Food for Thought Paper on H2020

prepared by SERIT (SEcurity Research in ITaly)

Introduction

The evolution of the complex scenario concerning the different aspects of Security is reflected by the attention and interest of a growing audience of academic and industrial researchers towards SERIT (Security Research in Italy – www.piattaformaserit.it), the Italian technological platform acting in security which gathers today more than 300 organizations and an increasing number of security experts that participate in all its activities.

SERIT, a joint initiative launched by CNR and Finmeccanica, brings together Italian industries (both large industries and SMEs), academia, research centers and end-users, in order to promote and develop a National Research Agenda to drive the future technological developments, while answering to the identified National Security needs. To this aim, SERIT has been originally structured in Leading-Sectors (representing the different area where Security needs to be investigated in Italy) and Technological Areas (identifying the technological priorities).

Within this role, SERIT aims to reinforce the networking among national researchers, industries, end-users and institution's representatives, allowing them to cooperate on common interest projects, to activate public-private partnerships and to strengthen national and international participation to research programs (including National research/national cluster activities and Horizon 2020).

In line with the goals and the future issues of the European Commission, the platform has been recently restructured to be more compliant with the issues launched by Europe for the next Framework Programme Horizon 2020, by proposing a new mapping and an appropriate aggregation of the leading sectors as well as a definition of new technological areas that are compliant with those who are the main drivers of Europe, without losing the original features in the application domains that reflect the national needs in terms of Security.

Considering the fact that the first H2020 ‘call for proposals’ might be launched in the beginning of 2014, it appears urgent to concentrate on the content aspects and to come up with some proposals towards the future European security research programme, in particular for the Work Programme 2014-2016.

Recalling the current preliminary state of H2020, this food for thought paper provides recommendations for the execution of the next phase of security research. These

recommendations are drawn from conclusions and experiences gathered in SERIT Platform.

The purpose of this publication is to present and describe those national needs mapped according to the priorities identified by European Commission, in order to present a roadmap for future research activities and to propose a list of projects for the related developments, also identifying the lighthouse projects acting as main achievements in the corresponding areas.

In particular we refer to the last available proposals from Commission, Council and Parliament and the specific themes we addressed are:

III Societal challenges, 6a. Secure societies – protecting freedom and security of Europe and its citizens

(a) fight crime and terrorism;

(b) protect and improve resilience of critical infrastructures;

(c) strengthen security through border management and maritime security;

(d) provide cyber security;

(e) increase Europe's resilience to crises and disasters;

(f) enhance the societal dimension of security and ensure privacy and freedom in the Internet;

(g) support the Union's internal and external security policies;

(h) strengthen security and the transformation of conflicts within third countries through conflict prevention, peace-building, dialogue, mediation and reconciliation and civilian security sector reform;

(i) enhance standardization and interoperability;

III Societal challenges, 3. Secure, clean and efficient energy

3.1.3. Foster European Smart cities and Communities

III Societal challenges, 5. Climate Action, Resource Efficiency and Raw Materials

5.6. Cultural heritage

III Societal challenges, 6a. Secure societies – protecting freedom and security of Europe and its citizens

a) Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs

H2020 Text:

"Work on data analysis should be continued (with focus on criminal activities, smuggling, money laundering, etc.), but here as well with a focus on standardisation effort of collected data to allow interoperability, exchange and operation at European level. Work on sensors should be more focused in the future on the supporting technology to be used in various scenarios (explosive, drugs, other chemical or bio hazards)."

Introduction

Organized Crime is spreading at an accelerated rhythm all along the world and in most of the European countries they are becoming an highly critical phenomenon. FP7 has already produced a number of technological innovations to supply new technologies, especially in the scope of the "Security of Citizens" mission. Under this umbrella the development of tools to support the different phases of crime fight have been started: surveillance systems, early warning devices, unmanned platforms, advanced and more sensitive detectors for the identification of forbidden or dangerous substances have been investigated.

Common procedures for the fight crime include well distinguished phases:

- Prevention;
- Direct Fight and event countermeasures;
- Analysis and Investigations;

Two of these phases, namely prevention and investigations, demands for a large cooperation among all the European authorities considering that the crime actions are nowadays largely over-nationals and the commitment, the preparation and the execution of the crime are more and more performed in different countries.

Italy is historically a target of organized crime and the methodologies for the fight against this plague have been refined more than in other countries. A number of technology producers are also operating at an excellence level on the national territory, coping with the most refined investigation procedures. Funding this kind of programs become then

central to improve their competitiveness, but also to increase the cooperation level with similar operators in the other European countries. The national presence is also important in ambitious CBRN demo (EDEN) that will start in early 2013 and has the aim to develop and establish a wide and open CBRN equipment and services online platform and store with direct access for suppliers (Industry, SMEs), users (CBRN operators and authorities) and RTOs (private/public).

The CBRNE area has contributed already to the mission of fighting crime and terrorism, in previous FPs. Yet, gaps in the applications and capabilities still need to be filled. One area which is largely underdeveloped is the surveillance and protection of environmental resources, which impact at large different sectors of everyday life: for example, food production and energy production, but also recreation and culture, welfare, health. New research needs for the development of Early Warning Systems require the applicability of current CBRNE detection systems to a continuous and capillary monitoring of these resources, often remote and secluded. Many of the technologies applied for CBRNE detection are highly effective in controlled conditions, laboratories, uniform environments. Their application in field conditions require therefore further development in some critical aspects, including: (i) miniaturization; (ii) autonomy in power supply; (iii) possibility of diagnostics about correct functioning and self-repair; (iv) automatic sampling or data acquisition; (v) unmanned operation; (vi) networked connections with data fusion; (vii) resilience towards confounding factors and environmental disturbance; (viii) qualitative and quantitative data elaboration.

A peculiar area that should also be taken into account is the prevention of attacks that seriously threats the citizen security by means of modifications of the food chain: what that is called “food terrorism”. Organized crime can take advantage of this opportunity not only to menace the community, but especially to found new sources of illicit gains by means of the unsafe food and, what is also crucial, acting on the tampering of health products that become uncontrolled, unsafe, with direct and indirect threats for the citizen safety. Develop new technologies for monitoring agri-environmental resources remotely and for deployment of in-field rapid diagnostic techniques to measure the level of agri-environmental disruption after disasters. Develop surveillance systems in the food industries to monitor hostile tampering behaviors during agricultural and food processes.

What needs to be done

Within the past work of SERIT platform a number of technological areas that impact on the mission of organized crime fighting has been identified:

1. Surveillance & Situation Awareness;
2. Detection and Identification Systems;
3. Crisis Management and citizen protection technologies, asset and infrastructures;
4. Information Processing and Management;
5. Chemical Biological Nuclear Explosion threats;

Focus will be on the following capabilities that comes from the items addressed by the security Italian community, and that should be developed at local, regional, national and European level.

Develop tools to support interoperability to exchange data among the different Law Enforcement agencies, share applications, use common user interfaces to fight against crime projects (definition and adoption of common ontologies, data and protocols standardizations, interoperable processing tools)
This objective is especially crossed by The 'Information Processing and Management' technology area that feeds the research begin from data fusion, classification and analysis algorithms and developing a software infrastructure based on modern ICT technologies such as:

- Cloud Computing,
- Semantic Web
- Authentication system,
- Resilience and Quality of Service

These infrastructures are needed to realize a number of resources available to Law Enforcement Agencies allowing them to easily work together with colleagues across borders in terms of definition and adoption of a common ontology for the domains of interest, of exchanges of standardized data, of exploitation of common or compatible tools and processes needed to achieve their missions.
The information infrastructure shall guarantee the information and network protection against Cyber attacks and enhance and even enforce the standardization and interoperability for data, procedures and information and data processing tools to improve cooperation.

Foster the development of intelligent sensing subsystem, improving the transportability level, reducing in size critical technologies endowed with networking connection with intelligent data fusion centers able to identify critical alarms combinations
To fulfill this objective, the 'Surveillance & Situation Awareness" technology area feeds the research theme by means of the enabling technology of MEMS (Micro Electromechanical Systems), of data fusion, of data classification and analysis algorithms. The reference architectures should be based on pillars like:

- Cloud Computing,

- Hybrid Computing, High Performance Computing
- Wide scale multisensor surveillance systems

Another fundamental contribution to the addressed objective comes from the 'Detection & Identification Systems" technology area that feeds the research theme by means of the enabling technology of Ionic mobility, X and Gamma rays, TeraHertz technology, data fusion, data classification and analysis algorithms, developing a software infrastructure necessary to realize a system to detect and identification intruders and analyze the anomalous behavior and alarm detection
Crisis Management and citizen protection technologies feeds the research themes coming from X and Gamma rays technology, data fusion and classification and analysis algorithms, developing a software infrastructure necessary to realize a sensors like fixed and mobile sensors to recognize the picture.
Sensors and unmanned platforms aims at wide multisensor surveillance systems, interoperable and able to collect information to C3I system.

Increase investigation capabilities in the area of forensics, in priority areas of Fire Arms and projectile identification, GSR (Gun Shot Residue), Ballistic, Explosion investigation and explosives, drug analysis and biometrics

Forensic is the application of a broad spectrum of science and technologies to investigate and establish facts of interest in relation to criminal or civil law. Forensic science covers many disciplines, such as biology, geology, chemistry, engineering, medicine, phonetics, computer science, among others. Therefore, this area is very complex and dynamic due to the confluence of the Society security needs and requirements, requests coming from the legal and institutional Systems.

The demand for a high-quality diagnostic is generally growing and technological advances are particularly important, as the design and manufacture of portable instruments and databases for fast and reliable diagnosis and precise identification of specific and characteristic specificity.

Priority research areas are identified in Fire Arms and projectile identification, GSR, Ballistic, Explosion investigation and explosives, drug analysis and biometrics. These research areas require the creation of data bases, image analysis, analysis of materials, development of new methods for detection, analysis of audio signal, and the development of protocols for forensic inspections.

Lighthouse projects

Lighthouse projects are normally perceived as projects with the explicit goal of accelerating changes in perceptions and beliefs on a wide scale. They are based on the scheme of large Demo projects, collecting most of the progresses achieved in previous H2020 or even FP7 projects. The following proposals, treated in this report at a very general level, are inspired to this vision.

First proposal : "Common action of European Agencies against the Crime"

Demo project on the cooperation among the European Law Enforcement Agencies exploiting advances in system and networking architectures, maintaining information assurance, confidentiality, reliability. Exploitation of data analysis tools, addressing interoperability standards, legal and ethical issues. The tackled problems also cover the need to select the information to be shared: this requires advanced organization of data bases, hiding information capability, protection technologies relevant to the system organization.

Second proposal: "Forensic technologies advances".

Demo project that collects the recent and future advances based on the available capabilities and excellences to implement new methodologies and protocols for investigations in the fields of Fire Arms and projectile identification, GSR, Ballistic, Explosion investigation and explosives, drug analysis and biometric analysis

Third proposal: "Multisensing platform for agro-environment monitoring"

Demo projects on multisensing platforms for monitoring agro-environmental resources towards deliberate attacks. Starting idea: what if recent outbreaks of Escherichia coli or Salmonella in food products had been determined by deliberate and fraudulent practices? The project should develop a complex multi-tiered system for surveillance, monitoring, information flow and exchange, decision support, redress across European countries.

b) Protect and improve the resilience of critical infrastructures, supply chains and transport modes

H2020 Text:

"New technologies, processes, methods and dedicated capabilities will help to protect critical infrastructures, systems and services which are essential for the good functioning of society and economy (including communications, transport, finance, health, food, water, energy, logistic and supply chain, and environment). This will include analysing and securing public and private critical networked infrastructures and services against any type of threats".

Introduction

The Financial Times of January 30th, 2013, on page 5 gives a good taste of the physical and cyber threats that the energy infrastructures will have to face in the next years. The time span of H2020 will be characterized from an increasing complexity and uncertainty, with consequent increase in the vulnerability of Critical Infrastructure. The conventional approach on risk management, based on a "a priori" classification of all the potential risks is not sufficient any more. "Think about unthinkable" is becoming a mandatory strategy in the field of CIP. Events like United States hurricane Sandy 2012, Japanese tsunami 2011, Icelandic volcano 2010, Thailand flooding 2010, have shown that the "Black swan" can be real. A margin of safety is always needed to deal with the unexpected, as well as understanding critical dependencies. These new dimensions of the CIP require a new approach to resilience, going well beyond the past approach to fortress. Initial interest in resilience was stimulated primarily by the fact that scientists and policy makers realized that protecting our infrastructure from all possible threats, man-made and natural, was just unreasonable. First of all, the cost of doing so would be astronomical. Secondly, the more important priority is to maintain the continuity of essential life resources: food, water, power, etc. So the question became: is this possible even if key assets are lost? Consequently, new capabilities at technological and organizational level have to be considered.

To have an idea of these new capabilities we have to address all the different type of possible threats. The new classes of threats, which are cross-cutting, unpredictable, and potentially highly disruptive, include:

- Cyber attacks – they constitute a new frontier for most risk managers.
- Climate changes including space weather - No one is immune from the effects of this category of threats.
- Critical Interdependencies and Failure Paths – Disruptions can cascade across geographies, across infrastructures, across industries and between the public and private sectors.

A special attention should be devoted to the implementation of the concept of "stress test", defined as "*a targeted **reassessment** of the safety and security margins of a critical infrastructure in the light of the possible threats identified above"*
Protection and improved resilience of infrastructures is a key point also for smart cities that can be considered as networks of different infrastructure networks, since there is no smartness without safety and security. Improved resilience design of critical infrastructures allows reducing their vulnerability against natural and man-made hazards, also taking into account cascading effects, which can be particularly severe in the case of smart cities.
A key tension that stems from the economic vs. national security debate is the tension between the forces that are driving infrastructure modernisation (economic stimulus) vis-à-vis the forces that are demanding critical infrastructure protection. The discussion around "smart grids" is emblematic. Thus, a potential 'modernisation' agenda is brought into direct conflict with a security agenda. The policy intervention that a government uses to meet the needs of the nation must be carefully balanced to heighten security without creating barriers to innovation, economic growth, and the free flow of information.

What needs to be done

Here following is a list of capacities that should be developed at local, regional, national and European level.
Conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences of critical infrastructures: to identify and determine ways to manage risk to best allocate resources. These assessments include threat analysis, against all threats and hazards, to provide a baseline and frame of reference for risk management and investment decisions on new technologies. Possibly, a stress test approach should be followed.

Explore methods and develop appropriate technologies to authenticate and verify personnel identity: to provide better means of identifying people in order to increase the security of critical facilities, systems, and functions. These means include systems for the recognition of biometric features (such as fingerprints, face, iris, dynamics of signing or voice).

Improve technical surveillance and situation awareness, monitoring and detection capabilities: to enable effective critical infrastructure and key assets vigilance along perimeters, entry area and key nodes like key points of access, through the application of intrusion detection technologies, data collection, classification and analysis, behavioral analysis, digital images elaboration and pattern re-identification, wide scale multisensor surveillance systems, etc. These means include also Common Operational Pictures, the capability to synthesize information coming from different sensors, units, equipment and people acting on the field.

Develop Public Regulated Regional Maritime Traffic Monitoring Service: to increase the trustworthiness and to guarantee the reliability and integrity of the ship reported data by checking the content of ship reporting messages against a common shared semantic.

These means putting in place technical counter-measures against fakers, i.e. malevolent agents putting deceiving information inside ship reporting messages.

Develop an integrated observational system: to couple current monitoring, alerting systems and quick damage assessment. It shall be based on the integration of observing capabilities (both ground based airborne and satellite based) with navigation, TLC and ICT technologies and on the development of new observational platforms (e.g. UAV) and new advanced observing technologies (as new non-invasive sensing technologies, low cost technologies, “sensors not sensors” , dust of sensors, etc.). This is of particular relevance for implementing the security of smart cities.

Develop detection technologies and procedures to screen food productions, food supply chains, intermodal containers, cargo and passenger baggage: to identify and explore technologies and processes to enable efficient and expeditious screening of containers, cargo, passengers and baggage, especially at intermodal stations, like rail stations, ports and airports, for rapid identification of counterfeited goods, with a special emphasis on technologies for detecting explosives and hazardous materials or contaminants.

Develop a Multi-Modal Transport Service Platform to improve the cooperation and interoperability of different transport modes*:* the increasing integration of different types of transport, make the system more fragile and complex, generating scenarios sensitive to possible malicious and terrorist acts. The security of transport by rail, road or sea, and the ability to move goods and people through different transport modes (multi-mode / inter-modality), requires the availability of data and information coming from the several information systems, the development of tools for analysis and correlation of such information aiming to detect the threats. Such a platform could be incrementally defined and implemented and can grow in order to provide the institutions with a single system view of the whole transport sector.

Improve the security of health infrastructures: the healthcare systems of all developed countries are moving from being organization-centered to person-centered architectures, enabled by appropriate information and communication technologies. We can envisage the idea of a diffused health-care system both for improving cost-efficiency as well as resiliency. A diffused system, based on delivering health-services in several places (also physically distributed), as health-care at home through biomedical sensors, considering family doctor studies (supported by limited diagnostic devices) at the district level, supported by secondary hospitals (mainly for post-operations convalescence) and eventually with main hospitals for surgeries and research at city/regional level. A main element of our interest in terms of security, comes noticing that usually centralized systems represent a single point of failure and thus are less resilient than distributed systems whose diversity and often geographical distribution help to survive to incidents.

Develop further our ability to prevent, detect, defend against and recover from cyber-attacks**:** following the principles of prevention and resilience and non-duplication.

Prevention and resilience are particularly important given the reality that certain threats will persist despite all efforts to protect and defend against them.

Explore methods and develop appropriate skills and technologies for addressing cloud computing security challenges: Implementing a cloud-computing solution incurs different risks than with dedicated data centers. Risks associated with the implementation of a new technology service delivery model include policy lags, implementation of dynamic applications, and securing the dynamic environment.

Lighthouse projects

Lighthouse project is normally perceived as a project with the explicit goal of accelerating changes in perceptions and beliefs on a wide scale. We envisage the need of at least two lighthouse projects:

A first one in the area of improving integrated risk modeling of “system of systems”, intended as a combination of critical infrastructures from different sectors, interacting each other. Important questions arise when identifying priorities for design and protection: Which components, if compromised, can lead to significant service delivery disruption? What topologies are inherently robust to classes of cyber attack? How to do dependencies analysis of critical services and impact assessment of possible cascading failures? A key research challenge in addressing these fundamental questions lies in the effective understanding of the cyber-physical synergy and cascading effects.

A second one in the area of improving the resilience of complex cyber – physical systems (e.g. communication networks, smart grids, high speed transportation systems, smart cities). Recently, security researchers and standards bodies have begun to develop socio - technical requirements and potential solutions for protecting complex cyber – physical systems. A key research challenge in addressing these questions is the capability to synthesize information coming from different sensors, units, equipment and people, acting in the physical domain and in the cyber domain.

c) Strengthening Security Through Border Management

H2020 Text:

"Technologies and capabilities are also required to enhance systems, equipments, tools, processes, and methods for rapid identification to improve land, marine and coastal border security, including both control and surveillance issues, while exploiting the full potential of EUROSUR. These will be developed and tested considering their effectiveness, compliance with legal and ethical principles, proportionality, social acceptability and the respect of fundamental rights. Research will also support the improvement of the integrated European border management, including through increased cooperation with candidate, potential candidate and European Neighbourhood Policy countries."

Introduction

At the present time, free movement of EU citizens and the abolition of checks at the internal borders in the Schengen Area are some of the most tangible achievements of the European Union. These imply that the integrity of the Union's external borders is a prerequisite for the Schengen area as we know it today and will remain a prerequisite also in the future. Measures to manage the external borders must meet the dual objectives of enhancing security and facilitating travel and goods exchange.

The potential offered by new capabilities and enabling technologies in this regard was addressed in the Commission's efforts during the past R&T Frameworks trying to figuring out the possible components of what are going to be the future EU "smart borders". The effort should continue and be sustained in the forthcoming H2020 in order to evolve toward a real smart border security in such a complex and heterogeneous geographic area as the European one.

Analogous effort should be continued in the specific area of border surveillance where the route traced by the EUROSUR initiative should be enhanced by technology innovations and new capability developments, taking advantage from a coordinated collaboration of Civil and Military sides (dual use approach).

What needs to be done

Here follows a series of needs and suggested developments in order to meet the requirements of a stronger European Border Management.

According to the forthcoming EU border policies and roadmaps, a relevant support is requested to enhance/improve the border check capabilities by means of new technologies (e.g. for multiple advanced biometrics, abnormal behaviour detection at

multiple temporal scales, selective face recognition, multi-sensor analysis, identity management, intelligent information management) and novel approaches (e.g. automatic accreditation through “smart” biometric check points). Beyond people, screening of goods and food should be improved and made more efficient and reliable (e.g. by means of automated and unmanned custom systems or new sensors, portable and miniaturised tools with their ICT interfaces), in order to avoid degradation and/or intentional contamination. Any further research activity, aiming at implementing the smart border concepts, should pay attention to the specific aspects of usability (e.g. automated and time-efficient procedures), societal acceptance (e.g. smooth and fast border crossing for travellers, while ensuring an adequate level of security), privacy (e.g. non-invasive border checks) and legal viability (e.g. harmonic compliance with local and global regulations).

Airports represent the key nationwide access and exit points and, consequently, they constitute a “constellation” of relevant border points at European/International level. The challenges coming from the mobility needs of citizens and the evolution of threats affecting the airport security, require an integrated approach that will more and more involve Industries, Security Operators and different Public Institutions. The development of an advanced system devoted to safety, security, dynamic risk management and passengers’ management shall then be encouraged and validated by all the above mentioned stakeholders, and shall include: complete luggage tracking, including smart association traveller/luggage; advanced RFID identification techniques; multi-scanning devices application based on innovative screening techniques for detection of hidden/dangerous materials; efficient information sharing among actors, subsystems and devices (e.g. cameras, crossing detection, infrared, etc. in order to detect and notify the security state of airport’s assets and infrastructures); advanced decision support, enhanced by the correlation of intelligence information and external data sources.

New sensors, portable and miniaturised tools with ICT interfaces should be developed for customs and borders in order to increase the speed and reliability of identification of unsafe foods, which can derive from accidental or intentional contamination. These sensors and ICT tools should be further conceived to be interoperable, linked to infrastructures for collection and analysis of data.

In 2011, over 90% of illegal border crossings took place in four EU countries: Italy, Malta, Greece and Spain. Italy, because of its central position in the Mediterranean Sea and its relevant coastal extension, aims at exploiting all the potentialities of an European Border Surveillance System and the forthcoming Common Information Sharing Environment. In the framework of “EUROSUR” guidelines, Italy is particularly interested in enhancing the capabilities of monitoring, detection, identification, tracking, prevention and interception of illegal border crossings as well as protecting and saving the lives of migrants and refugees, especially those in distress at sea. For this reason, a set of new technologies (e.g. unmanned systems, multi-sensor platforms, network architectures) shall be improved and integrated, together with innovative approaches and operational procedures. Finally, beyond conventional funding processes of H2020, PPPs (Public Private Partnerships) should be started up and sustained in order to encourage the fruitful collaboration between the Industrial Solution Providers and the European User Community.

Regarding the specific theme of Maritime Surveillance, supporting the development of techniques and technologies to detect small boat, to go beyond the current coastal observational system capabilities, is needed; at the same time, the development of smart systems, for managing a huge amount of heterogeneous data, need to be supported in order to improve the detection of crime/illegal activities (such as drug trafficking, illegal immigration). More advanced methodologies and techniques able to correlate different observations of the same target (from different systems, such as the evolutions foreseen for the Regional Traffic Monitoring Systems), need to be developed in order to increase and make more reliable the necessary Maritime Domain Awareness (as clearly established in the EU Integrated Maritime Policy Paper and in the recent Draft Roadmap for the Implementation of the EU Common Information Sharing Environment - CISE). This case evidences the condition for a dual-use research approach and the need for a strong collaboration between Civil and Military operators, that shall be then encouraged and sustained by proper funding frameworks (EFC- European Framework for Cooperation).

Still on Maritime Surveillance, the development of on-board sensors processing capability, data management, network servers (i.e. to generate automatically alerts regarding suspicious vessels over heavy traffic areas with numerous objects) should be further encouraged. Moreover, on board satellite communication data–link, to establish data streams across the networks, shall provide end users/customers with relevant information rapidly when required. Finally, a network centric system based on privilege and authorization regime (also allowing data provision on demand) would help users, customers and agencies to share information in a timely and more efficient manner.

Lastly, as a cross-cutting issue, enhanced Interoperability should be one of the objectives of further R&D activities for both border control and surveillance. Definition/adoption of European and worldwide standards (both at system and operating levels) should be encouraged and supported by technical solutions (e.g. Semantic Interoperability, Ontology Fusion, …), in order to involve and manage the cooperation among a large number of actors, while making available, correlating and exploiting huge global datasets (*see also* Big Data challenges), to achieve an integrated operational border management across boundaries.

Lighthouse projects

Several Lighthouse projects should be started in order to enhance and organize the efforts in the following R&D streams.

Enhanced adaptive wide area surveillance & monitoring system, capable to facing various security issues (illegal migration of people, piracy, trafficking of drugs and weapons, as well as various natural disasters such as earthquake, flooding…) over large sea and land environments, where response effectiveness will be further steered by an accurate and precise environment observation, and by a cooperation among manned and unmanned systems equipped with heterogeneous sensors. Developments have to be designed in order to pave the way for "affordable" solution to be implemented in the operations.

New methods to improve border surveillance, taking into account crossing people and goods, are required, while achieving a full coverage of ground, air, sea, underwater and underground environment:

- Detection and Classifications of “objects”: e.g. detection of humans, classification of border crossing events for ground surveillance, detection of small vessels and small airplanes at low altitudes and at long ranges;
- Interoperability among different sensing systems and different sensors modalities;
- Interoperability of detection, risk assessment systems and response systems to be deployed in complex contexts such as multinational operations, heterogeneous end-user organizations etc.; interoperability developments shall be harmonized with standardization processes.

To meet all these challenges, reinforcing the cooperation among involved operators and improving the situational awareness, a set of advanced technologies and components such as sensors (low cost radars, hyperspectral, active optronics, dust of sensors …), platforms (HASP, airships, UAV, UGV, USS, …), data fusion and big data management platforms need to be developed.

Airport can be considered as a comprehensive and fully integrated system for border checks through a wide security monitoring network. Future R&D projects shall be planned in order to support:

- the improving of processes for identifying suspicious event/crimes and awareness about the current state of airport operational activities without degrading the levels of airport performance and services for the public;
- the dynamic adaptation of the security assets for collecting information on scenario changes (dynamic evolution of risks) as well as the management, in a dynamic way, of the actions to mitigate risks;
- the improving of collection and processing of early detections of crimes/violations (timing/frequency and levels of detail of the information gathering and aggregation) and the management of countermeasure actions in case of suspicious events (automatic control and dynamic reconfiguration of sensors and controlled systems).

As regard the maritime surveillance one or more lighthouse projects shall be launched to support the development of maritime awareness tailored for specific civilian goals; the development of suitable info-space environment as generated by putting together new surveillance capabilities/technologies and data sharing policies (e.g. CISE) shall be supported by H2020 initiatives. Implementation of secure data transfer technology shall also allow the adaptation of military data for a civilian use, being compliant to privacy needs of the public and EU/National legal frameworks.

A more specific example of project in the area of maritime domain could be generated by the main current limitations that prevent the full exploitation of Regional Vessel Traffic Monitoring Systems to have a real and reliable situational awareness:

- lack of any mechanism to assess the reliability of the (cooperative) data sources, specially of on-board AIS stations;
- absence of any agreed validation framework for the reported information:
- absence of a common semantic not even for the key information reported (ship type, ship status);
- lack of specific technical counter-measures against fakers.

Overcoming these needs by the development of new technologies/solutions would lead to the definition of a totally new concept which can be synthesized as “Public Regulated Regional Traffic Monitoring Service” (borrowing the definition from other Services like the Galileo EU Navigation System), meaning a service where:

- the reliability and integrity of the ship reported data is guaranteed and measured by applying appropriate protocols and technical measures, able to signal when and under which conditions a ship report can be considered reliable enough for a security sensitive application;
- the content of ship reporting messages is checked against a common shared semantic, and validated according to predetermined agreements supporting the identification of “abnormal reports”, also on the base of sensor and static data bases information correlation and fusion;
- technical counter-measures are put in place against fakers, i.e. malevolent agents putting deceiving information inside ship reporting messages.

Lastly, the use of Medium Altitude Long Endurance (MALE) and Unmanned Air-Vehicle System (UAS) for maritime surveillance should be promoted, in order to act as a node in a global network that will automatically generate alerts about suspicious vessels based on analysis of data and information gathered from the designated surveyed area in all weather conditions. The use of Unmanned Air-Vehicle System (UAS) for land border surveillance, should be also promoted in order to detect, locate and track illegal movements of people and goods crossing borders. The UAS shall be the aerial node of a global system that integrates land based and airborne sensing technologies.

d) Improve cyber security

H2020 Text:

"Cyber security is a prerequisite for people, business and public services in order to benefit from the opportunities offered by the Internet or any other additional data networks and communication infrastructures. It requires providing an improved security for systems, networks, access devices, and software and services, including cloud computing, while taking into account the interoperability of multiple technologies. Research and innovation will be supported to help prevent, detect and manage in real-time cyber-attacks across multiple domains and jurisdictions, and to protect critical ICT infrastructures. The digital society is in full development with constantly changing uses and abuses of the Internet, new ways of social interaction, new mobile and location-based services and the emergence of the Internet of Things. This requires a new type of research which should be triggered by the emerging applications, usage and societal trends. Nimble research initiatives will be undertaken including pro-active R&D to react quickly to new contemporary developments in trust and security. Particular attention should be given to the protection of children, as they are highly vulnerable to the emerging forms of cyber crime and abuse.

Work here should be conducted in close co-ordination with the ICT strand of the "Industrial Leadership" pillar."

Introduction

Cyber Security is a wide concept, and there is still little consensus regarding what is within its scope and what should be left out. It is a well known fact that the pervasive deployment of Information and Communication Technologies (ICT) has resulted in a dramatic improvement of our quality of life. However, this comes at the cost of increased exposure of the society at large to cyber threats (suffice to mention the recent sharp increase in targeted attacks to Critical Infrastructures). Evidence is demonstrating that we are witnessing a dramatic increase of external borne security incidents, while internal are basically stable, and accidental have increased only slightly (most probably, such a slight increase is mainly due to the increased complexity of the equipment, which results in more operator mistakes and interactions faults in general). A whole new generation of attacks has seen the light, characterized by a more distributed, subtle, and ultimately harmful nature, such as botnets and low-rising and stealthy attacks. Cyber Security has thus become a global issue, to be dealt with on a global scale. It is not by chance that Cyber Security is a key priority of the HORIZON 2020 program.

What needs to be done

Since the scope of cyber security is so wide, it is important to identify the objectives which need to be prioritized. Specifically, we have identified the following six objectives:

- Cyber-physical protection systems;
- Cyber intelligence via information management;
- Design and development of crisis management systems;
- SCADA and Smart Grid Security;
- Cloud Computing Security;
- Mobile Security.

Cyber-physical protection systems. The research activity encompasses the whole cycle of electronic access (including authentication and authorization/profiling of users), network control, and system monitoring with respect to complex, distributed ICT systems. Users can be individuals, groups, physical objects, logical entities, or applications. The objective is to make the interconnected system of national critical networks and individual infrastructures more resilient and secure. This is typically achieved by a combination of means, and in particular: i) enforcing both passive (firewalls) and active (intrusion detection and prevention) perimeter defense systems, ii) improving the technologies for design and development of network protocols and services, and iii) continuously monitoring network status and traffic. Network protection is of paramount importance, since it is a pillar on which many other vital aspects of the modern society are based. With respect to prevention and investigation, lawful interception is a key topic. Important mechanisms also include intrinsic security of unmanned systems, and specific solutions for secure network communication in wireless segments (e.g. surveillance, intrusion detection, and mitigation of cyber attacks). More effective convergence is needed among a plethora of cyber security technologies, including: Physical Security Information Management (PSIM), Security information and event management (SIEM), Security Operation Center (SOC), Identity Management, Building Automation, Video Surveillance, Access Control, and Forensics.

Cyber intelligence via information management. The objective of the research activity is the development of effective cyber intelligence features, to guarantee citizens' global security, by exploiting the huge potential of currently available as well as emerging Information Management technologies (including high-performance and cloud computing platforms). Security will be improved along several axes, including protection of ICT systems, Critical Infrastructures, and assets. The developed technologies will provide a set

of tools which will support a security process consisting of the following three phases: plan, control, and react. A key role will be played by information flow collection technologies, e.g. those based on video surveillance.

Design and development of crisis management systems. The research activity is targeted at studying systems which can improve crisis management functions and interventions, in various contexts. The amazing complexity and scale of systems and infrastructures to be protected call for solutions that allow effective coordination of actions, in a timely fashion. This entails support for near real time analysis and correlation of symptoms related to attacks targeting individual components/systems, as well as the overall system. Mechanisms should be developed to counter/mitigate attack effects and consequences.

SCADA and Smart Grid Security. Traditional Critical Infrastructures (CIs) were intrinsically secure systems, due to a combination of factors, and in particular: i) they consisted (almost exclusively) of special purpose devices, which were based on proprietary technologies; ii) individual sub-systems operated almost in isolation, i.e. they did not interact with the external world, with the exception of the system being controlled; iii) they were largely based on dedicated (as opposed to shared) communication links; iv) they massively relied on proprietary (as opposed to open) communication protocols. These trends have been largely subverted, and it will be even more so in the future. First, Wireless Sensor Networks (WSNs) have become an integral part of virtually any CI. Second, Commercial-Off-The-Shelf (COTS) components are being massively used for implementing Supervisory Control And Data Acquisition (SCADA) systems. Third, subsystems are being connected using the infrastructure of the corporate Local Area Network (LAN), or even Wide Area Network (WAN) links, possibly including the public Internet, as well as wireless/ satellite trunks. An important objective will be improving SCADA and smart grid security and resilience, via effective integration of State-Of-The-Art sensor, communication, information, and control technologies. This will entail developing the following main functional blocks, all operating in real time: i) monitoring, ii) detection and diagnosis, iii) risk assessment, and iv) reaction and remediation. Data will be collected from a variety of heterogeneous hw/sw components that are typically found in SCADA networks and smart grids (e.g. PMUs, PDCs, smart meters, databases, Operating System logs, network devices). All functions must be designed and implemented using fault- and intrusion-tolerance techniques , so to achieve a high level of trustworthiness.

Cloud Computing Security. In a nutshell, the objective of Cloud Computing Cyber Security research will be to build cloud platforms that are more secure, confidential, and dependable, meaning that they will allow honest users to do their business and/or social activity reliably (since they benefit from improved security, confidentiality, and dependability), while also limit the possibility for malicious users of exploiting the

aforementioned properties for their evil purposes. To achieve this, effective support is needed for: 1) accurate and timely fault and intrusion detection & diagnosis features, to be made available both to cloud providers and to cloud users; 2) fault- and intrusion-tolerant forensic facilities for producing evidence to be used to prosecute criminals in court, 3) efficient and scalable mechanisms for implementing confidential communication channels exclusively dedicated to authorized users and 4) access and usage control mechanisms for the transparent as well as accountable dissemination of data in the cloud. These objectives address some of the thirteen technical risks that have been identified by ENISA in their recent report on cloud security open issues. Research should take a use case driven approach, meaning that it should be inspired by substantial case studies, which are diverse enough to provide a comprehensive set of requirements. Demonstrators should be set up, which should consist of multiple clouds, based on heterogeneous technologies, and located at geographically distant sites. The research program, while extremely rich in RTD content, should also make substantial contributions in terms of innovation, i.e. efforts should be made to take research results to the next step (i.e., "out of the lab").

Mobile Security. Over the last years we have witnessed a proliferation of mobile devices, such as smartphones and tablets, which are becoming day-by-day more pervasive. Current operating systems for mobile devices are based upon the concept of apps. Apps are lightweight applications that are distributed through on-line marketplaces, such as the Apple AppStore or Android Google Play. Using this paradigm, users browse apps on markets and install them directly on their devices. Regrettably, this model is affected by major security and trust issues that can lead to massive malware spread. Three main factors are worth mentioning: 1) a widespread platform, 2) readily accessible development tools, and 3) sufficient attacker motivation (typically, but not always, monetary). With the advent of open platform smartphones, the growing market-share parallels the rise in the number of mobile threats. It is easier for developers, including malware writers, to write and distribute applications and it is easy for malware authors to create trojans that are very similar to popular apps. Currently, more than half of all mobile threats collect device data or track users' activities. Almost a quarter of the mobile threats are designed to send content and one of the most popular ways for phone malware authors to make money is by sending premium SMS messages from infected phones. Increasingly, phone malware does more than send SMS. For example, we see attacks that track the user's position with GPS and steal information. People regard their phones as personal, private, intimate parts of their life and view phone attacks with alarm. Mobile threats are now using server-side polymorphic techniques, and the number of variants of mobile malware attacks is rising faster than the number of unique families of mobile malware. Effective mechanisms must be made available to users to discriminate good apps from malware apps. Flexible trust models must be developed, to favor openness while preserving security and privacy.

Lighthouse projects

We envision two lighthouse projects, in the form of demo projects, with the following objectives:

- Building a trans-national infrastructure for cyber-security data sharing and analysis;
- Developing techniques and tools for forensics in the cloud.

Building a trans-national infrastructure for cyber-security data sharing and analysis. The objective is to build a cross-overlay trans-national cyber-security information exchange network and governance structure, for improving cyber-security decision support and cyber attack response in situations where multiple stakeholders from different countries and/or sectors are affected. Challenging requirements must be satisfied, in terms of trust management, scalability, timeliness, situation awareness, and more. An integrated approach will be taken, that will allow incremental data sharing and information exchange among security stakeholders of individual member states. Loosely-coupled communication mechanisms, data aggregation solutions, incentive based models, and confederated access control mechanisms shall be used to increase trust among stakeholders. Data analysis techniques will be developed, to implement complex correlation rules, also including organizational, legal, economic, and other non strictly technical requirements. The research will also address relevant issues such as governance, business model and incentives.

Developing techniques and tools for forensics in the cloud. Forensics in Cloud deals with evidence collection and forensic investigation of criminal activity in the cloud. In this context, by digital evidence it is meant any information of probative value that is either stored or transmitted in a digital form. Even if digital forensics is a relatively young discipline, good practices have been established, and a number of tools is available to help the process of gathering digital evidence from devices. The collection process in cloud computing is made particularly challenging due to some peculiarities of these environments, such as: multi-tenant hosting, time synchronization, cross-border data distribution, and virtualization (resulting in the splitting of data between hypervisor and virtual machines). Law Enforcement Agencies (LEAs) of individual member states are encountering situations where the seized materials do not contain any information, and the traces on such materials indicate that all data and digital information that was manipulated by the suspects is located in some sort of cloud-computing based service, possibly hosted in a foreign country. The Forensics in the Cloud lighthouse project will deal with evidence collection and forensic investigation of criminal activity, following trails and information that may be stored or processed in the cloud. The goal is not specifically to investigate unlawful activity in the cloud, but rather to collect forensic evidence of unlawful activity, be it in the "real world" or in cyberspace, when such evidence may be in the cloud.

e) Increase Europe's resilience to crises and disasters

H2020 Text:

"This requires the development of dedicated technologies and capabilities to support different types of emergency management operations (such as civil protection, fire fighting and marine pollution, humanitarian aid, civil defence, conflict prevention, development of medical information infrastructures rescue tasks, disaster recovery processes and post-crisis-stabilisation) as well as law enforcement. Research will cover the whole crisis management chain and societal resilience, and support the establishment of a European emergency response capacity.

This also requires promoting interoperability between civilian and military capabilities in tasks ranging from civil protection to humanitarian relief, border management or civilian peace-keeping. This will include technological development in the sensitive area of dual-use technologies to enhance interoperability between civil protection and military forces and amongst civil protection forces worldwide, as well as reliability, organisational, legal and ethical aspects, trade issues, protection of confidentiality and integrity of information and traceability of all transactions and processing."

Introduction

In the field of crisis and emergencies associated with natural and human pressure induced hazards and aging/degradation there are urgent needs with regard to the development of technologies for both the prevention-preparedness and the crisis response. World is changing and spending constraints force to the optimization and rationalization of the efforts for crisis mitigation and intervention. One of the key points for public safety will regard therefore the use of cost effective solutions capable also of integrating free and accessible information and opportunities offered by modern societal aspects to establish and maintain a foresight capability covering a large range of applications. The technological development must be brought to the level to allow proactive plan and security as a practice of communities on a global scale. Risk-management and risk assessment tools should also account for dynamic risk changes further emphasized by climate changes.

A key role in crisis management – whatever the origin of the crisis would have been: natural or anthropic, technological accident or large scale terrorist attack – is played by First Responders (FR) Teams. The use of unmanned ground platforms as support to FR Teams is advised by a number of factors, including the societal attitudes toward risk and acceptability of human casualties and loss of life: a robotic platform should be able to a) improve the awareness of FR on the disaster scene (Fukushima) and b) operate in dangerous sites in place of human FR (Fukushima).Looking after cheapness in platform realisation would allow to deploy a large number of units on the field, so improving the

effectiveness of search and rescue operations, which have to be concentrated in early stages of disaster management (earthquakes: L'Aquila, Haiti).

What needs to be done

Following EU recommendations a list of capabilities follows, which already are in *Serit Program* and which development is considered of particular interest .

Services based on sensing capabilities. The growth of Earth Observation satellites has boosted the application of remote sensing in crisis and disasters. Core services are fostering the use of space technologies in support to ground operation during emergencies: see f.i. the Haiti earthquake case. Nonetheless satellite data is still lacking of the development of specific services for the prevention/preparedness and the dynamic evaluation of risk during crisis and in the post crisis phase, as well as of market oriented solutions. Current and forthcoming sensors are capable of acquiring very high details on single structures but the development of improved, suitable and user-oriented tools is mandatory to reliably and accurately extract the multidimensional information content instrumental to new security, planning and crisis governance applications. Airborne sensing offers high operative flexibility thus providing a unique technology for the post event phase. At the present status airborne sensing is restricted to mapping purposes whereas development is required to provide accurate monitoring capabilities to deliver quantitative and key information for situational awareness and decisions makers during emergencies. Another relevant point is associated with social aspects of modern society and citizens habits which are the more and more "on the web" thus providing a source of information of "opportunity" (sensing with non-sensors) that needs to be accounted for during crisis. A primary challenge associated with sensing capabilities is the management of huge data which need to be accessed, integrated with other measurements, and assimilated into models for use at the prevention stage for civil protection. Data interoperability and real time data access is crucial both to improve data gathering and information distribution in order to guarantee real time situation awareness. A further mandatory aspect is related to federate and scalable ICT architecture to remotely control sensors and manage data fluxes, so to permit both to change the monitoring strategy, depending on events that are occurring, and to deliver web services to stakeholders and citizens. Adaptive Wide Area Surveillance and Monitoring Systems, which integrate ground based, airborne and satellite based technologies with position and navigation technologies and ICT and web tools, will be crucial for awareness, preparedness and post-crisis stabilization. The exploitation of data acquired by sensing technologies is necessary to mitigate threats and reduce the occurrence of crises in Europe and at the same time to increase Europe competitiveness on the market of resilience at a global scale.

Large scale disasters governance. A strong research effort is still required to work around the factors which presently limit the widespread introduction of unmanned platforms, like the insufficient situational awareness, the excessive mental burden required to operate present devices, the poor adaptability to different kind of grounds/scenarios.

Great market opportunities for EU enterprises would be opened by a higher diffusion of such devices, in addition to the obvious societal/humanitarian positive repercussions.

First of all, a significant improvement in mobility should be pursued, to allow a mobile platform to cope with different grounds – like rugged soils, debris, stairs; weight reduction and speed increase should be part of this research task. Another important matter is the enhancement of communication capability in shielded areas – e.g.: the inner areas of the Fukushima nuclear plant, or of a building collapsed by fire or earthquake. A wide field of research is related to the degree of autonomy of mobile platforms, which is presently insufficient and implies matters like artificial vision and cognition capabilities development, which have been yet extensively studied but are still liable to broad improvements. Moreover, the caution required to manage the present devices – and the consequent mental burden for operators (FR) – is one of the greatest obstacles to the mobile platforms diffusion; further, careful studies on human-robot interfaces are of the maximum importance.

The above-mentioned capabilities need further implementation in the development of sensors into "multisensor intelligent platforms", providing the possibility of increasing the detection efficacy for chemical, biological, radionuclear and explosive hazards. The number of technologies currently available needs further improvements for miniaturisation and increase in throughput level. To achieve real time sensing and data fusion, implementation in communication interfaces, databases for storing, and decision support systems are required. Finally, to establish field deployment near the point of concern, all sensing platforms must be modified for adaptation to rugged situations, and simplification in operational procedures, even to reach unmanned performance. Besides modifying the equipments and platforms, protocols and procedures must also be adapted to introduce automatic sampling, extraction-less sample preparation, multi-target analyses, non-targeted analyses.

Lighthouse projects

A possible project could be explored in connection with dual-use research. The plethora of technologies, equipment, devices and protocols which can be employed in a crisis situation has been produced by years of research in different fields, such as environmental monitoring, medical diagnostics, food control to mention but a few. This research has been carried out by civil scientists and at the same time by military structures. It is time that a closer cooperation is established between the two environments, to benefit of the different approaches, knowledge, and requirements. The proposal is therefore for a project directed towards development, implementation, tailoring and adaptation of technologies for surveillance and detection, which must join efforts from the civil and military worlds, to achieve efficient, rapid, multitarget, high-throughput, ruggedised systems taking into account also new priorities regarding the improvement of the smart cities resilience against crisis events and disasters The focus will be also on detection of CBRNE threats, and it must be directed towards prevention and preparedness.

Another project targeted to the concept of operations based on use of sensing capabilities for the crisis management outside of Europe with a specific focus to humanitarian crises and disaster management is fundamental to support a European External Action Service being one of the priorities at the EU level. It would regard not only disaster management and humanitarian aids due to events (wars, droughts, famines) but also prevention and mitigation strategies. In this frame, the satellite and airborne sensing capabilities as well as non-sensors data and interoperability tools should be enhanced so to perform a global quick assessment of the crisis scenario and to support the coordination of the aid and recovery actions. Remote sensing capabilities should be integrated in order to develop global scale long-term monitoring systems for the protection of natural resources and the prevention or mitigation of factors leading to humanitarian crises

Finally, FP7DEMO projects are aimed at demonstrating European emergency capacities. Nonetheless, capabilities related to outside and inside Europe intervention have significant differences especially in terms of available technologies and source of information. Inside Europe intervention will necessitate to integrate future technological progress, to comply with opportunities offered by federated and scalable ICT solution for operational service optimization and to benefit of holistic approaches to crisis and disaster in the prevention and mitigation stage as well as for quick damage assessment in a cost sharing logic. In this framework the problem of security and safety in smart cities should be addressed taking into account that there is no smartness without safety and security and that smart cities, which are based on networks of different infrastructure networks, are particularly vulnerable to cascading effects.

f) Ensure privacy and freedom, including in the Internet and enhancing the societal legal and ethical understanding of all areas of security, risk and management

H2020 Text:

"Safeguarding the human right of privacy including in the digital society will require the development of privacy-by-design frameworks and technologies to underpin new products and services. Technologies will be developed allowing users to control their personal data and its use by third parties; as well as tools to detect and block illegal content and data breaches and to protect human rights on-line preventing that people's behaviours individually or in groups is limited by unlawful searching and profiling. Any new security solution and technology needs to be acceptable to the society, comply with Union and international law, be effective and proportionate in identifying and addressing the security threat. Better understanding the socioeconomic, cultural, and anthropological dimensions of security, the causes of insecurity, the role of media and communication and the citizen's perceptions, are therefore essential. Ethical and legal issues and protection of human values and fundamental rights will be addressed, as well as risk and management issues."

Introduction

With reference to the security context of Horizon 2020, the SERIT TA 7 intends to propose two research frameworks: "Inclusive Security" and "Legal and Ethical Aspects of Biometric Data International Sharing"

Inclusive Security. In keeping with the concept that every technological solution must be acceptable, in a generic sense, to the whole society, it should tend to be usable by all components of the population. In practice several technological tools of the today society, including those oriented to security, seems to be oriented only to specific segments of the population while other subjects, such as the elderly and people with disabilities, are often not appropriately considered.

With reference, for example, to the biometric technologies, the elderly are likely to be excluded from various applications due to possible physical or cognitive deficits or, in drawing a project for Automatic Border Crossing, very rarely a gate is designed to be used by a person with mobility problems. The theme of the inclusive security is, therefore, an important area of research for the SERIT TA 7 whose prerogatives include, among others, the assessment of the social and ethical aspects of security.

Legal and Ethical Aspects of Biometric Data International Sharing. The international exchange of information is rapidly becoming a crucial issue in a society in which the process of globalization requires always more intensively the sharing of data pertaining to

individuals among different countries. The exchange of data, which is already massive, for example, in the financial sector, in recent years is investing other highly sensitive areas, such as biometrics. Currently various European and non-European countries regularly exchange fingerprints and DNA data on the basis of international multilateral or bilateral treaties and, on the other hand, the generalized increase in security measures suggests a proliferation of such exchange of data in the near future.

Of course the sharing at the international level of biometric data requires a strong caution from the legal and ethical points of view and many aspects related to these issues are still under study and improvement.
In line with what reported in the programmatic document of Horizon 2020, with reference to the point *"Any new security solution and technology needs to be acceptable to the society, comply with Union and international law, be effective and proportionate in identifying and addressing the security threat"*, a transversal research area focused on the biometric data international sharing and aiming to promote a possible homogenization of systems and procedures appears particularly significant, mainly in the light of a potential future extension to extra-European contexts.

What have to be done

Inclusiveness-by-design. The expression "privacy-by-design" is becoming rapidly popular as a project modality in which the protection of personal data is a fundamental prerogative of the technology, from the early design stage to its deployment, use and ultimate disposal. Similarly to the concept of “privacy-by-design”, the SERIT TA 7 suggests the adoption of the expression “inclusiveness-by-design” to designate a technology that tends to be offered to a wider users’ population and characterized by a very high level of usability, defined as a primary constraint of the project.

The inclusiveness-by-design in the context of security could provide an appropriate answer to the instances “*Better understanding the socioeconomic, cultural, and anthropological dimensions of security”* and *“ protection of human values and fundamental rights”* reported in the document targeted to the implementation of Horizon 2020.

Explore the Legal and Ethical dimension of Biometric Data International Sharing. With reference to the European context, the biometric data exchange among some of its Countries actually occurs in the framework of the "Prüm Treaty". The treaty includes cross-border cooperation by means of exchanging judicial and police information and by providing mutual assistance. With regards to the exchange of information, among other data, each member state has to make different biometric databases available to other member states for automated searches. The exchange of information occurs by existing mutual legal assistance procedures (police or judicial). The adoption of the Prüm Treaty has clearly highlighted both the advantages offered by the data sharing and, on the other side, some points of difficulty, mainly in the area of the homogenization of systems and procedures. The TA 7 proposes to explore the legal and ethical dimension of the Biometric Data International Sharing with particular reference to a some possible future geographical

extensions or even cooperation with other biometric data sharing systems.

Lighthouse projects

A “Lighthouse Project” (LHP) is effectively an extended scale Demonstration where the new technologies can be assessed under pseudo-commercial conditions, in which key stakeholders such as public agencies, users, and technology and infrastructure providers participate. Two lighthouse projects could be presented:

- *Inclusiveness-By-Design for security technologies*

The project should stimulate both industrial partners and public agencies in defining a minimum set of requirements for the security technologies as concerns their impact on disable categories of users. The project could use, for example, an Automated Border Crossing system to evaluate how the Inclusiveness-By-Design could promote a better and more appropriate implementation of the technology.

- *Legal and Ethical Dimension of the Biometric Data International Sharing*

The project should address the legal, ethical and technological dimension of the biometric data sharing in a vision enlarged in respect to the Prüm Treaty. Such project should require a strong cooperation of TA7 with other SERIT TAs, specifically the TA 3 (Detection and Identification Systems) and the TA 5 (Information Processing and Management).

g) Support the Union's internal and external security policies

The content of the main EU strategic documents issued during the last 10 years regarding respectively internal and external security shall be considered in order to properly address the research priorities related to the mission "support the Union's internal and external security policies".

As regards internal security we shall consider the "Internal Security Strategy for the European Union (ISS), Towards a European Security Model" (2010) issued by the European Council, and the document on its implementation "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (2010), issued by the European Commission.

Concerning external security, we shall consider the following documents issued by the Council: "European Security Strategy (ESS), A secure Europe in a better world" (2003), "Report on the implementation of the European Security Strategy, Providing security in a changing world" (2008) and the "Statement on tighter international security" (2008).

The comparison of key threats/factors highlighted in these documents results in a number of areas of intersection between internal and external security.

Table 1 – European security in the EU strategic documents – Key threats/factors

	ESS	**ESS Report**	**Council Declaration**	**ISS**	**ISS 5 Steps**
	2003	**2008**	**2008**	**2010**	**2010**
Terrorism	✓	✓	✓	✓	✓
Organised crime	✓	✓		✓	✓
Weapons of Mass Destruction (WMDs)	✓	✓	✓		✓
Cyber	✓	✓	✓	✓	✓
Pandemics	✓	✓		✓	✓
Piracy	✓	✓	✓		
Regional Conflicts	✓	✓			

Energy	✓	✓	✓	✓	✓
Poverty	✓	✓			
State failure	✓	✓		✓	
Cross-border crime		✓	✓	✓	✓
Natural or man-made disasters		✓		✓	✓
Infrastructures	✓	✓		✓	✓
Climate change	✓	✓			✓
Border security	✓			✓	✓
Violence	✓	✓		✓	
Others to be identified	?	?	?	?	?

Beyond these key threats/factors, the key "mandate areas" covered by the internal and external security policies should be properly considered. Internal security mainly corresponds to the field of justice and home affairs (JHA) while external security mainly corresponds to the foreign and security policy (i.e. the Common Foreign and Security Policy, CFSP, which includes the Common Security and Defence Policy, CSDP).

Since both are arguably extremely variegated domains, it is essential a reassessment of the strict separation between internal and external security goals embedded in EU structures, policies and practices.

The ESS originally expressed the concept that "with the new threats, the first line of defence will often be abroad". Such concept has to be implemented by assessing the possibility for internal security actors to use CSDP activities for returns in internal security, and by considering JHA expertise as a crucial resource for EU foreign policy objectives such as promoting the rule of law and preventing state failure.[1]

How can we best direct investments towards research projects aimed at supporting the Union's internal and external security policies?

The selection should focus on the areas of intersection shared by internal and external security, for instance terrorism, organised crime (mentioned at the strategic level), but also the protection of critical infrastructures and response to natural and man-made disasters

[1] Florian Trauner, *The internal-external security nexus: more coherence under Lisbon?,* ISS Occasional Papers, March 2011, n. 89, p. 5, http://www.iss.europa.eu/uploads/media/op89_The_internal-external_security_nexus.pdf

(treated in implementation documents rather than strategic ones, and/or just under the competence of those institutions which are in charge of JHA and CFSP/CSDP domains) and other possible areas/sub-areas to be identified up to implementation levels.

The areas of possible intersection should be properly verified through an analysis comprising at least three priorities of research:

1. The first research priority is somehow "ontological" and should be conceived as a precondition of the following ones, therefore its realization should be set within the first phase of Horizon 2020.
   It should be devoted to the in-depth analysis of both strategic statements, starting from the wording of strategic and policy/normative documents, and the respective implementation documents. This will help to define in details the real contents of each domain, including also the "mandate areas" of those institutions in charge of JHA and CFSP/CSDP, behind the formal wording at strategic level.
   This should enable the definition of the real commonalities between an area X (for example terrorism) of internal security and the correspondent area X (again terrorism) of external security.
   In order to go beyond the wording used in strategic documents, it should be checked whether certain areas/sub areas mentioned only in the framework of external security (for example poverty) have in reality indirect effects on internal security (for instance by causing the conditions for large-scale illegal immigration towards Europe) although they are not formally mentioned in documents related to this domain.
   Investments could therefore be optimized within the real borders of these commonalities, thus favoring a "functional" security in certain areas/sub areas regardless their formal and direct links to internal or external security policies.

2. The second research priority concerns the level of formal competencies and functioning (decision-making) of EU and national institutions and agencies in the areas/sub areas of intersection identified by the first research priority. This research activity should be conducted also at technical-operational level, again both at EU and national level, regarding also the mechanisms, the capacities and above all the procedures that are currently available (especially when it comes to improve interoperability).
   The unavoidable areas of overlap and/or gap should be identified and managed with guidelines aimed at improving coherence and coordination among the variety of actors involved, bearing in mind that different situations require different solutions (at EU and at national level).
   It shall be considered the potentiality of the Lisbon Treaty to improve EU institutional coherence in the complex balance between internal security needs and external security goals. This kind of analysis should also comprise a review of the provisions laid down in the Lisbon Treaty relevant for internal and external security policies, which: a) are new and not yet implemented, for instance solidarity clause, permanent structured cooperation; b) are already foreseen in previous provisions but never implemented, for instance the CSDP civilian operations including civil protection; c) are under implementation, for instance the changes concerning the EU mechanism of civil

protection that will pave the way for more integration and better cooperation inside and outside the EU. Such analysis shall to reassess the viability of certain provisions and the possible measures to implement them.

3. The third research priority shall be devoted to map the technologies applicable to areas/sub areas of intersection identified by the first research priority. It shall aim to individuate shortfalls and direct investments accordingly, by avoiding duplication and taking advantage of double application of certain technologies.
   Such mapping should not be separated from an accurate consideration of dual-use domains, bearing in mind that technology itself is not military or civil but rather is the application to make the difference. This shall consider the synergies pursued by the European Framework Cooperation for Security and Defence among EC, EDA and ESA, whose overall aim is to prevent duplication between defence and civilian research in order to save resources, and to improve civil-military interoperability and standardization. This effort could also contribute to the process to define quality and size of security market in Europe, including the progressive extension of the dual-use segment, and the potential effect on the EU market itself.

Last but not least: in order to carry out the analysis described by the aforementioned research priorities, a proper involvement of relevant stakeholders is recommended at public and private, European and national, politico-institutional and technical-operational level, including experts and industry representatives, with the aim of identifying a “real” framework that will provide a basis for recommendations tailored to the “real” situation/needs.
Furthermore, it is recommended to provide proper access to relevant results of previous and current projects within the FP7, not only within the theme of security, but also concerning other fields (for instance former DG JLS).

i) Enhance standardisation and interoperability of systems, including those for emergency purposes

H2020 Text:

"Pre-normative and standardisation activities will be supported across all mission areas. Activities across all mission areas will also address the integration and interoperability of systems and services including aspects such as communication, distributed architectures and human factors, including those[3] for emergency purposes."

Introduction

The European Union, its citizens and its international partners are confronted with a range of security threats such as crime, terrorism and mass emergencies caused by man-made or natural disasters. These threats can span across borders and aim at physical targets or the cyberspace. Attacks against internet sites of public authorities and private entities, for instance, not only undermine the citizen's trust but may seriously affect such essential sectors as energy, transport, health, finance or telecommunications.

The increasingly rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats and the presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of Information and Communications Technology (ICT) systems and networks.

In the past few years security has quickly moved on, with areas such as cyber-security, cloud, mobile, machine-to-machine (aka internet-of-things) producing more requirements. We have seen demands placed by the growing threat of criminal activities and risks to critical infrastructure. In some cases, protection infrastructure may even get hijacked, to serve as a Trojan horse in order to attack protected infrastructure. Just to make an example, hackers are taking over an increasing number of security cameras to spread malware, break in to networks and to see what governments and businesses are keeping an eye on. To minimize exposure to risks, security must be built in from the beginning when designing new architectures, not added on later as an optional feature.

Sensitivity towards the privacy of the citizen, of his freedom and of his data is increasing but is lagging behind the rollout of new services and applications which depend on a culture of openness and sharing. Definitively, the user demand for open, quick, free access to services (transport, telecommunications, power supply, etc.) must be traded off with adequate privacy, security and data protection.

Interoperability entails the capability of different standards to be reciprocally compliant. In the context of Systems of Systems (SoS), interoperability is the ability of different types of

[3] "those": Missing in the original text; added.

computers, networks, operating systems, user terminals, network management platforms, telecommunication standards and applications to work together effectively. In this framework standardization in security implementation plays a key role.

Security is a common requirement for SoS, its standardization is essential to ensure interoperability among systems and networks, compliance with legislation and adequate levels of security. These standards provide the means for protecting the user, especially wherever and whenever cyber-security and data integrity also entail physical safety in a complex framework of "digital living". Security standardization is also a mean to create a more secure and profitable environment for the industrial sector, from SMEs to large global companies, and to provide benefits for a diverse range of interest groups: first-responders, communities, government and non-government organizations, research bodies, universities and so forth.

What needs to be done

Here follows a list of capacities that should be developed at local, regional, national and European level.

To foster radio interoperability based on IP protocols and spectrum harmonization[4].
Lack of interoperability in telecommunications is an urgent problem affecting every level of government as well as citizen trust in government. When different first-responder organizations convene at an incident scene, their radios are often mutually incompatible, since they operate over different frequencies and often use different technologies. Swapping radios and implement mutual-aid channels, and gateways that bridge two or more radio systems are partial solutions: none of them completely solves the inherent limitations of radio communications. Limitations include lack of standards (or, what is worse, multiple standard proliferation), exclusion of people using devices other than radios, inability to communicate from outside the radio range, and in some cases lack of resiliency of the radio infrastructure. Additional interoperability impairments may be encountered dealing with multiple nations' first-responders organizations, during cross-border operations and international cooperation.

An approach based on IP standards, including IMS, SATCOM, QoS and multi-level security, shall overcome these limitations.

Standardization at technological level shall also imply a specific activity at regulatory bodies' level to harmonize spectrum utilization at least at EU level, in order to overcome problems encountered by teams of first responders from different countries co-operating in a widespread, major emergency scenario.

[4] Reference to SERIT 2011 white book: TA2.3, TA2.5, TA2.6, TA2.7, TA2.9; reference to SERIT 2012 white book: "Interoperability", "Communication command and control and information systems".

To exploit IP protocols interoperability for implementing future-proof situation-awareness' information sharing, beyond radio integration [5] . When radio communications travel over IP networks like any other kind of voice, video, or data traffic, public safety agencies can communicate, collaborate, and coordinate response using any radio system, in any location with a connection to an IP network. Use of IP networks also enables public safety agencies to augment radio with other types of voice traffic as well as video and data, increasing situational awareness - including augmented reality contents - by delivering the right information to the right people at the right time and in the right format.

The inherent advantages of IP-standards, redundancy and resiliency, and scalability-are especially valuable in public safety environments.

Fast-deployable, delay-tolerant IP network segments, including security and QoS features should be developed, in conjunction with SDR and SATCOM evolutions.

Current evolution of LTE standard should be exploited in order to push introduction of non-consumer features like group-call and to enhance secure multicast and broadcast capabilities.

To exploit current and near-future technologies for legacy systems interoperability[6]. Interoperability endeavors must aim to develop new solutions compatible with legacy, current and near-future technologies (e.g. TETRA, DMR, Athena Fidus, Galileo, LTE). Backward compatibility with legacy systems and analog to digital interoperability, migration towards IPv6, interoperability among operators, service integration/portability shall also be pursued. In particular, it is necessary to design multi-network solutions assuring a transparent connectivity to the user in any circumstances, and able to improve the efficiency for public security operations, emergency care services, homeland security applications. Cloud computing being an opportunity, securing the cloud in a multi-level security framework becomes of the uttermost importance.

To leverage crowd-sourced data for security and safety[7]. The rise of crowd-sourced data is no surprise to anyone in business and government. The growing importance of social networks to support business initiatives has been documented many times over in the news media.
The implications of this type of data collection for early warning and/or confirmation of information – social media as a sensor – are significant if applied to the field of public safety. By combining social media data with geospatial analysis, officials may be able to

[5] Reference to SERIT 2011 white book: TA2.3, TA2.5, TA2.6, TA2.9; reference to SERIT 2012 white book: "Interoperability".
[6] Reference to SERIT 2011 white book: TA2.3, TA2.4, TA2.6, TA2.7; reference to SERIT 2012 white book: "Interoperability", "Communication command and control and information systems".
[7] Reference to SERIT 2011 white book: TA2.3, TA2.6, TA2.7; reference to SERIT 2012 white book: "Interoperability", "Communication command and control and information systems"; Wide-scale long-range multi-sensor surveillance.

prepare for and respond to a disaster faster than ever before. Sensory data when combined with social media data and/or sentiment analysis, provides both the "what," or that an event has just occurred or is about to occur, and the "who," the "why," and the "how" – or the context of an event, including the public's level of understanding, its reaction to and knowledge of factual information, may even assist in predicting second and third-level events that might arise as a result of the original disaster.

Despite the benefits of collecting crowd-sourced data during an emergency, it has not yet been adopted by incident response agencies for a variety of reasons. Many in the incident response community are reticent to social media data a valid information source. In large part, this is due to the difficulty (including data reliability and liability concerns) in processing the potentially vast amounts of data during a major operation.

However, new systems for situation awareness exploiting crowd-sourced data in a proper way, also integrating them with data collected from wireless sensors networks, from sensors embedded in smartphones and PDAs, and from conventional sensors are deemed essential in the future. Simulation and modeling "in-the-loop" may play a key role in properly understanding crowd-sourced data and in real-time decision support during crisis management.

To leverage geo-referencing and multimedia for security and safety purposes[8]. In today's world, texting has become second nature to most people. Current college students don't know a world without texting words, pictures, and videos. And even those college kids' grandparents are texting now. Texting is ingrained into everyday life now, so Public Safety Answering Point (PSAP) technology needs to evolve to catch up in order to meet the needs of today's wireless, mobile society. Text messages coming from e.g. a mobile phone are inherently geo-referenced.
Emergency/mass notification services (EMNS) are focused on the electronic activation and management of notification messages to groups or individuals, including first-responders teams, employees, citizens, residents, students/parents, customers, suppliers or government officials. EMNS can be used to organize contacts into an unlimited number of groups (including geo-referenced ones), to send emergency messages, to track receipts or responses for message delivery confirmation, and to perform workforce and citizen disaster relief management.

Systems for secure and reliable transmission of custom or previously crafted message to multiple endpoint devices, such as phones, PDAs, desktops, email systems, fax machines, desktops, physical security systems, facility management systems, public announcement systems (analog and digital TV, radio broadcast, radio amateurs) and, increasingly, to social media networks should be implemented at EU-wide level.

[8] Reference to SERIT 2011 white book: TA2.3; reference to SERIT 2012 white book: "Communication command and control and information systems".

To standardize ICT for health-care management. The information and communication technologies (ICT) play central role for the increased efficiency of the health-care systems and are the glue that connects together the different components of any modern health care system. ICT are crucial both for patient treatment as well as for cost reduction through adoption of telemedicine . This however demands for an additional effort of standardization and interoperability of systems among local, regional, national and international health-care providers.

To standardize and enforce procedures [9] **.**To enhance the capability to manage emergency and to coordinate heterogeneous teams, also standardization of procedures and languages (intended as symbolic) must be pursued.
In addition, in the realistic hypothesis of an emergency scenario with the presence of people (common citizens and/or operators) communication messages and information flow to citizens and among operators must be standardized in order to greatly improve effectiveness of the exploitation of the emergency management plans.

Lighthouse projects

Lighthouse projects are normally perceived as projects with the explicit goal of accelerating changes in perceptions and beliefs on a wide scale. We envisage the need of lighthouse projects in the area of improving integrated risk modeling and resilience of "system of systems", intended as a combination of critical infrastructures from different sectors, interacting each other. Two meaningful examples follow:

1) A project in the domain of radio communication for first responders and Law Enforcement Agencies with a view to transition from the old TETRA/TETRAPOL systems to a new communication system based on several interoperable components built around a security enhanced LTE standard and satellite systems;
2) A project demonstrating how urban security and citizen safety may be enhanced and enforced through multiple systems interoperability.

[9] Reference to SERIT 2011 white book: TA2.6; reference to SERIT 2012 white book: "Interoperability".

Security of the Smart Cities

H2020 Text:

"3.1.3. Foster European Smart cities and Communities
Urban areas are one of the largest consumers of energy in the Union and emit a correspondingly large share of greenhouse gases, while generating a substantial amount of air pollutants. At the same time, urban areas are affected by decreasing air quality and climate change and have to develop their own mitigation and adaptation strategies. Finding innovative energy solutions (energy efficiency, electricity and heating and cooling supply systems), integrated with transport systems, smart construction and urban planning solutions, waste and water treatment as well as ICT solutions for the urban environment are therefore crucial in the transformation towards a low carbon society.
Targeted initiatives in support to the convergence of industrial value chains of the energy, transport and ICT sector for smart urban applications need to be envisaged. At the same time, new technological, organizational, planning and business models need to be developed and tested at full scale according to the needs and means of cities and communities and their citizens. Research is also needed to understand the social, environmental, economic and cultural issues that are involved in this transformation."

Introduction

The concept of the Smart City takes into account that urban settlements can be considered as a network of networks that interact among each other and are mutually dependent; thus, a Smart City is founded on the reliability and the strict interconnection of its infrastructures, energy, ICT, mobility, etc.
Accordingly, the concept of smartness is strongly linked to the concepts of safety and security: in fact, a city cannot be smart if it is very vulnerable. Therefore, prevention and mitigation technologies as well as early warning and alerting tools play a key role in smartness, since key points are the mitigation of the vulnerability of urban areas (i.e damages suffered due to natural hazards and threats) and the improvement of their resilience.
The vulnerability of urban areas and of their infrastructures depends on their status: vulnerability status is affected by many different factors (as e.g. ageing of infrastructures or differential displacements or effects due to extreme weather conditions). Urban areas and infrastructures could be seriously damaged even by events whose impact would be negligible in "normal situations" when their status is "optimal". These considerations bring the necessity to perform long-term assessment of the status of cities and of the embedded infrastructures in order to "monitor" their time-behavior taking into account the multiplicity of the risks/hazards and point to the necessity of "scenario analysis" tools able to support the City managers in long term planning of the City and Infrastructures evolution.

For these reasons current management of urban areas as well as early warning, alerting systems crisis management systems (in a first instance, quick damage assessment) and scenario analysis / planning tools should be seen as a whole in terms of necessities and opportunities. This holistic approach not only avoids duplications but allows too to share costs (e.g. monitoring systems allow to plan ordinary/extraordinary maintenance and by this way to get saving).

What needs to be done

Due to the pervasive presence of infrastructures in the urban areas, Smart City security requires:

- Integration of different sensing technologies to provide the monitoring, surveillance and the quick damage assessment. In this frame, efforts should be focused to build "a toolbox" of different observation technologies, whose integration should be performed so to deal with different infrastructures and type of hazards. The most promising techniques are the ones based on the remote and not-invasive sensing as the electromagnetic and acoustic ones, possibly to be integrated with the usual systems (video surveillance,..).
- Adaptive Wide Area Surveillance and Monitoring Systems, developed integrating ground based, airborne and satellite based technologies with navigaton technologies and ICT In this way, a new concept of an integrated monitoring should be developed and tuned to the different types of urban areas, infrastructures and hazards/risks.
- The interoperability of the different monitoring systems so to allow the information transfer among them and with a command and control center supervising all the network of the infrastructures and related monitoring systems
- Common operational monitoring protocols, for the most relevant typologies of infrastructures and risks, so that sensing techniques can be deployed in cascade depending on the status of the infrastructure and the observed urban scenario.
- The improvement of ICT tools able to control the single monitoring system in order to provide real time information about the "status" of the infrastructures and the urban territory
- The improvement of the usage of mobile devices both as non-traditional distributed sensors and as ubiquitous and real time information channel for citizens during normal life and crisis events.

Main areas for Research Projects are:

Smart City is a critical Infrastructure. Smart Cities rely on digital infrastructures and information generated and distributed through them. There is a significant convergence between resilience and continuity issues of Critical Infrastructures and of Smart Cities, with the major difference that Smart Cities always are densely populated areas and therefore have to deal with problems in term of goods provisioning, evacuation, public health, etc. The identification of infrastructures needed for the orderly functioning of a Smart City must be part of the definition of the Smart City itself even if it is not one of the "traditional" smart infrastructures (e.g.: financial, GPS, Tetra, etc.).

Improved resilience design of critical infrastructures has to be promoted so to reduce their vulnerability against natural and man-made hazards, also taking into account cascading effects.

The protection of these infrastructures must be assured through prevention and mitigation technologies as well as early warning and alerting tools, taking advantage from opportunities provided by the development of systems, which are able to couple current monitoring and quick damage assessment and are based on state-of art non-invasive sensing technologies combining ground based, airborne and satellite observations and ICT concepts (cyber intelligence, analytics, threat detection, etc.)

New and smart European early warning and alerting systems as well as crisis management systems have to be based on an accurate knowledge of the status of the infrastructures. In this framework, the assimilation of monitoring data into the structural modeling of infrastructures plays a key role, since, by this way, it is possible to update the current assessment of the infrastructure vulnerability and to develop all the necessary actions.

Adaptive Wide Area Surveillance and Monitoring Systems should be developed, integrating ground based, airborne and satellite based technologies. In this way, a new concept of an integrated monitoring will be developed and tuned to the different types of infrastructures and of the hazards/risks. Operational monitoring protocols have to be defined so that sensing techniques are deployed in cascade (from the cheapest one up to the more expensive ones) depending on the status of the infrastructure and the observed scenario.

The sharing of costs is very important in order to ensure the sustainability: the approach that couples current monitoring with quick damage assessment allows to plan ordinary and extraordinary maintenance, reducing not only the vulnerability of the infrastructure but also the costs that in any case, have to be devoted to infrastructures long term maintenance.

In this framework a key point is represented by the development of an integrated observational system able to couple current monitoring, alerting systems and quick damage assessment . It will be based on the integration of observing capabilities (both ground based airborne and satellite based) with navigation, TLC and ICT technologies and on the development of new observational platforms (e.g. UAV) and new advanced observing technologies (as new non-invasive sensing technologies, low cost technologies, “sensors not sensors” , dust of sensors, etc.). The use of “not sensing instrumentation” as sensors opens new frontiers, particularly when linked to the increasing use of mobile advanced technologies by citizens, and to information sharing. Moreover improved and ubiquitous connectivity will allow to “use” citizens themselves as a real integrated suite of sensors, which can be very useful both for current monitoring and crisis management.

New federated and scalable ICT architectures have to be developed in order to obtain a high observational flexibility; to support advanced data processing (e.g. High Performance Computing, Grid/Cloud Computing, etc.) of information delivered by heterogeneous sources (extraction, classification, semantic analysis, correlation, fusion); to exploit the opportunities offered by web (web sensors, web services, etc.) and to provide effective technological indicators at support of the decision from stakeholders.

Data management must guarantee both real time situational awareness for wide areas (by real time data gathering and integrating from different data sources) and full and open

access of citizens to data and real time information dissemination to citizens (everywhere and every-when).
Standardization and interoperability are key points not only for the efficacy of operations but also to guarantee economic sustainability of monitoring systems allowing the data sharing and development of services by many different end-users. Great attention should be devoted to the interoperability among different monitoring systems, which are in charge of different stakeholders.

Smart City needs to manage crises and disasters.. Cities may be the likely target of a crisis or a disaster and a Smart City must be able to perform better of a traditional city when facing a crisis event.
The ways through which a Smart City implements resilience and/or mechanisms to cope with crises and disasters must be part of the design of the Smart City itself. These mechanisms will rely on the more extended availability of information that is typical of Smart Cities and on the presence of many systems to acquire sensors data, evaluate warnings, streamline processes and flows, distribute information and provide advice or mandatory indications on the behaviors to follow during a crisis event (e.g. integrate ground based, airborne and satellite based technologies with position and navigation technologies and with ICT, exploiting opportunities offered by web and mobile based tools).
Development of prevention and mitigation technologies and the design for an improved resilience have to be addressed in order to reduce the vulnerability of urban areas and infrastructures.
New Concept of Operations have to be developed, covering both the whole crisis management chain and societal resilience.

Early warning and alerting systems will take advantage from the development and standardization of technological solutions able to couple the capabilities of quick damage assessment and long-term monitoring. New systems will greatly benefit from incorporating information delivered by a large arena of different sources so to allow combined capabilities of current monitoring, alerting capability and crisis management. The new advanced Adaptive Wide Area Surveillance and Monitoring Systems, which integrate ground based, airborne and satellite based technologies with position and navigation technologies and with ICT (exploiting opportunities offered by web based tools), will be crucial for from awareness, preparedness and recovery phase.
Data interoperability and real time data access is crucial both to improve data gathering and information distribution in order to guarantee real time situation awareness and to deliver real time and multi-content information to stakeholders and citizens.

In a crisis systems continuity and on-going interoperability must be preserved and emergency communications must be guaranteed. The options available to permit communications interoperability across different networks and protocols to maximize the capability of the city to manage the event and bounce back must also be a focus of this mission.

Smart City should ensure privacy and freedom and be inclusive. Many of the topics considered of interest in this area are relevant to ore feature particular characteristics in the Smart Cities environment:

- The socio-economic dimension: public security vs. crime costs in Smart Cities where multiple systems and intelligence information should be available
- The cultural and anthropological dimensions: the inclusion focus in Smart Cities should help address the culture and community building issues caused by immigration, values diversity, beliefs
- The security and architecture dimension: the introduction of security systems should be part of Smart Cities planning and lead to reducing risks due to spatial segregation while enhancing opportunities to mix and exchange
- The role of media and communication: design the Smart Citizen interaction systems to maximize the distribution of information and of crisis indications

Lighthouse projects

Smart Cities improved resilience to crisis and disasters

A Smart City must be able to perform better than a traditional city when facing a crisis event. The ddevelopment of prevention and mitigation technologies able to reduce vulnerability and cascading effects, and the design for an improved resilience and of mechanisms to cope with crises and disasters must be part of the design of the Smart City itself. These mechanisms will rely on the extended availability of information and on the development systems able to manage in Real Time (RT) large data fluxes (integrating ground based, airborne and satellite based observation technologies with position technologies and with ICT, exploiting opportunities offered by web and mobile based tools and using citizens themselves as sensors), evaluate warnings, distribute information and provide advice or mandatory indications to the population. New Concept of Operations will developed covering the whole crisis management chain and taking aadvantage by the development and standardization of technological solutions able to couple quick damage assessment and long-term monitoring. Data interoperability and RT data integration is required in order to improve data gathering and information distribution to guarantee RT situation awareness and to deliver RT and multi-content information to stakeholders and citizens.

Integrated and Participated Security in Smart City

The necessity of security of citizens in urban areas has several peculiarities due to the high density population in these areas and, at the same time, the opportunities that the joint ubiquitous presence of citizens and their mobile tools offer. Therefore, the development of an integrated surveillance system based on technologies non-invasive and compliant with privacy issues, represents key tool for an improved security both during ordinary functioning and crisis events. The other scientific/technological challenge regards the deployment and improvement of the mobile systems as tools to gather information about crisis scenarios and to provide the citizens with reliable information for a participated crisis management.

"5.6. Cultural heritage

H2020 Text:

"Cultural heritage assets are unique and irreplaceable in their tangible form as well as in their intangible value, cultural significance and meaning. They are a major driver of societal cohesion, identity and well-being as well as contributing significantly to sustainable growth and job creation. However, Europe's cultural heritage is subject to deterioration and damage, further exacerbated by increasing exposure to human activities and extreme weather events resulting from climate change as well as due to other natural hazards and disasters.

The aim of this activity is to provide knowledge and innovative solutions, through adaptation and mitigation strategies, methodologies, technologies, products and services for the preservation and management of tangible cultural heritage in Europe at risk from climate change.

To achieve this, multidisciplinary research and innovation will focus on the following:

5.6.1. Identifying resilience levels via observations, monitoring and modelling

New and improved damage assessment, monitoring and modelling techniques will be developed to improve the scientific knowledge-base of the impact on cultural heritage of climate change and other environmental and human risk factors. The knowledge and understanding generated with the help of scenarios, models and tools, including analysis of the perception of value, will help provide a sound scientific basis for the development of resilience strategies, policies and standards, within a coherent framework for risk assessment and management of cultural heritage assets.

5.6.2 Providing for a better understanding on how communities perceive and respond to climate change and seismic and volcanic hazards

Research and innovation will, through integrated approaches, develop resource efficient solutions for prevention, adaptation and mitigation, involving innovative methodologies, technologies, products and services for the preservation of cultural heritage assets, cultural landscapes and historic habitats. "

The need to ensure the Safety of cultural heritage and built environment has a tremendous social and cultural impact, as evidenced in occasion of some recent events like the earthquakes in Abruzzo (2009) and in Emilia Romagna (2012) as well as the

series of damages that have caused the collapse of one of the archaeological sites most important to the world as Pompei.
This necessity has an ambivalent character regarding both the Safety, with reference to the risk associated with environmental changes and natural disasters, and the Security, with respect to damages due to human acts and, in particular, to criminal and terrorist events. Furthermore, the fruition of cultural heritage asks for Safety conditions for the users as, for example, visitors of a museum or an archaeological site.
The need of an integrated approach to Security of the two areas (cultural heritage and built environment) is well pointed out by the 2012 UNESCO Recommendation on the Historic Urban Landscape; UNESCO Recommendation sees the historic urban landscape urban area as a result of historical stratification of cultural and natural values, which go beyond the usual concept of "center" or "ensemble", so as to include the broader urban context and its geographical location. This wider context includes the topography, geomorphology, hydrology and natural features of the site, its built environment, both historical and contemporary, its infrastructure above and below ground, its open spaces and gardens, its models of land use and spatial organization.
With respect to the above sketched model, Confindustria Innovative and Technological Services and the Industry and Culture Foundation, in order to increase the Italian participation in European research programs in the field of the cultural heritage, promoted the creation of the Italian Technology Platform for the Cultural Heritage (CH) "IPOCH2" attended by over 130 companies, universities and research centers Italians, whose themes are of great interest for the protection and Safety of both the cultural heritage and new built. In addition, the Focus Area Cultural Heritage (FACH) of the European Construction Technology Platform (ECTP) states that the protection of cultural heritage is one of the significant social needs at European level. Furthermore, the technological Platform “Security Research in Italy (SERIT) ”, focused to the thematic of the Security and promoted jointly by CNR and Finmeccanica, has identified the “Integrated Security of the Cultural Heritage and Built Environment” as one of the application sectors of national priority. At the present stage, SERIT is attended by over 250 partners and more than 1000 members.
It should be emphasized that the Safety requirements are at the basis of the new concept of "Smart Cities" and cut across the fields of "smart mobility, smart culture and smart environment" in order to ensure a balanced and well-behaved development in urban and metropolitan areas.

From a technological point of view, the need for Safety and Security requires a multiform action able to account for both the heterogeneity of environmental hazards (climate change, seismic, hydrogeological, ..) and human factors, and to provide its impact in all the different life phases of the cultural heritage and built environment. It follows that most part of the enabling technologies is common to the two areas and should comply with the relevant need of non-invasiveness.
In this frame, the development and use of the observation and sensing technologies are very important in order to ensure a long-term monitoring of the cultural heritage, which is necessary for a proper maintenance planning and programming of the interventions of consolidation, restoration and retrofitting. The other stringent need is concerned with the

possibility of a quick damage assessment, which requires the development and use of sensing/observation technologies for a fast evaluation of the status of the structure and for the identification of anomalies in the dynamic behavior of the structure.

Main areas for Research Projects are:

Security and sustainability of cultural heritage and built environment. The cultural heritage represents a priceless treasure for our country so that all aspects regarding actions to prevent critical situations and ensure Safety during crisis events are focal points of interest. Such issues are concerned with cultural heritage (movable, immovable, archaeological and natural) and built environment and involve both Safety issues, with respect to risks related to environmental changes and natural disasters (floods, earthquakes, landslides, fires), and Security issues with respect to human influences on them.

Looking specifically at fruition processes, the valorization approach should take into account models and guidelines as the ones included in management plans of UNESCO sites. The visitors Security has also to be ensured and a crucial point regards the design and implementation of tools for handling situations related to tampering or theft. In fact, the symbolic value of cultural heritage, which represents the identity of a people, makes them very attractive as targets of the terrorist phenomenon (bear witness to the attacks against the Uffizi Gallery and the Basilica of St. John Lateran). Not less important are the movement issues relating to conditions of handling and risks that can lead to situations during transport. The protection of cultural heritage sites requires an integrated strategy based on the synergic combination of different techniques and rises a series of important technical/scientific challenges: in fact, systemic approaches are needed with the aim to identify and integrate methodologies and technologies, suitable for dealing with complex systems, such as the archaeological sites. Unfortunately, recent experiences have shown, as a low attention is due to the proper planning and implementation of preventive measures necessary for the protection of cultural heritage: therefore, it is necessary to adopt organizational strategies supported by technological tools that make it possible to significantly reduce the risks.
Research and innovation efforts should be done for the promotion and improvement of the Safety of the built environment (also in cultural heritage contexts) through monitoring strategies for the efficient maintenance and prevention against natural hazards (earthquakes, landslides ..) and human factors. The results of the monitoring should be used even as “constraint and input data” to structural models of the heritage so to improve the prediction capabilities of these structural models about the vulnerability assessment. The long-term monitoring is also important to ensure early warning detection capabilities in the case of inadequate planning and to get information on construction methods and on the deterioration status also due to normal aging. The monitoring of the slow movements of the structures and of the deformation of the surrounding territory is also necessary even for the identification of patterns of behavior of structures in relation to exposure to different types of risk. In addition, the diagnostic tools are important for the verification of the

goodness and effectiveness of reinforcement operations and pose interesting scientific challenges related to the need to monitor new materials behavior.
In addition, the need for a quick damage assessment, after a crisis event , requires a fast analysis of the status of the structure also in terms of dynamic behavior. This need is particularly felt in the first operational phases of the crisis, because it has impact on both prioritization in planning interventions, and for a situational awareness.

Sub-thematics

- **Monitoring and quick damage assessment of cultural heritage and built environment**

  Research efforts should be made to allow the implementation of systems able to couple both the monitoring and the quick damage assessment for both the cultural heritage and built environment. This calls for development and integration of sensing/observation techniques, with a null or low-level of invasiveness, able to perform a monitoring, which has to be: continuous in time, capable of a rapid and/or on-demand diagnostics, multi-sensing, multi-scale (global view of the and structure of the area and detailed diagnostics of single parts of the heritage) multi-resolution, multi-depth approach Main key ingredients are requested like: advanced systems based on wireless networks, ICT system architecture, integration of non-invasive diagnostic techniques based on electromagnetic and / or acoustic sensing.

- **Control and monitoring of the works to the public and the Safety of visitors**

  Efforts should be performed for the development of integrated systems designed to ensure the Safety of the heritage (movable, immovable, archaeological and natural) during exhibits, against tampering, environmental alteration or theft, natural disasters (floods, earthquakes, landslides, fires) or sudden failures. Development of integrated systems should be performed so to ensure the Safety of visitors and of the exhibited works and also to increase the Security conditions of the fruition (natural or archaeological sites) by means of tools for the individual identification of the visitors. In particular, the Safety of people and visitors of archaeological sites and museum buildings arises to main issues. The first one is concerned with the design and implementation of technologies based on the analysis of time-related observations for: automatic recognition of people, the automatic analysis of scenes and the identification of potential non-licit behaviors. The second one is concerned with the issues of privacy of individuals.

- **Systems for the integrated management and remote Security of movable works**

  Efforts should be performed to set-up strategies able to ensure the Security of the movable heritage during transport, with a particular focus to ICT tools to:

  - enhance the Safety of cultural heritage in the areas of fruition and during transportation, by means of traceability and monitoring of the visit, integrated

planning in the frame of the Emergency Plans (identification of objects and procedures for emergency evacuation);

- carry out a time-continuous monitoring in order to mitigate risks during emergency transport;
- support organizational aspects: impact assessment and development of protection schemes of the artistic furniture.

- **Emergency management in occasion of criminal acts and disasters**

  Efforts should be performed for the development of techniques able to efficiently perform a crisis management in order to avoid permanent damages. The focus should be given to the study of tools, such as robotics for targeted interventions, and to enhance the capability of a dynamic survey and planning of interventions so to properly act even in crisis events. In this frame, state of art and novel observation technologies should be improved as a first step of a strategy able to: monitor in real time the evolution of the phenomena; use predictive and simulation techniques; provide fast and appropriate response plans. Finally, for a reliable crisis management, a key factor is the training: in this frame, it is important to evaluate the effectiveness of software tools to provide total immersion and virtual environments or serious gaming techniques.

In Summary

MISSIONE	Progetti Proposti	Keywords Horizon 2020	Keywords SERIT	Indicazione delle Tecnologie (sulla base delle pubblicazioni SERIT) per la proposizione di progetti	CSA/ CP (STREP) / IP / DEMO
1 -Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs	European information platform for fighters against organised crime and terrorism	Preventing and fighting organised crime and terrorism; Cooperation among Law Enforcement Agencies; Interoperability and standardisation; Exchange of standardized data, tools and processes;	Interoperability Architectural models and technologies for fusing, processing and presenting	Interoperable platforms for sharing relevant information; Techniques for secure data exchange; Data Processing techniques	DEMO
1 -Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs	Definition of a common ontology for the law-enforcement domain		Knowledge Management Ontologies	Semantic Technologies for description, classification and identification of relevant information; Semantic Web Engine – Ontologies, Reasoning, Spatial Mining	CP
2 - Protect and improve the resilience of critical infrastructures, supply chains and transport modes	integrated risk modeling of "system of systems"	critical infrastructures, threats, good functioning	transportation security, energy security, cyber security, agro-food security, health security	Survaillence and Situation Awareness, Communications, Detection & Identification Systems, Technologies for Crisis Management and for the Protection of People, Assets and Infrastructures, Information Processing and Management	IP/DEMO
2 - Protect and improve the resilience of critical infrastructures, supply chains and transport modes	resilience of complex cyber – physical systems	critical infrastructures, threats, good functioning	transportation security, energy security, cyber security, agro-food security, health security	Survaillence and Situation Awareness, Communications, Detection & Identification Systems, Technologies for Crisis Management and for the Protection of People, Assets and Infrastructures, Information Processing and Management	IP/DEMO
3 - Strengthening Security Through Border Management	Secure and Trusted Public Regulated Regional Traffic Monitoring Service	rapid identification, marine and coastal border security, surveillance, border management, cooperation, EUROSUR, CISE	sicurezza e dei confini, cooperazione, sorveglianza integrata	TA1.2, TA1.6, TA1.8, TA1.10, TA5.1, TA5.6	IP
3 - Strengthening Security Through Border Management	Realtime screening systems for contaminants in bulk food	enhance systems, equipments, tools, processes, and methods for rapid identification, food security	Sicurezza agroalimentare, dogane, porti, varchi transfrontalieri, sicurezza nei sistemi di logistica avanzata degli alimenti	TA1.2, TA5.1, TA5.6, TA6.1, TA6.2, TA6.3, TA6.4, TA6.7	CP/IP
4 - Improve Cyber Security	Protection mechanisms against social engineering attacks	social interaction; cyber-attacks across multiple domains and jurisdictions	cyber intelligence via information management; cloud security	Secure and resilient ICT systems (data security); Monitoring methodologies and systems for detecting anomalies, unauthorized access attempts, and incidents in large networked ICT architectures	IP/CP
4 - Improve Cyber Security	Cyber-security and Resilience of Heterogeneous, Inter-Operating, Critical ICT Infrastructures	interoperability of multiple technologies; resilience; real-time detection of cyber-attacks	cyber intelligence via information management; mobile security; cyber-physical protection systems	Secure and resilient ICT systems (data security); Monitoring methodologies and systems for detecting anomalies, unauthorized access attempts, and incidents in large networked ICT architectures; Platforms, architectures, and algorithms for real-time analysis of massive data volumes (high performance computing)	IP/CP
5. Increase Europe's resilience to crises and disasters	Unmanned ground platform in disaster governance	Emergency management, civil protection, humanitarian aid, rescue	Ground Platforms - Unmanned ground vehicles	Cognitive and autonomous capabilities - Human-Robot Interfaces	CP
5. Increase Europe's resilience to crises and disasters	Adaptative Wide Area Surveillance and Monitoring systems	Emergency management, civil protection, disaster prevention/prepardness, post-stabilization	Space, airborne and ground remote sensing, interoperability	Sensor related imaging and mapping techniques	IP
6. Ensure privacy and freedom, including in the Internet and enhancing the societal legal and ethical understanding of all areas of security, risk and management	Inclusive Security	Societal issues, legal issues, ethical issues, citizens's perception	Biometrics, Automated Border Crossing, self-accreditation	Facial Recognition, digital signal processing technology	DEMO
6. Ensure privacy and freedom, including in the Internet and enhancing the societal legal and ethical understanding of all areas of security, risk and management	Legal and Ethical Aspects of Biometric Data International Sharing	Privacy, international law, proportionality, human rights	Data processing, confidentiality, critical infrstructures	Related biometric equipments, Biometric data management, Secure and privacy-aware distributed computation	DEMO
7 - Enhance standardisation and interoperability of systems, including for emergency purposes	Radio communication for first responders and Law Enforcement Agencies	Critical Infrastructure Protection, standardisation, dual-use technologies to guarantee interoperability between civil protection and military forces and amongst civil protection forces worldwide, Crisis management / civil protection	Communicazioni, interoperabilità, Tecnologie per Crisis Management	Interoperability, Communication command and control and information systems	CP/IP
7 - Enhance standardisation and interoperability of systems, including for emergency purposes	Urban security and citizen safety	Critical Infrastructure Protection, interoperability, Crisis management / civil protection	Communicazioni, interoperability, Sicurezza e sostenibilità del costruito,Tecnologie per Crisis Management	Interoperability, Communication command and control and information systems	CP/IP