

The Italian Technological Platform on Security

SERIT – SEcurity Research in ITaly

Cristina Leone and Fabio Martinelli

www.piattaformaserit.it



Agenda

- 10.30-10.50 Saluto del Presidente del CNR e del Sindaco di Napoli;
- 10.50-11.40 Presentazione del Documento Serit (ing. Cristina Leone e dott. Fabio Martinelli)
- 11.40-12.00 Presentazione relativa a H2020 con riferimento alla Societal Challenges nella quale ricade la tematica Security (dott. Angelo Marino Head of Unit Security Research Commissione Europea)
- 12.00-13.30 Tavola Rotonda: Le opportunità di finanziamento per le tematiche "Security in H2020" (con particolare riferimento al ruolo della ricerca e dell'industria nell'Italia Meridionale)
- Presiede: Angelo Marino
 - Controammiraglio Leonardo Bianchi, Vicedirettore IV Reparto di SEGREDIFESA, Ministero della Difesa;
 - Assessore Guido Trombetti, per la Ricerca scientifica, Statistica, Sistemi informativi ed Informatica, Regione Campania;
 - Dott. Marco Conti, Direttore Dipartimento Ingegneria ICT e tecnologia per l'Energia e Trasporti, CNR;
 - Ing. Massimo Claudio Comparini, Chair della Piattaforma Tecnologica Spazio Spin-IT;
 - Dott. Paolo Graziano, Presidente Unione Industriali Napoli.
- 13.30-14.30 Lunch 14.30-15.00 Presentazione dell'IREA (ing. Riccardo Lanari)
- 15.00-15.30 Serit Award (ing. Michela Alunno Corbucci)
- 15.30-15.45 Presentazione dell'iniziativa Dottorato in ambito SERIT (prof. Luigi Romano)
- 15.45-16.00 Saluti finali (Cristina Leone e Fabio Martinelli Co-chair Piattaforma SERIT)



Outline

- The Italian Technological Platform on Security Research (SERIT)
- The SERIT volume 2013 for H2020



SERIT – SEcurity Research in ITaly

SERIT is the **Italian Technological Platform**, jointly launched by CNR and Finmeccanica, which brings together Italian **industries** (both large industries and SMEs), **academia**, **research centers** and **end-users**, in order to promote and develop a **Research Agenda for future technological developments**, answering to the identified **National Security needs**.



High Level Objectives

Reinforce National and International Cooperation and competitiveness:

- SERIT aggregates a number of experts and competencies under different domains, stimulating a fruitful network among stakeholders, users, technologies experts and national institutions.
- SERIT promotes a dialogue with end-users and national stakeholders to bridge the industrial and academic research with the real needs and requirements expressed by users.
- SERIT acts as a catalyst to access to both national and European funds for research.

Promote the development of Human resources in Security research:

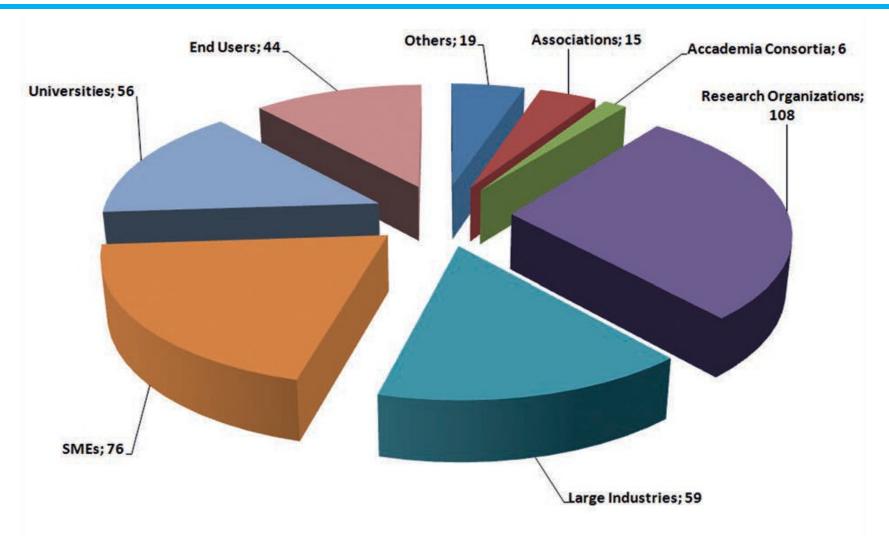
SERIT aims to promote and to develop the human capital in security, by promoting and supporting PhD. in collaboration with industries and academic members of the platform, in order to maintain the national excellences and the know-how in security research.

Contribute to the national technology development and innovation:

SERIT has defined a national technology roadmap that is under continuous refinement.



SERIT is composed by more than 300 members





A sample of SERIT members

Partial list of members:

- Companies: Finmeccanica (Alenia Aeronautica, Ansaldo Energia, Ansaldo Nucleare, Ansaldo STS, SELEXELSAG, SELEXGALILEO, SELEX SISTEMI INTEGRATI, SELEX SEMA, SESM, Telespazio), Akhela, Almavivaitalia, Calzoni S.r.l., Centro Ricerche Fiat, D'Appollonia, Engineering, Gilardoni, Intecs, Thales, Thales Alenia Space, VARLIFE, Vitrociset, ...
- **SME:** A.I.TECH., AIEM, Araknos Situational Awareness Systems, ASTER, ELESIA, Fondazione Graphitech, Kee Square, Mobilway, Ninmbus, PQE, Planetek, Resitech, ...
- RTO: CNR (DPC, GE, IAC, IAMC, IASI, IBAM, IBP, ICAR, IDASC, IEIIT, IIT, IMC, IMEM, INO, IREA, ISMN, ISPA, ISSIA, ISTI, ISTC, ITB, ITIA, DET, DM, IMAA), Centro di Studi sul Rischio, Cira, ENEA, INFN, Istituto Superiore di Sanità, NATO Undersea Research Centre, Semeion, SiTI, Tecnoalimenti, ...
- Universities: Bologna, Cagliari, Campus Biomedico, Cattolica del Sacro Cuore, Firenze, Genova, Napoli, Napoli Parthenope, Padova, Parma, Salerno, Sapienza, Seconda Università degli Studi di Napoli, Tor Vergata, Udine, Politecnico di Torino, ...
- Scientific Consortia: CINI, CNIT, NITEL, ...
- Consortia:, Filas, IAI, Sinergie-italia, ...
- End-user: ENAV, ATAC, ...
- Categories: AIAD, A.I.M.C, Confapi, Covalori, FEDERALIMENTARE, ...



SERIT – a Matrix Organization Technological Areas and Sectors

SERIT had been organized according a **Matrix** structure composed by **8 Sectors** (representing the different area where Security needs to be investigated in Italy) and **7 Technological** Areas (identifying the technological priorities).

The structure has been **aligned** with a wider **European strategic vision**, always keeping into account the national requirements and priorities identified, by SERIT Members.

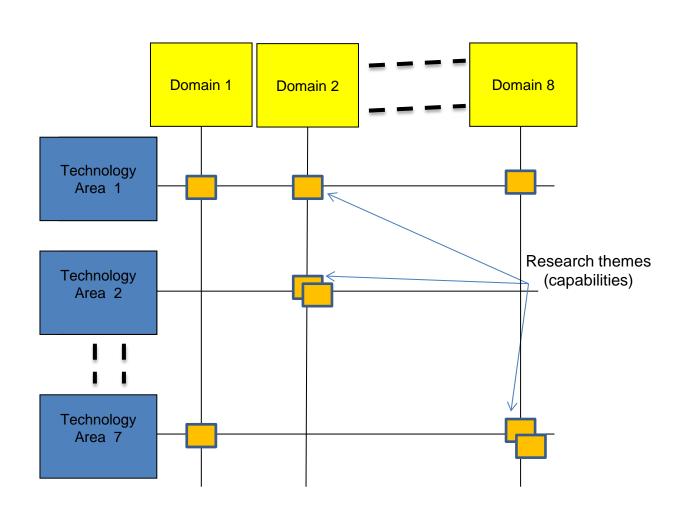


Matrix

Situation Awareness Cultural heritage and Building protection Communications System Security **Transportation Security Smart Cities Security Agrifood Security Detection & Identification Borders Security** Security Cybersecurity **Information Technologies** Health **Energy Supply** Technologies for Crisis Management & People, Assets and Infrastructures Protection **CBRNE** Legal & Etical Issues

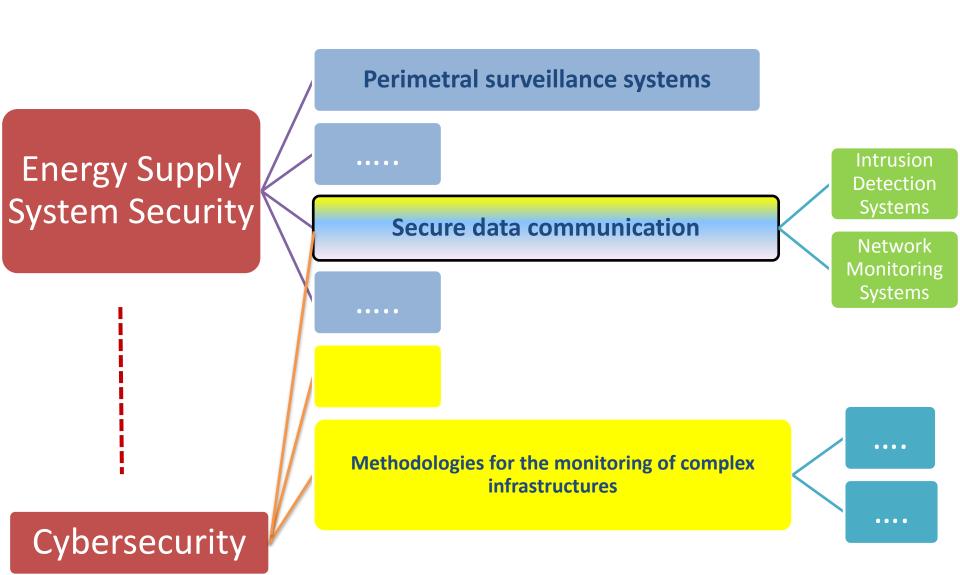


Methodology: how to develop Technologies enabling the needed capabilities for each Domain





Example





- Railway Security
- Multi-modal Transport
 Security
- Road Transport Security
- Maritime Security

 Integrated solutions for Energy Infrastructures protection

- Interdependent Energy Infrastructure Simulation and Vulnerability Analysis
- Diagnostic and control of Energy Infrastructures
- Smart Grids Cyber Security





- Airport Security
- Border Surveillance
- Luggage Inspection and people scan, including biometric systems
- ATM security
- Surveillance of maritime borders

- 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





- Emergency Management
- Security in Hospital
- Security Products-Pharmaceutical Processes
- Resilient health care system
- Standardization and interoperability

- to ensure the integrity of the supply chain
- to prevent the manipulation and alteration of food along the same
- Quick contaminant detection





- Safety and sustainability of the Built Environment
- Cultural Heritage Protection

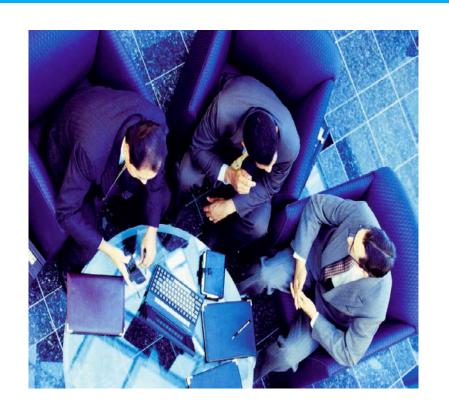
- Smart Cities Security Framework
- Urban Security Innovation







End Users



- The active involvement of end-users within the Platform is an essential element
- Creation of a Liaison
 Committee
- Increased involvement of End Users



For 2013, SERIT for H2020

- We considered the timing for Horizon 2020 (H2020) and the possibility to contribute to the topic definition
- We thus decided to have our annual research agenda in English for the first time!



STATUS ...

- The platform is in continuous growth
 - From 50 to more than 300 institutes/departments/organizations since 2011

Some results:

- Formal recognition from MIUR as an Italian Technological Platform
- Communication strategy based on web site, newsletters and mailing list (more than 1200 addresses)
- Two research roadmaps (2011/2012) published and presented to the Italian community
 a position paper for H2020 delivered to Italian Institutions (Feb. 2013) and volume
 2013 to be presented today
- Fostering a culture for competitive funding acquisition (several research projects proposals have been created -both at national and international level)
- Institution of a SERIT label for PhD fellowships (two awarded from University of Naples)
- The Security research day organized at CNR on June 27 2012 with the cooperation of APRE
- The creation of the SERIT Award (won by IREA for 2012)
- This third annual meeting ...
- ... and the consolidation of the Italian community!



SERIT Volume 3 Position paper on H2020



The H2020 New Structure

Horizon 2020 Priorities

Excellence Science

- European Research Council
 - Frontier research by the best individual teams
- Marie Curie actions
 - Opportunities for training and career development
- Future and Emerging Technologies
 - Collaborative research to open new fields of innovation
- Research Infrastructure (including e-infrastructure)
- Ensuring access to world-class facilities

Industrial leadearship

- Leadership in enabling and industrial technologies
 - ICT, nanotechnologies, materials, biotechnology, manufacturing, space
- Access to risk finance
 - Leveraging private finance and venture capital for research and innovation
- Innovation in SMEs
 - Fostering all forms of innovation in all types of SMEs

Societal Challenges

- Health, demographic change and wellbeing
- Food security, sustainable agriculture, marine and maritime research & the bioeconomy
- Secure, clean and efficient energy
- Smart, green and integrated transport
- Climate action, resource efficiency and raw materials
- Inclusive, innovative and secure societies

European Institute of Innovation and Technology (EIT)

Combining research, innovation & training in Knowledge and Innovation Communities

Joint Research Center (JRC)

Providing a robust, evidence base for EU policies



H2020 proposed budget

	Compromise %
I Excellent Science, of which:	31.73
II Industrial Leadership, of which:	22.09
1. Leadership in	17.60
2 Risk Finance	3.69
3SME's	0.80
III Societal Challenges, of which:	38.53
1. Health	9.70
2. Food quality	5.00
3 Energy	7.70
4 Transport	8.23
5. Climate	4.00
6Inclusive Societies	1.70
7. Secure Societies	2.20 (1,54€)
Science with and for society	
·	
Others, including Science with and for society, EIT, JRC, Non-nuclear	7.65
Total	100.00 (70.2B€)

.



Specific thematics addressed by SERIT

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
- (g) support the Union's internal and external security policies;
- (f) enhance the societal dimension of security and ensure privacy and freedom in the Internet
- (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



Methodology: how to develop Technologies enabling the needed capabilities for each Domain

Domain 1

Domain 2

Domain 8

Research themes

(capabilities)

In 2011, SERIT was mainly focused on the identification of those required capabilities at National level, through the jointly activities among Sectors (application domains) e Technological Areas representatives (results presented in vol.1);

evaluation of TRL, and innovation as a result of

technological roadmap



Technology Area 7 In 2012, on vol.2, SERIT SERI On vol.3, SERIT has presented the Research identified the research Priorities definition process, gap priorities to be promoted analysis, costs associated for further developments, as National priorities to Horizon 2020

Technology

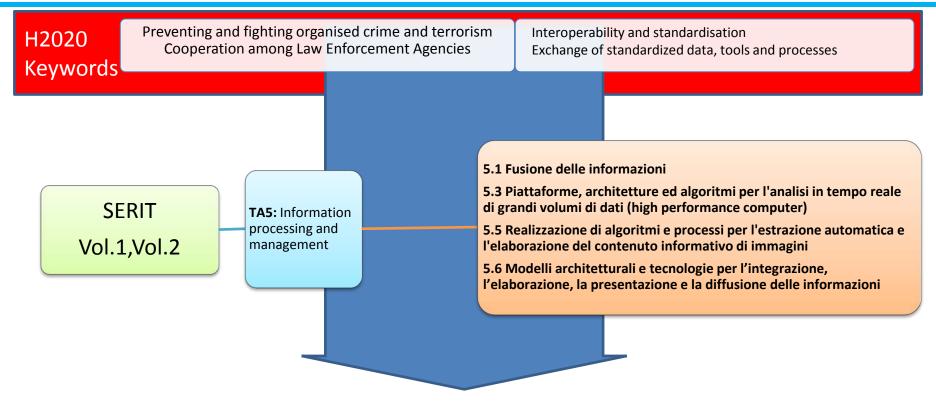
Area 1

Technology

Area 2



Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs – Short term projects



- European information platform for fighters against organised crime and terrorism- DEMO:
 - \checkmark Develop tools and toolkits to support interoperability to exchange data and share applications among the different Law Enforcement agencies.
- Definition of a common ontology for the law-enforcement domain— IP:
 - ✓ Allow Law Enforcement Agencies to easily work across borders through the definition and adoption of a common ontology, the exchanges of standardized data, the exploitation of common or compatible tools and processes needed to achieve their missions



Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs - Technologies

					TI	RL 1	3	TRL 4-6			TRL 7-9		
Technologies	5.1	5.3	5.5	5.6	1	2	3	4	5	6	7	8	9
Architetture Software													
Biometrics													
Cloud Computing								ĺ	İ				
Data Fusion													
Data collection, classification & analysis													
Modelling and Simulation													
Tecnologia per l'elaborazione numerica di immagini e													
pattern - Re-identificazione													
Protezione della diffusione e memorizzazione													
dell'informazione (network and storage protection)													

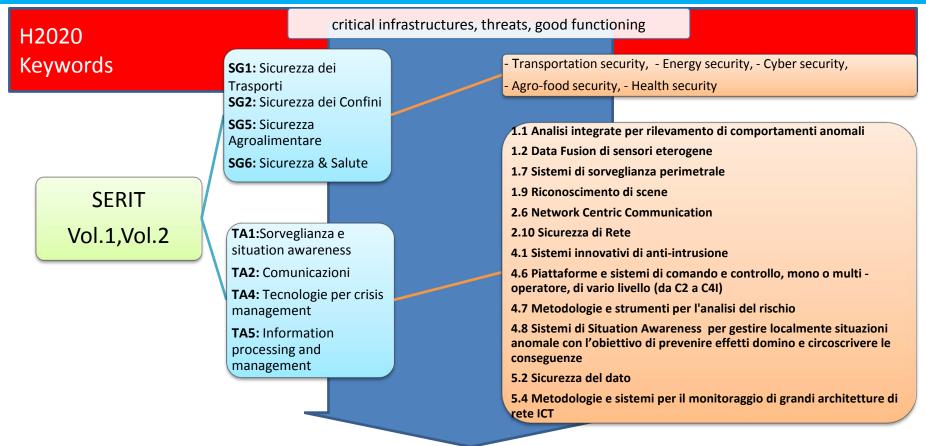


Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs - Future Calls

- 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.
- 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
- 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.



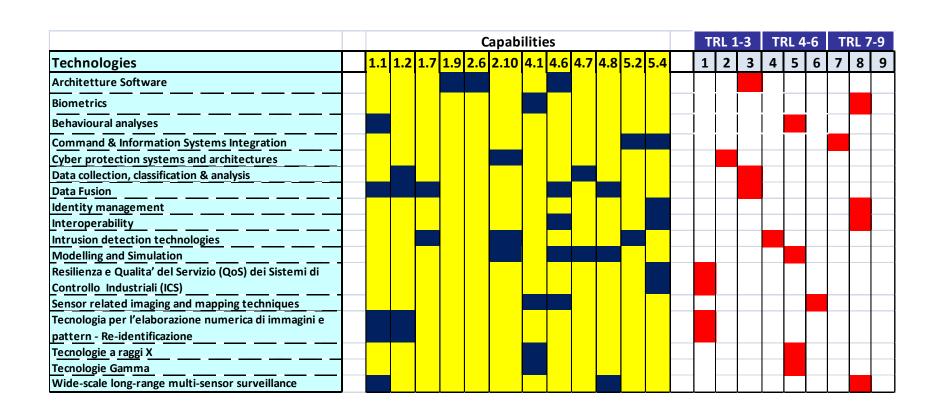
Protect and improve the resilience of critical infrastructures, supply chains and transport modes – Short term projects



- Integrated risk modeling of "system of systems IP/DEMO
 - Understand the cyber-physical synergy and cascading effects.
- Resilience of complex cyber physical systems *IP/DEMO*
 - Synthesize information coming from different sensors, units, equipment and people, acting in the physical domain and in the cyber domain.



Protect and improve the resilience of critical infrastructures, supply chains and transport modes – Technologies





Protect and improve the resilience of critical infrastructures, supply chains and transport modes – Future Calls

- 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 a Multi-Modal Transport Service Platform to improve the cooperation and interoperability of different transport modes: 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
- Improve the security of health infrastructures: 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:** 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.



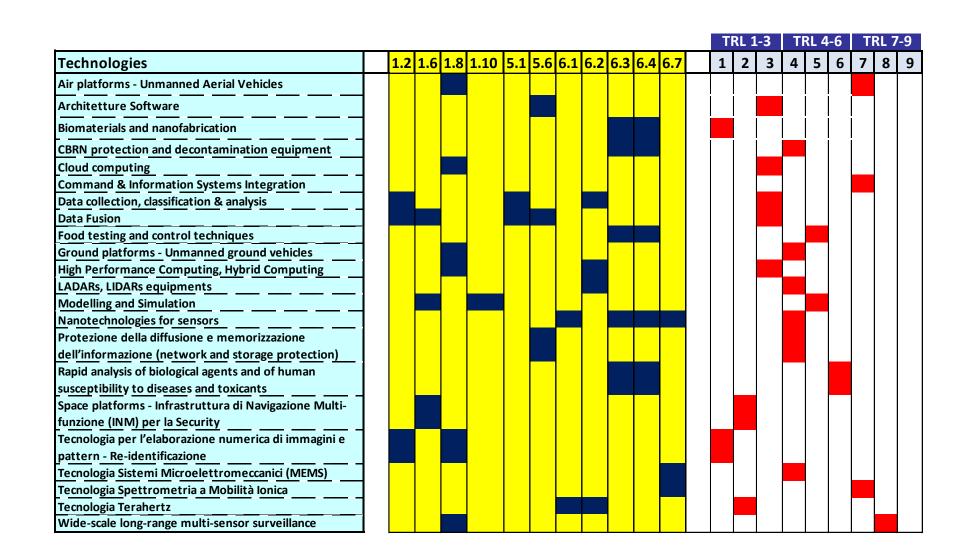
Strengthen security through border management – Short term projects

rapid identification, marine and coastal border security, Logistic & Supply Chain Security: H2020 surveillance, border management, enhance systems, equipments, tools, processes, and methods for cooperation, EUROSUR, CISE Keywords rapid identification, food security - Sicurezza e dei confini, cooperazione, sorveglianza integrata SG3: Sicurezza dei - Sicurezza agroalimentare, dogane, porti, varchi transfrontalieri, Confini sicurezza nei sistemi di logistica avanzata degli alimenti SG5: Sicurezza Agroalimentare 1.2 Data Fusion di sensori eterogenei **SERIT** 1.6 Sistemi di localizzazione, navigazione e guida assistita 1.8 Piattaforme di sorveglianza marittima, terrestre e aerea TA1:Sorveglianza Vol.1,Vol.2 1.10 Sensori per la sorveglianza marittima e costiera, basati a terra o imbarcati e situation 5.1 Fusione delle informazioni awareness 5.6 Modelli architetturali e tecnologie per l'integrazione, l'elaborazione, la **TA5:** Information presentazione e la diffusione delle informazioni processing and 6.1 Rivelazione di composti in tracce management 6.2 Stand-off detection di minacce chimiche e biologiche **TA6:**CBRNE 6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard 6.4 Tecnologie microfluidiche per la detezione di biohazard 6.7 Nanotecnolgie per rivelazione di esplosivi, droghe

- Secure and Trusted Public Regulated Regional Traffic Monitoring Service IP
 - increase the trustworthiness and to guarantee the reliability and integrity of the ship reported data
- Real-time screening systems for contaminants in bulk food CP/IP
 - identify and explore technologies and processes to enable efficient and expeditious screening of containers, cargo, passengers and baggage



Strengthen security through border management – **Technologies**



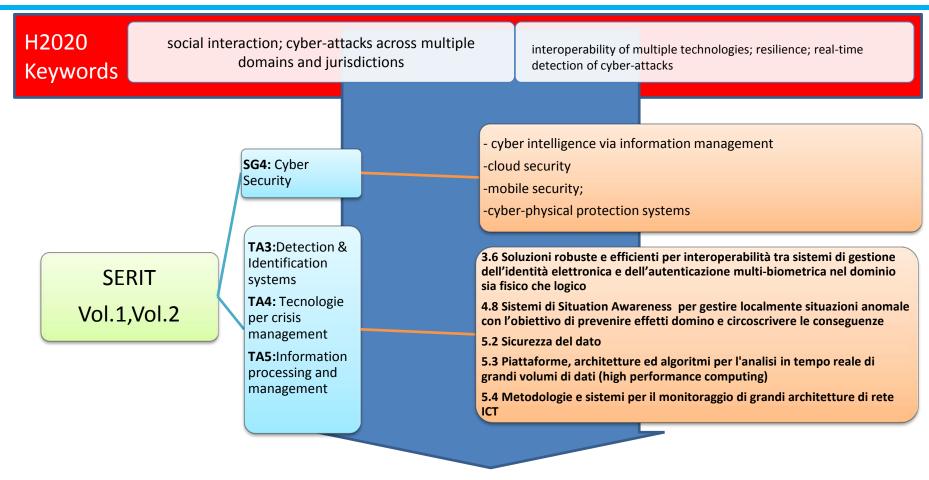


Strengthen security through border management – Future Calls

- 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.
- 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. Reinforcement of **cooperation among involved operators** and improving of the **situational awareness** by mean of a set of advanced technologies and components such as **sensors** (low cost radars, hyperspectral, active optronics, dust of sensors ...), **platforms** (airships, UAV, UGV ...), **data fusion and big data management platforms**.
- Initiatives to make the **Airport infrastructure** a **comprehensive and fully integrated system** for border checks through a wide security monitoring network with **dynamic adaptation** of security assets to the scenario changing, preserving the levels of performance and services for the public.
- Regarding the maritime surveillance one or more lighthouse projects shall be launched to support
 the achievement of a maritime awareness tailored for specific civilian goals, developing suitable
 info-space environment as generated by putting together new surveillance
 capabilities/technologies and data sharing policies (e.g. CISE). 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.
- Use of unmanned platforms (such as Medium Altitude Long Endurance, MALE, and Unmanned Air-Vehicle System, UAS) for maritime and land surveillance, acting as the aerial node of a global network that integrates heterogeneous sensing technologies and will automatically generate alerts about suspicious events.



Improve Cyber Security – Short term projects



- Protection mechanisms against social engineering attacks CP/IP
 - Cyber-security and Resilience of Heterogeneous, Inter-Operating, Critical ICT Infrastructures CP/IP



Improve Cyber Security – Technologies

Canabilities							TRL 1-3			TRL 4-6			TRL 7-9		
	3.6						1	2	3	4	5	6	7	8	9
			'												
							ĺ			ĺ					
		3.6	_			Capabilities 3.6 4.8 5.2 5.3 5.4							·		

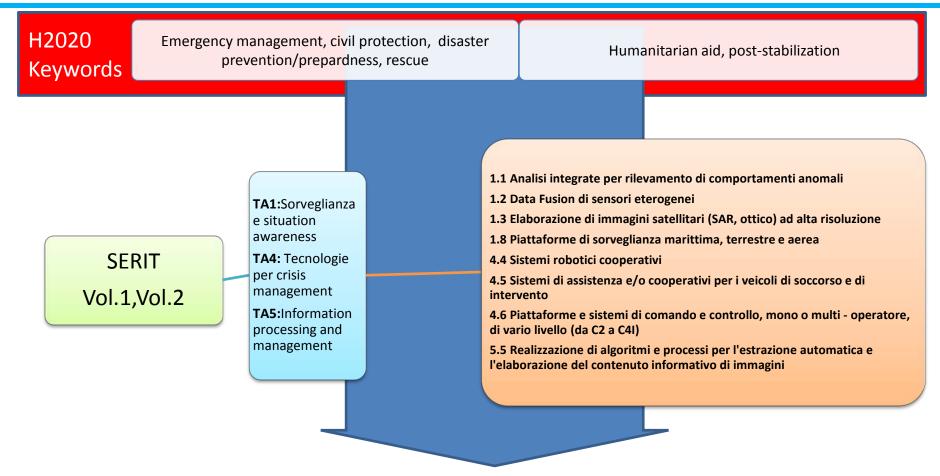


Improve Cyber Security – Future Calls

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



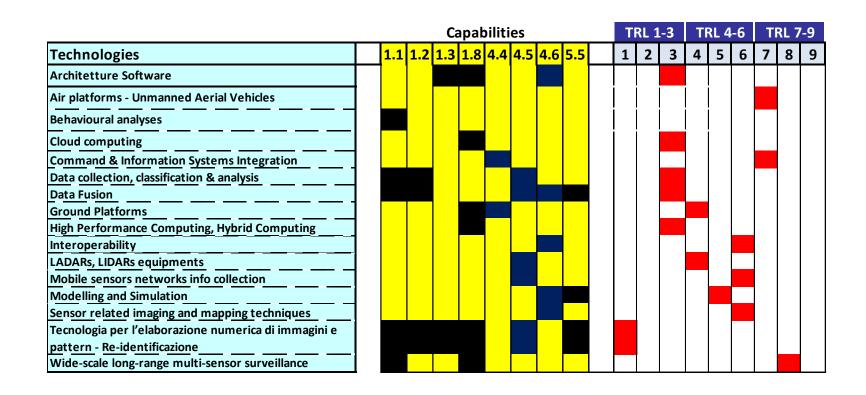
Increase Europe's resilience to crises and disasters & Support the Union's external security policies including through conflict prevention and peace-building— Short term projects



- Unmanned ground platform in disaster governance— CP
- Adaptative Wide Area Surveillance and Monitoring systems IP
 - 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.



Increase Europe's resilience to crises and disasters & Support the Union's external security policies including through conflict prevention and peace-building— Technologies





Research prioirties on external security policies - Short term Projects

	ESS	ESS Report	Council Declaration
	2003	2008	2008
Terrorism	✓	✓	✓
Organised crime	✓	✓	✓
Weapons of Mass Destruction (WMDs)	✓	✓	✓
Cyber	✓	✓	✓
Pandemics	✓	✓	
Piracy	✓	✓	✓
Regional Conflicts	✓	✓	
Energy security and dependence	✓	✓	✓
Poverty	✓	✓	
State failure		✓	
Cyber security			✓
Climate change		✓	

•European Security Strategy (ESS), A secure Europe in a better world (2003)

• Council declaration of 8 December 2008 on international security (2008).

Ontology: It should be devoted to the indepth analysis of strategic statements (starting from the wording of strategic and policy / normative documents) and of the respective **implementation** documents in order to define in details the **real contents** of each domain. It should be verified whether certain areas / sub areas named only in the framework of external security (for example poverty) have, in reality, indirect effect on internal security (for instance by causing the conditions for large-scale illegal immigration towards Europe)

Report on the implementation of the European Security Strategy, Providing security in a changing world (2008)

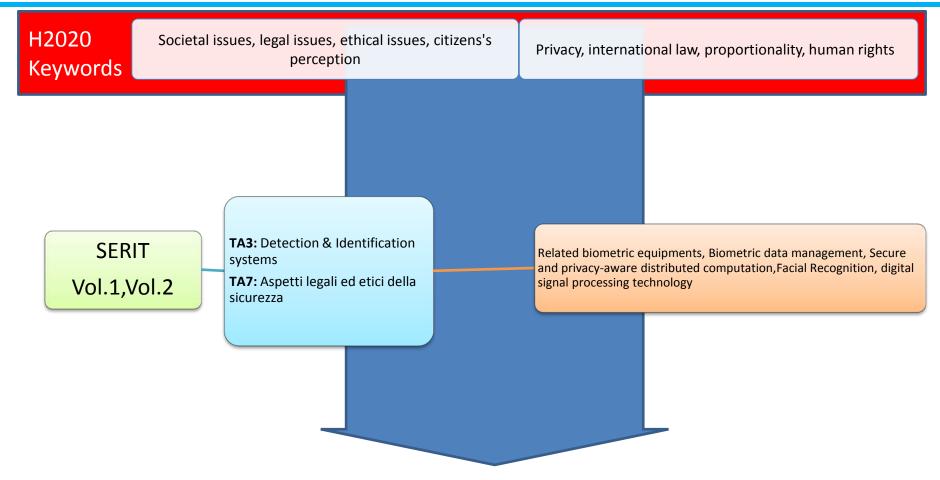


Increase Europe's resilience to crises and disasters & Support the Union's external security policies including through conflict prevention and peace-building— Future Calls

- Detection of CBRNE threats (prevention preparedness), focus on dual-use systems;
- Extra EU crisis management for humanitarian and natural hazard emergencies; focus on prevention/preparedness, mitigation and post-stabilization;
- EU crisis management, focus on technological advances, interoperability, ICT architectures and opportunity information based on social habits (ICT technolog
- Review on formal competences and functioning (decision-making) of EU and national
 institutions and agencies. Review also conducted at technical-operational level (EU /national
 level), regarding also the mechanisms, the capacities and above all the available procedures
 (especially when it comes to improve interoperability). Guidelines to improve coherence and
 coordination among the different actors, having in mind that different situations require
 different solutions ies available to citizens)
- Technologies mapping in order to individuate shortfalls and direct investments to avoid duplication and provided the added value of a double application. This mapping should not be separated from a consideration of dual use domains (technology itself is not military or civil: application makes the differences!) in the framework of synergies pursued by the European Framework Cooperation for Security and Defence among EC / EDA / ESA and it could contribute to the process of definition of the 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.



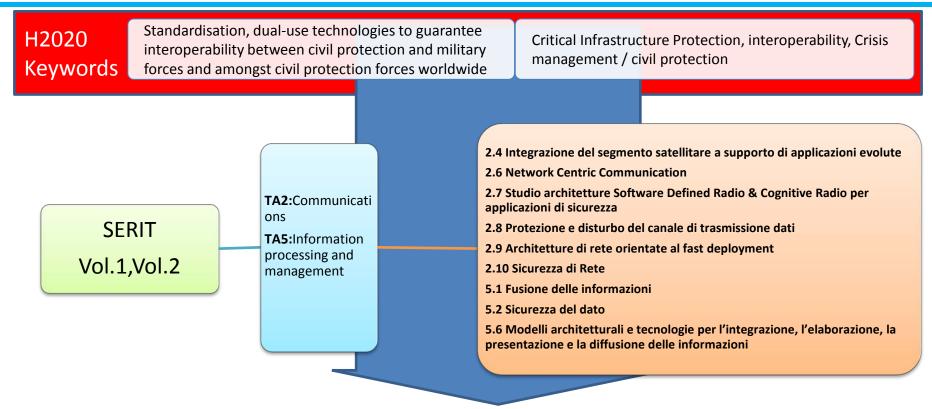
Enhance the societal dimension of security and ensure privacy and freedom in the Internet—Short term projects



- Inclusive Security DEMO
 - Inclusiveness-by-design applied on Automated Border Crossing
- Legal and Ethical Aspects of Biometric Data International Sharing **DEMO**
 - Homogenization of systems and procedures for biometric data sharing



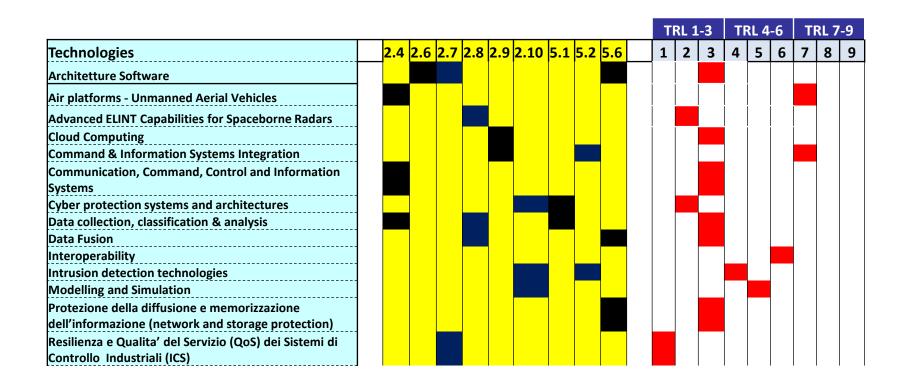
Enhance standardisation and interoperability of systems, including for emergency purposes—Short term projects



- Radio communication for first responders and Law Enforcement Agencies CP/IP
 - New radio communication system for first responders based on several interoperable components built around a security enhanced LTE standard and satellite systems;
- Urban security and citizen safety CP/IP
 - urban security and citizen safety may be enhanced and enforced through multiple systems interoperability



Enhance standardisation and interoperability of systems, including for emergency purposes— Technologies





Enhance standardisation and interoperability of systems,

including for emergency purposes Future Calls

- Exploit IP protocols interoperability for implementing futureproof situation-awareness' information sharing, beyond radio integration.
- Exploit current and near-future technologies for legacy systems interoperability.
- Leverage crowd-sourced data for security and safety.
- Leverage geo-referencing and multimedia for security and safety purposes.
- Standardize ICT for health-care management.
- Standardize and enforce procedures.



Foster European Smart cities and Communities

- «Smart Cities and Communities» is a multidisciplinary theme, involving not only Energy and ICT, but also Mobility, Logistics and, specifically, Security.
- In fact Secure Societies require safe & secure cities and therefore Security needs to be a core part of any Smart City: there can be no smartness without safety and security
- A Smart City is by definition a Network of Networks, i.e. a cooperative environment in which many infrastructures (smart and not-so-smart) provide services to citizens
- These infrastructures are always interrelated (all, at a minimum, dependent on energy and TLC) and are therefore prone to the risk of a waterfall effect in case of failures
- In Smart Cities, Security must thus be considered along two dimensions:
 - 1. Protection and resilience of the Network of Networks on which Smart Cities are based and on which they depend
 - 2. Urban Security, both traditional and innovative (e.g. participated security)



Foster European Smart cities and Communities Short term Projects

- Development and/or integration of Earth Observation and Navigation technologies with TLC and IT in order to create a Smart City situational awareness and support current management of infrastructures
- Advanced analytics, with a specific focus on Big Data analysis, both for the holistic management of the risk cycle (from prevention to crisis management and recovery) and for the planning of Smart Cities' resilience
- Innovative channels and applications for involving citizens in distributed sensing and information dissemination both in ordinary conditions and during crises.



Cultural heritage

To ensure **cultural heritage and built environment** has a tremendous social and cultural impact (earthquakes in Abruzzo (2009) and in Emilia Romagna (2012) and Pompei collapses,...)

This need has an ambivalent character:

- the Safety, with reference to the risk associated with environmental changes and natural disasters,
- the Security, with respect to damages due to human acts and, in particular, to criminal and terrorist events.

The fruition of cultural heritage also asks for **Safety** conditions of the **users** as, for example, visitors of a museum or an archaeological site.

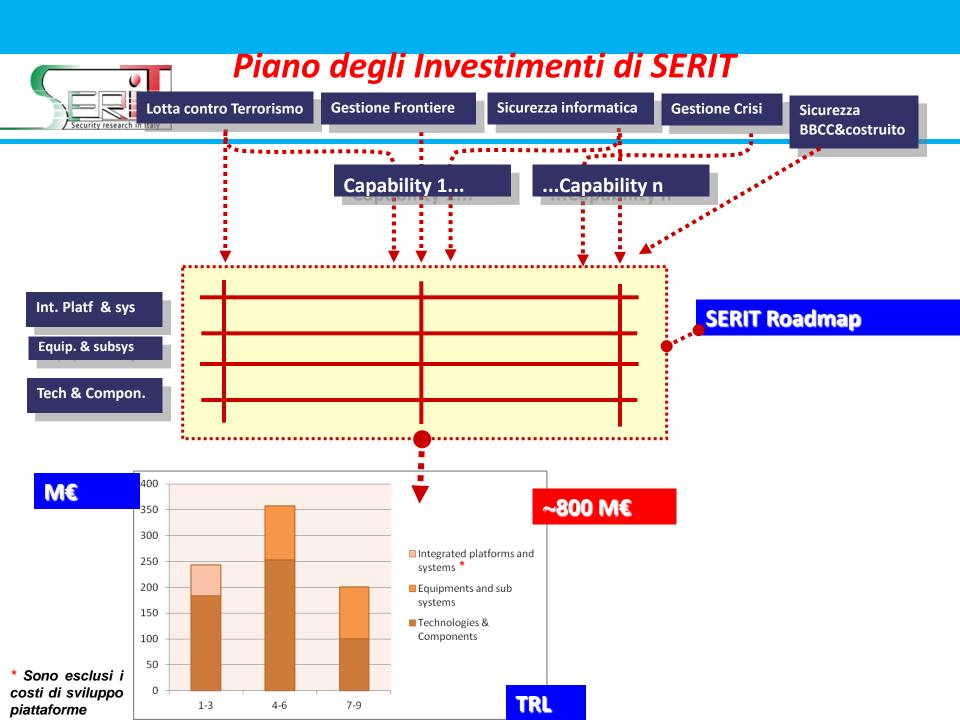


Cultural heritage - Short term projects

- Development and validation of an integrated approach to CH monitoring and quick damage assessment against natural hazards at European Level (Integration Project)
- Development and implementation of an integrated system for the Safety and Security of the fruition and the related emergency situations
- Development of ICT/sensing tools for movable heritage Safety and Security



Conclusions





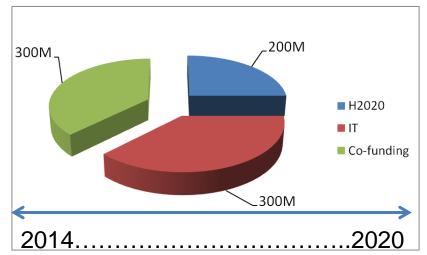
Raccomandazioni

1. Allineamento Strategico: E' necessario definire un Programma Nazionale sulla Sicurezza, che sia guidato da esigenze di tipo top-down (Vision), ma che nel contempo integri dei progetti "bottom-up", che rispondono ad esigenze di mercato. L'innovazione in ambito Security è complessa ed è necessario sviluppare "bricks" tecnologici (capabilities), che possano essere indirizzati e validati dagli utenti finali.

Riteniamo inoltre fondamentale l'adozione di un **Programma Nazionale della Ricerca**, che sia coerente con il quadro di riferimento europeo di Horizon 2020 - Security, con un budget certo ed in linea con le ambizioni tecnologiche del Paese, bilanciato nelle componenti di ricerca accademica ed industriale.

A tal fine, SERIT auspica l'istituzione di un tavolo di discussione tra il Ministero e la Piattaforma, in modo da approfondire le tematiche di

ricerca





Raccomandazioni

2. Coordinamento Nazionale

✓Un coordinamento delle strategie della ricerca, tra MIUR, Ministero della Difesa e Ministero dello Sviluppo Economico è auspicabile. Sinergie per quanto possibile tra R&T militare e civile, in particolare in ambito sicurezza sono possibili. Inoltre, il perimetro include non solo sicurezza civile e militare, ma anche lo spazio (dove ASI potrebbe essere un esempio della dualità), sul modello dell'EFC.

✓Un coordinamento nella definizione delle necessità operative, attraverso un coinvolgimento significativo di utenti finali ed utilizzatori pubblici e privati, è di sicuro stimolo per la creazione di un mercato della sicurezza.

✓Un coordinamento tra gli sviluppatori di soluzioni di sicurezza, che si sta provando a realizzare tramite la Piattaforma Serit, deve servire a far emergere le eccellenze nazionale e a fare sempre di più "sistema paese"