generations are not a new phenomenon, and can be traced back (at least) to ancient Egyptian manuscripts. Is it possible, though, that the theories that define generational change are simply an attempt to psychologically categorize what has been known throughout history? Jorgenson posits this possibility in his assessment of generational change effects and their implications for the ADF. In any assessment of generational change, however, credence must be given to the societal and historical background from which the different generations grew. Today's new employees are the products of a society that possesses values that are markedly different from those of their parents.

The previous focus within military organizations on roles that are purely focused on military tasks, narrowly defined, is being quickly replaced by new and widening liai-

[30] See A. H. Maslow, *Motivation of Personality* (New York: Harper and Row, 1954); and C. P. Alderfer, *Existence, Relatedness and Growth: Human Needs in Organizational Settings* (Boston: Free Press, 1972). Quote from Alderfer, cited in M. Morley, S. Moore, N. Heraty, M. Linehan, and S. MacCurtain, *Principles of Organisational Behaviour, An Irish Text*, 2nd ed. (Dublin: Gill & Macmillan, 2004).

sons that require new levels of professionalism. The lines of demarcation are being rewritten, and as the military diversifies into its new roles, the training and socialization of new employees needs to reflect the levels of managerial professionalism required to meet the military's new missions. Examining the motivations and future expectations of these new employees may provide a valuable insight into the aspirations of the military manager of the future.

The theory of generational change holds that today's employee, a member of Generation Y, displays different aspirations and attitudes in his/her approach to work and life than did members of earlier generations. Do the Irish Defense Forces therefore need to alter their approach to accommodate this difference, in terms of its methods of training and its practices of socialization?

Square Pegs and Round Holes

When reflecting on the lives of past generations, one tends to reflect on the qualities, the characteristics, and the tempo of the era in question. Life almost always appears to have been simpler in the past compared to the present. This simple reflective practice applies to all generations. When I began this thesis, I did so in the assured knowledge that the cohort I had identified, Generation Y, was somehow removed from me psychologically, and that their lives certainly reflected complicated influences that were unknown to me in my own formative years. Would it be feasible or even possible, however, to use an American model of generational delineation as a framework within which to evaluate an Irish generational equivalent in terms of chronological placement, attitudes, and traits? In my journey through the construction of this thesis, I have learned that the practice of attaching concrete rules and codes of behavior to an identified group of people can quickly become problematic. In many ways, deeply demographic studies amplify modern values in teaching us that no single, definitive scientific truth may be applied in its totality to the study of a complete generation. As Ryder summarizes, "It is invalid to transform a proposition about populations into a proposition about individuals."[31] The application, however, of a "simplification of values" that encompasses the expected attributes of a given generation, a generality of traits that distinguish one generation from another, can be constructive in the evaluation of predicted impacts upon society and, through more focused application, upon organizations.

Messages that Motivate

The Irish Defense Forces today coexists with a highly competitive corporate environment in which the institution of human resource management has emerged as an element of critical organizational importance. Human resource management recognizes that today's generation of employees exhibits fundamentally different values and attitudes to those of predecessor generations, and that they bring with them clear and un-

[31] N. Ryder, "Notes on the Concept of a Population," *American Journal of Sociology*, 69 (1964): 459.

ambiguous intentions for their future. If the IDF has an advantage over corporate career alternatives, it resides in the fact that today's cadet/employee chooses to serve their country in a career that promises and advocates continual challenge. It becomes evident from my research that this challenge is met during cadet training, as exhibited by the assured confidence of cadet participant responses. Developments demonstrated within the cadet training environment and within the socialization methods employed by the Human Resources Section of the Defense Forces, whether intentional or not, have served to meet the needs of Generation Y. The expectation of continued challenge by new cadets is also evident, and it is quietly assumed that the IDF will continuously provide meaning and direction in the form of active and considered socialization processes that will define, support, and nurture these expectations. The Irish military, much like its corporate peers, exists in an environment of changing visions, policies, and objectives. This is particularly true not just in the aims of the organization, but also in the conditions under which it employs and maintains its employees.

The effective propagation of the policies and purposes of the Irish Defense Forces relies on the continued effectiveness of its employees. An enlightened productivity may be achieved if employee potential is considerately nurtured right from the beginning: "The more effective and efficient the socialization, the sooner a newcomer can be productive for the organization."[32] The individualized socialization method currently adopted by the IDF post-commissioning does not effectively embrace the dynamism of Generation Y in a way that inculcates and encourages the possibilities that this generation brings to bear. Members of Generation Y require qualified direction that enables the expectations of the organization to be set unambiguously. Once the expectations are set, the organizational goal is clarified, and the ability to measure performance is heightened. If the expectations of the new employee are not frequently clarified and qualified, the resultant ambiguity will disappoint and disillusion the cohort. Members of Generation Y embrace the prospect of challenge in a way that distinguishes them from previous generations, and underpins their choice of career path. According to Grainne Cullen, the attraction towards personal challenge appears more prevalent through interviews among those members of Generation Y who aspire to a career in the military as opposed to a career outside the military.[33] Cullen highlights a surprising statistic from her research, in which she asked sixty cadet applicants what other career path they would pursue if they failed to achieve a cadetship. Almost fifty percent responded that they would pursue an entrepreneurial career path over the more stable and possibly expected civil, security, or banking environments.[34]

---

[32] Ardts, et al., "The Breaking in of New Employees."

[33] Grainne Cullen, a psychologist working with the Irish Defense Forces, was interviewed by the author. All quotations here and below are taken from the author's records and notes from the interview.

[34] Twenty-eight prospective Cadets chose an entrepreneurial career path as their preference should they be unsuccessful in their attempt to join the IDF. The choice of entrepreneur was not listed among the career alternative options, but rather was independently written in under the option "Other Careers."

Why? The Benefits of Questioning

Members of Generation Y will question everything. This is a natural progression from an upbringing that permits and encourages such inquisitiveness. It is a method through which clarity of purpose is identified and security of purpose is ensured. It is a quality, though, that in an organization such as the military may serve to undermine older views of obedience and respect for authority. However, it is a practice that for this generation assures continued and unabridged application to task. If the ability to openly question orders is removed, so too is the confidence and assuredness of the employee. Through questioning authority, the ability of the employee to confidently dispel ambiguity preserves the motivation to complete the task at hand and confidently justify the resultant product. This questioning trait is not something limited to Generation Y, but rather is a quality that has naturally evolved with society. Older generations may have been more capable of tempering the desire to question, based on the situation and on the audience. Hence, this questioning phenomenon is reasonably new to the military. To Generation Y, however, questioning is a quality that is ingrained within the person, something that life has taught them should be practiced regardless of the weight or authority of the recipient. It is not done out of malice, but rather is well-intentioned and whole-heartedly justified in the eyes of the questioner.

The encouragement of questioning within the military can only serve to improve the transparency and legitimacy of what has traditionally been a hierarchical and bureaucratic structure. It cannot be ignored, though, that the latitude and flexibility that allow such a trait to openly express itself do not survive within the rigid chains of command that embody the military ethos. The military is possibly one of the last remaining organizational structures in which flexibility with regard to the questioning of authority cannot apply through all levels of the hierarchy. One aspect of a changing military, however, resides within the remit of operational planning processes for crisis management operations, in which the active encouragement of questioning ensures that all potential military responses are rigorously tested for every eventuality. The value of questioning in an open environment cannot be underestimated, and creating latitude for its productive employment within the confines of the employee's immediate environment should be embraced. Again, to cite Cullen, it is through questioning authority that one questions the organization, and it is only through questioning the organization that you enable organizational change. A future study based on this generation's progression might allow an evaluation of any correlation that might exist between rapid organizational change and the openness of that organization to employee inquisitiveness. Certainly, organizations today have achieved great success through open promotion of "flatter," less hierarchical management structures that actively encourage such a practice.

It follows that the questioning tendency inherent in Generation Y will be a by-product of the new employee's attempts to proactively influence their own adjustment to their new work environment. Questioning is a method of self-socialization, which serves to elicit information about the new employee's environment. Studies show that "newcomers who frequently seek information and ask for feedback have more knowl-

edge of the job and of the organization, and are more socially integrated."[35] The employee's formative years within any organization are a hugely important period of adjustment, in which the initial promises of the career are either fulfilled or belied. In organizations that have adopted institutionalized methods of socialization, this is the period where mentoring or coaching is deployed and aimed at "the affirmation of the newcomer's own identity and quality."[36] The indicated expectancy of some form of coaching on and after job commencement by the researched cadet group highlights a desire for methods of socialization that the IDF does not undertake as a formal practice. Coaching and/or mentoring is not a recognized pursuit within the Irish military, and when it is performed, while beneficial, it is entirely unregulated and informal. The annual performance appraisal system remains the sole mechanism whereby employees gain an insight into the level of their own performance against what is required or expected. Coaching and mentoring as a recognized organizational practice can serve to nurture this confident generation's aspirations, dispel ambiguities, and promote the levels of professionalism so strenuously demanded by today's changing military. The practice may serve to bridge the apparent disconnection between older military generations and the new cohort. It will serve to satisfy the insatiable questioning trait, and ultimately promote the career perseverance of members of Generation Y.

Parallel Study Possibilities

A factor that cannot be overlooked when debating the implications of generational change for organizations is whether or not work values remain constant throughout employment, or if in fact they change as employees mature into their chosen careers. Every employee will commence their career with pre-planned priorities and aspirations, but do these values change in consonance or dissonance with their employment? Are these values more influenced by generational experiences, or by age and maturation? Does the issue of work-life balance, so important to newer generations, imply that this factor alone will dictate employment values in future years? The issue of the achievement of a balanced lifestyle permeates Irish society today, and has become a necessary focus for the continued viability of commercial organizations. Given the nature and necessarily unique culture of the Irish Defense Forces, what adjustments (if any) can be made to accommodate the future requirements of the IDF's employees?

Conclusion

The Irish Defense Forces places great emphasis on the procedures and mechanisms employed in the recruitment and selection of prospective officers. The selection process is both rigorous and demanding, and is designed to identify those persons who possess the myriad qualities that define the ethos of military leadership and management. The process produces that small percentage of those persons who display the desired requirements, the "cream of the crop," as it were. The career motivations of today's

[35] Ardts, et al., "The Breaking in of New Employees."
[36] Ibid.

generation are generally more focused and calculated than those of previous generations. The successful lure resides within the career that offers diversity and consistency of challenge. The attraction is not the safe and secure, pensionable job that provides a reasonably comfortable refuge in less economically prosperous times. The problem now for the military consists in the maintenance of that challenge on and after commissioning. Career permanence is not as powerful a value as it once was. Thus, it is the retention of the engagement of the employee that now more than ever defines the challenge for the Irish Defense Forces.

It can be argued that youthful exuberance and motivation will always indicate a desire to change occupational course when occupational challenges fail to materialize. Certainly, as generations progress and mature, and their familial and financial responsibilities increase, their values may change, and occupational security can become paramount. Today's society, however, advocates occupational change as a natural matter of course. The robust state of the Irish economy has allowed the employee to become a valuable commodity, to be traded and upgraded across the spectrum of career opportunities that present themselves. Furthermore, previous studies have illustrated that "work values are more influenced by generational experiences than by age and maturation."[37]

As one generation learns from its mistakes, these lessons are passed on to the next generation. The ideal for all generations, though, is to ultimately achieve the "life fully worth living."[38] The members of Generation Y represent the workforce of the future. As modern progressive organizations embrace the use of psychological evaluation to assess and understand the motivations of their employees, and then seek to exceed them throughout their careers, so too should the military. In an age where the challenges facing the Irish Defense Forces are diversifying, the requirement to embrace employee values that in turn thrive on challenge is paramount to the successful achievement of organizational vision. Generation Y will meet and even exceed these challenges in an environment that recognizes, respects, and accedes to its needs.

---

[37] K.W. Smola and C.D. Sutton, "Generational Differences: Revisiting Generational Work Values for the New Millennium," *Journal of Organizational Behavior* 23 (2002): 379.

[38] H.A. Shepherd, "On the Realization of Human Potential: A Path with a Heart," in *The Organizational Behavior Reader,* 7th ed. (Englewood Cliffs, NJ: Prentice Hall, 2001), 146.