IMG-S – EARTO Joint Position Paper on Resilience in Security Research

1. Executive Summary

This document is published by the Integrated Mission Group for Security (IMG-S) and the Security Research Group (SRG) of the European Association of Research and Technology Organisations (EARTO) as a joint position paper on Resilience in Security Research, being in line with the objectives of the H2020 Secure Society Work Programme and other relevant actions and initiatives in the sector, taking into account the need to link security research to capacity planning and capability insertion for resilience.

The paper should be considered as an **introductory and non-exhaustive document in the topic** of resilience, providing basic concepts such as **framing challenges, setting priorities**, **providing recommendations**, etc. The aim is to help the readers to **identify areas and/or sectors that deserve particular attention** and to initiate a thorough investigation of the Resilience potential, within the overarching topic of Disaster and Risk management in the context of Security Research & Innovation initiatives. To this end, following this first document that provides initial fundamental concepts and guidelines on Resilience, a set of position papers addressing specific aspects (e.g., Resilience of Critical Infrastructure, Resilience of Soft Targets, Resilience of the Supply Chain, Resilience of Communities, etc.) will follow. Moreover, this document is intended to pave the ground for discussions among stakeholders involved in resilience-relevant topics and to provide a mechanism for engaging them in future and more detailed technical contributions. In this context, the **overarching aims** of this paper are:

- **To establish the resilience paradigm as an efficient aspect in the security culture** and adapt the design of socio-technical systems in terms of protecting critical services and strengthen society's adaptation to new and emerging threats and hazards;
- To address the topic of Resilience in the context of the **European Security Research**, with a focus on how to potentially deliver **harmonized policies and technologies, which can promote** the **take-up** of **best-practices** and **operational resilience** procedures, aiming to cope with current and **emerging risks;**
- **To define a common language** that will facilitate and support common understanding, perception, and modelling of Resilience;
- **To arrange and organize actual knowledge to develop and encourage** a **consensual view** on the concept of Resilience and to investigate Resilience strategies and approaches, strengthening cooperation and collaboration among stakeholders and Communities, aiming to tackle emerging societal challenges on security in a common, agreed and harmonized way.

To make this happen **a paradigm shift** is required, which will define the context and the rationale for reconsidering the actual security thought-pattern concerning disaster, risk and crisis management. In this frame, it is of upmost importance that all potential sources and causes of societal, technical, economic and environmental disruptions (e.g., physical, cyber and hybrid threats, CBRNE, natural and man-made disasters including terrorism, etc.) will be considered and revised[1].

[1] http://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

2. Background Information

Among others, the following background information have been considered when preparing this position paper:

- The **Global Strategy for the European Union's Foreign and Security Policy**[2], presented by Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy in 2016;
- the overall policy goals of the **Europe 2020 Strategy**[3], the European Union (EU) growth strategy for the next ten years supporting the European ambition to become a smart, sustainable and inclusive economy with associated societal and economic benefits in terms of safety, security, quality of life, well-being, productivity, employment and social peace;
- the **EU Security Industrial Policy**[4], promoting innovation and competitiveness in the security industry sector, with one of the highest growth and employment potential in Europe;
- the **European Security Strategy** – A secure Europe in a Better World (ESS)[5], adopted by the European Commission in 2013, that establishes for the first time principles and sets clear objectives for advancing the EU's security interests based on EU core values;
- the principles and guidelines set out in the **EU Internal Security Strategy**[6] (ISS) for dealing with security threats, namely organised crime and cross border illegal activities, through an integrated strategy;
- the **European Defence Action Plan**[7], which proposes a European Defence Fund and other actions to support member states' more efficient spending in joint defence capabilities, strengthen European citizens' security and foster a competitive and innovative industrial base;
- the **Community of Users (CoU)**[8] on Safe, Secure and Resilient Societies initiative of DG-HOME.

3. The Challenge

Within the European Research agenda, the thematic area of security is a well-established field of research since the 7th Framework Programme, which was initiated in 2007. Since then, a myriad of research projects have focused on investigating topics and developing solutions to prepare for risks, to prevent disasters, to manage a crisis' response efforts and to recover from them as quickly as possible. More recently, specifically with the introduction of Horizon2020, the security research agenda has evidently been broadened towards a more holistic disaster management approach that aims at linking the various perspectives and actions before, during and after an adverse event. **The term this development is prominently linked to is related to the concept of resilience**. Today, reference to resilience can be found in almost all research programs while the concept attracts the interest of social scientists, technology developers, risk managers, engineers, operational and academic researchers, etc. However, a **clear challenge** that is often observed **is that the term "resilience" and the perception of it isn't defined in a clear and transparent way**. Some argue that resilience is part of

[2] https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web.pdf
[3] https://ec.europa.eu/info/strategy/european-semester/framework/europe-2020-strategy_en
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF
[5] https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF
[7] http://ec.europa.eu/DocsRoom/documents/20372
[8] https://www.securityresearch-cou.eu/

disaster risk management, whereas others link most of the resilience perspectives to crisis management activities, hence to post-disaster situations, etc. Additional confusion results from the fact that in many cases, resilience is seen as a built-in feature of systems and societies that can be planted to engineered infrastructures by retrofitting technology or by design. Others rather refer to it as a strategic concept or a masterplan element that can be applied in order to reach comprehensive security for socio-technical systems.

In this fragmented, highly differentiated and dynamic context, **this paper can be seen**, in a first step, **as a starting effort and contribution towards a common understanding of the term and the concept of Resilience** and, in a second step, as a document to set the ground for identifying research needs and priorities to integrate the resilience culture within the European Security Research Programs.

4. The concept of Resilience within the entire cycle of disaster management

Resilience has emerged in the last decade as a concept for better understanding the performance of infrastructures, especially their behaviour during and after the occurrence of disturbances, e.g. natural hazards or technical failures. Recently, resilience has grown as a proactive approach to enhance the ability of infrastructures to prevent damage before disturbance events, mitigate losses during the events and improve the recovery capability after the events, beyond the concept of pure prevention and hardening (Woods, 2015)[9]. The concept of resilience is still evolving and has been developing in various fields (Hosseini, Barker, & Ramirez-Marquez, 2016)[10]. Like any new area or field, the interest gained for resilient systems has created a vast array of relative definitions, processes, tools and metrics that have clouded the concept of resilience. A first definition described resilience as "a measure of the persistence of systems and of their ability to absorb change and disturbance, and still maintain the same relationships between populations or state variables" (Holling, 1973)[11]. Several domain-specific resilience definitions have been proposed thereafter (among the others: Ouyang, Dueñas-Osorio, & Min, 2012[12]; Adger, 2000[13]). The resilience and policy committees of the National Academy of Sciences (NAS) defined resilience as the ability of a system "to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events" (Cutter et al.[14], 2012, Cutter et al., 2013[15]). A modern and simple definition of resilience is provided by Nan, Sansavini, & Kröger (2016)[16], stating that is "the ability of a system to resist the effects of disruptive forces and to reduce performance deviations". Ultimately resilience is not just about bouncing back from adversity but is more broadly concerned with adaptive capacity and how we better understand and address uncertainty (Gibson and Tarrant, 2010)[17].

From an **operational viewpoint**, *resilience can be defined as the ability of the system to withstand an unexpected harmful change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability)*. Enhancing any of these features will enhance system resilience. It is important to

[9] https://www.researchgate.net/publication/276139783_Four_concepts_for_resilience_and_the_implications_for_the_future_of_resilience_engineering
[10] https://www.irgc.org/wp-content/uploads/2016/04/Barker-Ramirez-Marquez-Infrastructure-Network-Resilience.pdf
[11] http://www.zoology.ubc.ca/bdg/pdfs_bdg/2013/Holling%201973.pdf
[12] https://www.researchgate.net/publication/261615193_A_three-stage_resilience_analysis_framework_for_urban_infrastructure_systems
[13] http://journals.sagepub.com/doi/abs/10.1191/030913200701540465
[14] http://www.tandfonline.com/doi/abs/10.1080/00139157.2013.768076
[15] http://www.environmentmagazine.org/Archives/Back%20Issues/2013/March-April%202013/index.html
[16] https://www.irgc.org/wp-content/uploads/2016/04/Sansavini-Engineering-Resilience-in-Critical-Infrastructures.pdf
[17] https://ajem.infoservices.com.au/downloads/AJEM-25-02

understand and quantify these abilities hat contribute to the characterization of system resilience (Fiksel, 2003)[18]. In addition and to be more specific, the following definitions of resilience seems to take the operational perspective into account: *"Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist" (Holling, 1973)*; *"Resilience is the ability of a system to resist the effects of disruptive forces and to reduce performance deviations" (Nan, Sansavini, & Kröger, 2016).* This leads to the consideration that the various aspects or phases of resilience can be depicted as a cyclical model, as presented below.

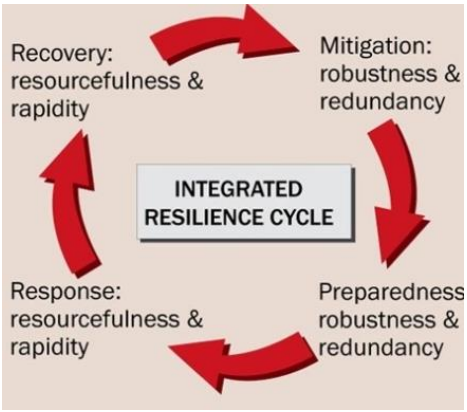

Figure 1: The Resilience Cycle (Charlie Edwards[19])

Anyway, before making any further assumption or attempting to quantify and model relative procedures to "measure" the resilience it is of primarily importance to create and reach a consensus on the concept of resilience in a very wide way. To this end, one can come up with the following widely-accepted definitions:

- Resilience is the capability of a system, organization (infrastructure, factory, business, city, region, etc.) when facing catastrophic incidents, emergency events or crises episodes to successfully overcome them, minimise their negative effects and recover to "normal" operational levels as soon as possible (i.e., the everyday way of living and performance of the community gets disturbed in lesser extent and during less time);
- Resilience is the capability of the infrastructure itself (including the managing/operating people at all levels) to maintain its operability under all circumstances and to minimize potential damages (i.e., assure business continuity).

In addition, how resilience is linked with the Disaster Risk Management approach is a further aspect to be considered and worth of clarification. Indeed, conceptually, risk analysis quantifies the probability that the system will reach the lowest point of the critical functionality profile. Risk management helps the system prepare and plan for adverse events, whereas resilience management goes further by integrating the temporal capacity of a system to absorb and recover from adverse events, and adapt accordingly[20]. Thus, resilience, on the basis of the definitions aforementioned, is not a substitute for principled system design or risk management[21] but is rather a complementary attribute that uses strategies of adaptation and mitigation to improve traditional risk management. Indeed, given a certain event, the customization of Resilience within the Disaster Risk Management Cycle is depicted below,

[18] http://www.eco-nomics.com/images/Designing_Resilient_Sustainable_Systems.pdf
[19] https://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf
[20] https://www.researchgate.net/publication/263808670_Changing_the_resilience_paradigm
[21] https://www.researchgate.net/publication/230831578_Integrating_Risk_and_Resilience_Approaches_to_Catastrophe_Management_in_Engineering_Systems

where the proper elements of resilience are integrated into or added to the phases (prevention, preparedness, response and recovery) of the Disaster Risk Management Cycle.

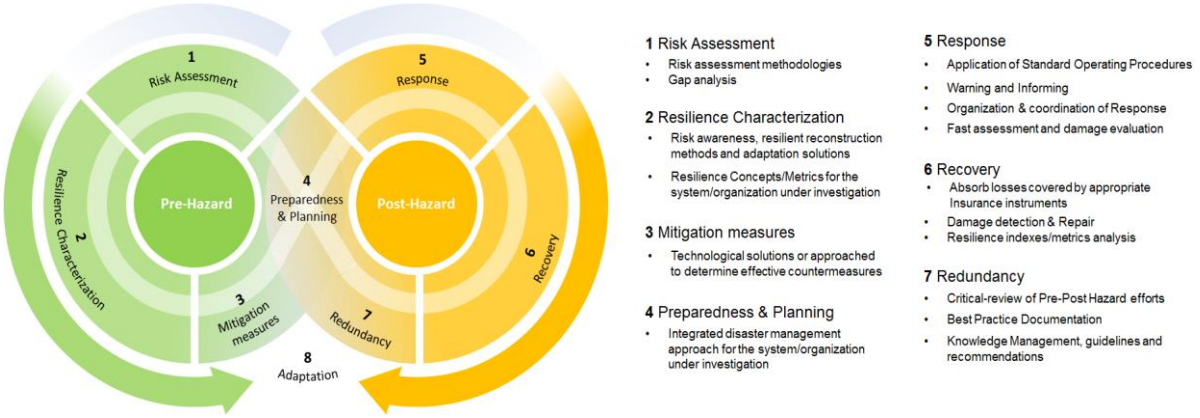

Figure 2: Holistic Approach in Disaster Management – Resilience as "linking" concept

In this sense, looking at the previous picture, Resilience can be seen as the link or capability to link pre-hazards and post-hazards activities/phases moving from 1) risk assessment to 2) resilience characterisation, to 3) mapping and screening of countermeasures and mitigation actions, to 4) preparedness and planning, enabling a more effective 5) response, leading to a 6) an efficient and timely recovery, that takes into accounts 7) redundancy actions up to adaptation 8), being represented by the outer arrows.

5. Resilience perception and strategies

Given the definition of Resilience provided above and the relation identified between the Resilience cycle and the lifecycle of disaster management, it can be said that resilience can be perceived as focusing on the fluctuation of the system performance which is harassed by an unexpected disturbance (also called resilience curve) (See below).

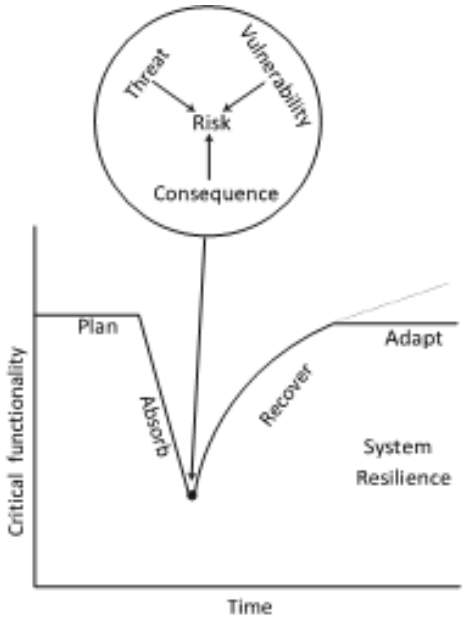

Figure 3: Risk and resilience management relationship (Linkov et al, 2014)

Over there, the transient area of performance defines the system response and the respective level of resilience. The smaller the area, the better is the resilience of the system.

The four schematic representations of changes in critical functionality over time, shown in the figure below, depict the interplay of risk and resilience in a system's performance during an adverse event. The size of the initial perturbation reflects the total risk to the system while the shape of the recovery curve is controlled by the system's resilience. The area under the curve is indicative of the overall system functionality. Systems that face high risks with high resilience perform better than those facing similar risks but with low resilience. Systems with low risk and low resilience may perform the same as, or possibly worse than, systems with high risk and high resilience.

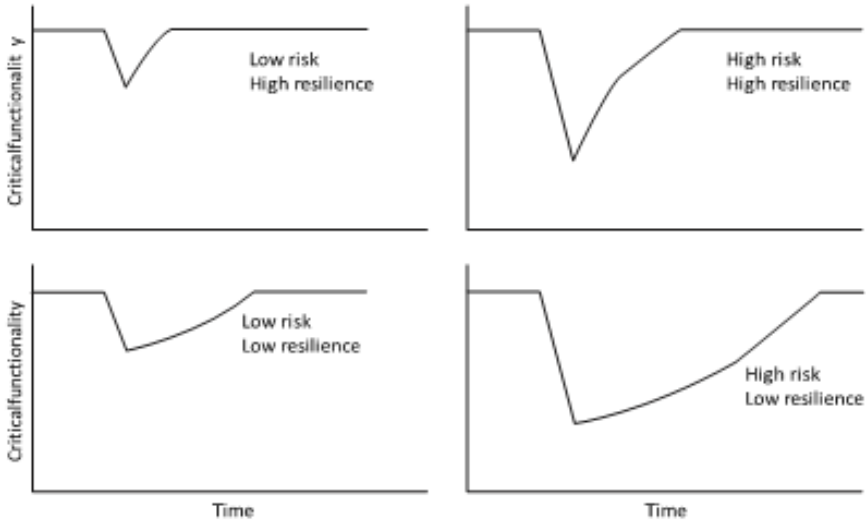

Figure 4: Interplay of risk and resilience levels (Linkov et al, 2014)

When the concept and context of resilient is perceived, a number of strategies have to be considered in order to strengthen the system's response and enhance its resilience. There are several strategies and improvements that might be considered for this purpose. In particular, in what regards systems, infrastructures, etc. such resilience strategies can be:

- **Planning ahead during the design phase**, aiming to ensure robust or stochastic optimization against uncertain future scenarios.
- **Self-healing, adaptation and control, i.e. graceful degradation**: the system cannot be design with respect to every uncertain scenario, therefore a resilient design should consider how to prevent the disturbance from spreading across the whole system, creating systemic contagion and system-wide collapse. In this respect, cascading failures analysis, and engineering network systems to be robust against outbreak of outages and propagations of cascading failures across their elements are key strategies. Control engineering can provide strategies to create robust feedback loops capable of enabling infrastructures to absorb shocks and avoid instabilities. Designing structures and topologies which prevent failure propagation, and devising flexible topologies by switching elements which allow graceful degradation of system performances after disruptions are also valuable resilience-enhancing techniques.
- **Recovering quickly from the minimum performance level**: robust or stochastic optimization of the recovery and restoration process in the face of uncertainties in the repair process or in the disruption scenarios.
- **Effective system restoration**: through the combination of restoration strategies, e.g. repairing the failed elements and building new elements, the infrastructure can achieve a higher performance with respect to the pre-disruption conditions.

- **Exploiting interdependencies among infrastructures**: interdependencies and couplings in systems operations can foster the propagations of failure across coupled system; on the other hands, interdependencies might also provide additional flexibility in disrupted conditions and additional resources that can facilitate achieving stable conditions of the coupled system.[22]

6. Setting a common ground for understanding and prioritizing

It is well assessed that Resilience depends on many factors such as technological (i.e., platforms and tools for monitoring and surveillance), human (i.e., capability of intervention by first responders and exploitation of social networks and citizens as a source of information) and acceptance by end-users (willingness and awareness of the necessity to consider the added value provided by the state of art and novel technological and scientific products for the improvement of operative capabilities in infrastructure and urban areas management, during ordinary and extraordinary conditions). Presently, the approach to improving resilience is going to change deeply, not only for the revolutionary evolution of technologies (i.e., technologies directly related to resilience and driven by resilience needs), but also because the approaches to the full risk cycles and multi-hazards risks understanding is changing. Therefore, new perspectives are arising in resilience, despite the fact that the already operative services still underexploit these new capabilities, which have been recently developed. Despite the fact that is being an established feature of sustainable technological, ecological and sociological systems[23], planned resilience still requires metrics that are both adequate to measure individual system qualities and generalizable to inform resource allocation and operations. To date, the failure to understand resilience in the context of complex system has precluded the creation of an actionable metrics framework to inform resilience decisions[24].

On this basis, the following issues among others need to be preliminary drafted, being relevant in setting priorities towards a common improvement of **Resilience in Security Research:**

- **To enable** a **resilient-informed risk assessment to tackle new and emerging threats**. In this sense the existence of a comprehensive risk management framework across the whole life-cycle of the disaster management loop is mandatory, in combination with a multi-hazards approach.
- **To build** a **rigorous resilience framework to organize** a comprehensive list of different notions of **resilience;** to associate the elements of such list to different contexts, to define smart adaptable measures to be taken into account in each case, and to make sure that the Resilience, the Context and the Measures are well-defined, adaptive and provable. The framework need to be extensible through refinement and to allow the analysis and reasoning of various capabilities and functions of resilience.
- **To strengthen preparedness by building disaster scenarios** to train relevant personnel and the society in addressing complex situations. By simulating threats and interdependencies, operational people can be better trained. In this context, the role of the practitioners serving the civil/public/societal sector should be enhanced. Costs should be analysed in order to provide financial information for preparing to address disasters. Also the use of Data Intelligence here could play a significant role.

[22] https://www.irgc.org/wp-content/uploads/2016/04/Linkov-Trump-Fox-Lent-Resilience-Approaches-to-Risk-Analysis-and-Governance-1.pdf
[23] http://www.eco-nomics.com/images/Designing_Resilient_Sustainable_Systems.pdf
[24] https://www.irgc.org/wp-content/uploads/2016/04/Seager-et-al.-A-Multidimensional-Review-of-Resilience.pdf

- **To identify**, among those already proposed in literature, appropriate **Resilience Metrics** (including financial and organizational aspects) in order to **quantify** the resilience in realistic ways (through benchmark, scenarios, etc.). This requires the integration of multi-sectorial expertise from several different fields.
- **To exploit cross-fertilization** (with other sectors/technologies/policies/procedures) so to secure the **take-up of good practices in Resilience** (for instance dual use) and to ensure **reusability of Resilience metrics,** when looking at new and emerging risks and threats (and how they would impact on the metrics).
- **To elaborate** the **operationalization of the resilience concepts** in order to harmonize them with disaster risk reduction and crisis management planning and move from single asset protection to the development of self-sustained, resilient critical services changing the current "modus operandi", providing management tools that can support, foster, and encourage such transition. In this sense, the definition of a **framework for Resilient Management Guideline** (RMGs) on the basis of disaster management mechanism deserves particular attention.
- **To investigate Societal Resilience** (e.g. Resilience of Communities) vs. **Resilience of Infrastructures** up to **Resilience of socio-technical systems** (e.g. including those using Linked Data, Big Data). Misfit individuals are a threat by themselves and infrastructure resilience has no meaning for individuals that cannot afford the costs involved. Reduction of societal costs thanks to a mature and consolidated approach to resilience by the community is a major effect
- **To investigate advances on dual use regarding Disaster Resilience Applications** in order to improve sustainability and resilience of smart cities and crisis management capabilities by focusing on terrorist threats and exploiting cross-fertilization with other sectors/technologies/policies/procedures including military research. In this field, it is necessary to overcome the difficulties related e.g. to the different IPR policies for civil and defence fields.
- **To investigate** new approaches for the **exploitation of ubiquitous** (social) **networks**, as well as of "sensors no sensors" (e.g. smartphones), changing substantially the system of information transfer, since all people connected contemporarily receive and diffuse information within these networks.
- **To disseminate** among the communities of interests (from end-users to suppliers) resilience-informed **risk management approaches** and solutions building a common ground of understanding risks and selecting more effective and reliable countermeasures (considering e.g. costs, benefits, factors, mitigating legal, political, social, psychological, etc. constraints)

Actually only part of these topics, approached and capabilities is used in resilience improvement. The implementation and combination of these approaches and capabilities could be a step forward towards a real benefit when they are integrated in a holistic approach for resilience dealing with all the aspects related to the disaster management cycle.

7. Concluding remarks

Resilience is the ability of a system to withstand an unexpected harmful change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability).

In line with the aim of this document, the following conclusions can be drafted as a synthesis of priorities based on the information provided here above:

- **To promote the concept of resilience** within community's organization and strengthen the **sharing of information** and data to build **resilient socio-technical systems**;
- **To integrate the potential of resilience** within the Disaster Risk Management Cycle and security plans to maintain the **continuity of essential services** against actual and emerging threats and ensure **system's bounce-back**;
- **To advance** in the fundamental **understanding and practical application of resilience** towards the **development of resilience process quantification,** as well as **comparison of resilience approaches in multiple social, environmental and engineering contexts** in order to come up with generalizable principles.

On this basis, among the others, the following high-level capabilities can be identified as highly recommended in the context of Resilience in Security Research:

1. **Connection**: to establish, in line with policy goals, a common understanding of resilience capacity to address uncertainty shifting thus from robust to sustainable sociotechnical systems, built on resilient approaches.
2. **Communication**: to organize open-discussions among security stakeholders and spread the word on resilience capacity to address and counterbalance actual and emerging risks so that people can understand (raising awareness) and participate (end-users and citizens' involvement here is mandatory).
3. **Modeling and Quantification**: to figure out ways to model, assess and quantify resilience aspects, by means of proper and agreed methodologies.

Therefore, the way forward for relevant Security Research R&D can be shaped around the following recommendations:

- **Recommendation 1: Investigate policies and elaborate research frameworks that may contribute to strengthening the design and development of socio-technical solutions** enhancing resilience and systems sustainability. This can be achieved by raising awareness on resilience, supporting and strengthening discussion among decision and policy makers, on the basis of groups of interests and group of experts, supporting the work of the CoU on Disaster Risk Management which aims to provide a common understanding of the matter and a contribution to a consolidation of priorities (short term).
- **Recommendation 2: Be ready to tackle emerging risks, based on adaptative capacities developed within a relevant resilience framework,** by creating a common understanding on the new and incoming risks and assessing the benefit in making systems resilient towards them. Bringing together all stakeholders, end-users and suppliers, will set the way to plan for an EU framework for resilience and later on for market uptake of innovative solutions, based on such framework and, aiming to tackle such risks (short to medium term).
- **Recommendation 3: Elaborate ways to model and quantify Resilience**, encouraging to build the future generation of practices and afterwards standards in resilience metrics. This could be supported by working on methodological approach and paradigm shifts in cooperation with, among others, research initiatives in US, Japan, and Australia (medium to long term).

Note to the reader:

The "Joint Position Paper on Resilience in Security Research" has been elaborated by:

The Integrated Mission Group for Security (IMG-S)

IMG-S is a wide multi-disciplinary European professional network bringing together experts from Industry, SMEs, Research and Technology Organisations (RTOs), Academia and End-users. It has more than 200 members from more than one hundred organizations representing 24 European countries. IMG-S aims to support the European Commission and its Member States to build world-class European technological capabilities. By defining research priorities for the security domain at all levels, from fundamental research to mission capabilities and system integration, IMG-S contributes to ensure that short, mid- term and long-term security needs are addressed (http://imgs-eu.org).

European Association of Research and Technology Organisations (EARTO)

EARTO is the European Association of Research and Technology Organisations (RTOs) founded in 1999. It promotes RTOs and represents their interest in Europe. EARTO groups over 350 RTOs with a combined staff of 150.000, top-level R&D infrastructures and facilities and more than 1000 000 partners from public and private sector annually. The EARTO Security Research Group (SRG) is a working group comprised of 14 RTO's experts from member organisations, assisting EARTO in formulating security research policy positions and elaborating technically complex issues in topics of security (www.earto.eu).

IMG-S Contact:	*EARTO Contact:*
Clemente Fuggini, R&D&I Responsible in the areas of Transport & Infrastructures; Security & Space, D'Appolonia S.p.A.	*Georgios Eftychidis, Research Associate, Project Manager DRM & CIP Group, Center for Security Studies - KEMEA*
IMG-S TA4 Chair	*EARTO Working Group Security Research Member*
clemente.fuggini@dappolonia.it	*g.eftychidis@kemea-research.gr*
+39 3440179979	*+30 2107710805 (ext.339)*
www.imgs-eu.org	www.earto.eu

This paper has been edited by Clemente Fuggini, D'Appolonia (clemente.fuggini@dappolonia.it), IMGS-TA4 Chair, and by Georgios Eftychidis, KEMEA (g.eftychidis@kemea-research.gr), EARTO SRG Member.

Contributors and reviewers are listed below (in alphabetic order)

Juan Arraiza Irujo, jarraiza@vicomtech.org, Vicomtech, EARTO SRG Member

Andrzej Bialas, andrzej.bialas@ibemag.pl, Institute of Innovative Technologies EMAG, IMG-S TA4 Member

Matthaios Bimpas, mbibas@esd.ece.ntua.gr, NTUA, IMG-S TA4 Member

Miklos Biro, Miklos.Biro@scch.at, UAR/SCCH, EARTO SRG Member

Géraud Canet, geraud.canet@cea.fr, CEA, EARTO SRG Chair

Vincenzo Cuomo, vincenzo.cuomo@imaa.cnr.it, CNR IMAA, IMG-S TA4 Member

Luis Emaldi Atucha, luis.emaldi@tecnalia.com, TECNALIA, IMG-S TA4 and EARTO SRG Member

Jakub Główka, jglowka@piap.pl, PIAP, IMG-S TA4 Member

Clive Goodchild, clive.goodchild@baesystems.com, BAE Systems, IMG-S TA4 Co-Chair

Sorin Iacob, sorin.iacob@nl.thalesgroup.com, Thales, IMG-S TA4 Member

Anna-Mari Heikkilä, Anna-Mari.Heikkila@vtt.fi, VTT, EARTO SRG Member

Daniel Hiller, Daniel.Hiller@emi.fraunhofer.de, Fraunhofer EMI, IMG-S TA4 Member

Marcin Kowalski, marcin.kowalski@wat.edu.pl, WAT, IMG-S TA4 Member

Artur Krukowski, krukowa@intracom-telecom.com, Intracom Telecom, IMG-S TA4 Co-Chair

Isabelle Linde-Frech, isabelle.linde-frech@int.fraunhofer.de, Fraunhofer INT, EARTO SRG Member

Marco Manso, marco.manso@imgs-eu.org, Rinicom ltd., IMG-S Chair

Francesco Soldovieri, soldovieri.f@irea.cnr.it, CNR IREA, IMG-S TA4 Member