Recommendations on the Future of Security Research

Towards Framework Programme 9

Executive Summary

In response to the Tallinn Call for Action 2017 "Seize the opportunity now: research and innovation matter for the future of Europe"[1], and in relation to the upcoming proposal for the next Multi-Annual Financial Framework, the European Security Community represented by the European Organisation for Security (EOS), reaffirms its support for Framework Programme 9 (FP9), calls for extensive Research and Innovation (R&I) funding and, more specifically, Security Research in alignment with the Security Union priorities.

EOS recommends that:

1. **The budget for FP9 should be doubled, and in line with this so too the security funding chapter;**
2. **Targeted strategies are launched to close the research-to-market gap, including further leveraging instruments such as Pre-Commercial Procurement (PCP);**
3. **Security topics under FP9 should be more forward-looking and foster innovation potential through an end-to-end approach.**
4. **Participation of SME's to FP9 should be incentivised.**

Introduction

R&I activities within the EU are paramount for bringing together supply and demand to develop, deploy and enable procurement of innovative European solutions. Within the civil security sector, EU-funded research represents 50% of overall public funding in Europe[2]. European security industry, SMEs and RTOs are technology innovators. EOS and its members are a driving force for the security industry in Europe, and have been involved in a number of projects since FP7, shaping a more secure society that can respond to current and future security challenges. Investment from both the public and private sector has been key to achieving this, and has led to a unique level of public-private cooperation. ***EOS sees the trend towards an incentivised public-private cooperation continuing over the coming years, as it delivers significant advances through alignment on key European priorities***. A stronger, more established European-based security industry can better respond to an ever-changing security ecosystem, resulting in a more resilient society.

> *EOS supports a strong European Research Area, to overcome barriers and increase innovation to realise a resilient European*

European security R&I added value

European research cooperation has proven to be of clear 'added value' for European competitiveness. The coupling of research and innovation has enhanced resilience and created a more competitive and sustainable EU security

[1] TALLINN CALL FOR ACTION 2017 - Seize the opportunity now: research and innovation matter for the future of Europe - Statement of the Estonian Presidency of the Council of the EU

[2] Towards a Stronger Security Union: Current state of play and future trends in EU Security Research, November 2017

industry. Research funded at the EU level brings together different ecosystems dealing with the multi-facetted and combined threats in Europe (e.g. terrorism, hybrid threats, climate change, cybersecurity, migration and border control, critical infrastructure protection (CIP), and organized crime). European funded research stimulates high-quality, innovative and disruptive security research, also benefiting SMEs[3]. However, ***internal security is dependent on a strong and innovative European-based security market to increase autonomy and global competitiveness.***

European R&I and the next Multi-Annual Financial Framework

EOS supports the opinions of the European Parliament and the High-Level Group[4] for increasing financing for research and particularly security related research within the next MFF.

Today's innovation dynamics impact every aspect of European society. By leveraging public R&I funding, Europe creates jobs, enhances markets, increases competitiveness and secures its citizens and infrastructures. R&I funding facilitates innovation that covers requirements and current needs, it also ensures continuous collaboration between industry, RTO's, universities, start-ups and, of course, end-users. With the increasing complexity of security concerns however, research and innovation initiatives must be enhanced to overcome current bottlenecks. ***Security funding under FP9 needs to focus on creating synergies between new research activities and existing initiatives, developing mechanisms for more flexibility in defining future FP9 calls, as well as closing the research-to-market gap***. All these aspects can benefit EU society and strengthen the EU security market.

Policy/Budget recommendations

EOS members call for:

- more transparent and regular interaction with the EU policymakers to better address gaps between research and the market.
- the security research programme to remain separate from the defence research programme, but synergies between the two should be better explored.
- enhanced foresight methodologies and operational capabilities that are able to respond to a global scenario of evolving risks and changing threats.
- specific actions, such as the pooling of demand and development of standards, interoperability and certifications, that contribute to creating a holistic European security market supporting a strong and stable industrial base.
- the deployment of new models of governance that facilitate innovation, encourage a greater role for industry and SMEs, and give coherence and continuity to existing financial resources.
- More incentives for SME's to participate to FP9.

[3] Ibid

[4] Report of the independent High-Level Group on maximising the impact of the EU Research and Innovation Programmes

Recommendations on processes and implementation

Significant advancements should be made to:

- eliminate the research-to-market gap through new models of strategic innovation that integrate the offer and demand into a single roadmap, ensuring continued investment in research.
- support measures for the uptake of research results, which should be encouraged and accompanied accordingly. One way is a dedicated online "Observatory" platform where project results can be searched by key words or outcomes. This would also help avoid duplication in topics and be a very clear indication of what exists and what does not.
- provide a more effective evaluation process. The evaluation process should be as end-user focused as the implementation process. The solutions anticipated in proposals should be evaluated by at least one end-user in the field to better assess the need for a specific outcome. Furthermore, an end-user Board of Evaluators would be highly relevant for the future implementation of the project outcomes. Call-specific evaluations could also be considered.

Future calls for FP9

Future FP9 security-integrated calls should consider that the digital ecosystem will influence forthcoming security solutions. Future calls should concentrate upon:

- **Integrated Border Security:** Maritime surveillance and integrated communication systems are essential components.
- **Soft Target & Critical Infrastructure Protection:** Technologies that can support the protection of these unique and increasingly threatened environments are critical to EU resilience.
- **Security Screening and Detection Technologies:** Evolving current screening and detection technologies to respond to emerging threat substances, particularly CBRN, as well as encouraging scalable security solutions remains a priority.
- **Cyber Security:** Research should concentrate upon enhancing European digital autonomy and critical infrastructure resilience.

We also point to the importance of funding cognitive security initiatives. We are increasingly relying on artificial intelligence (AI) serving or assisting security. While the potential of AI is far from being fully exploited, it is clear that the technology will continue to advance, and the demand for it will grow. This is partially driven by the fact that AI relies on ICT domains such as big data, cloudification, servicification, virtualisation & softwarisation of networks – all of which continue to evolve apace.

Themed success stories

EOS success stories from previous FP's

In this section we concentrate the success stories in three research areas, and all three represent key Security Union priorities to consider in the future FP9. One very relevant characteristic of these projects is that they require a demonstration of the results in a real environment involving end users. This has proven to be critical to the uptake of innovation and transfer of knowledge. The security issues below are not the only threats to EU security, but what we recognise as the more mature topics showcasing EU research and innovation success stories.

Border security

EU funded research projects have gathered outstanding groups in terms of multinational composition and complementarities. A great effort has been devoted to the seamless cooperation of "experimental" with real-life "operational" assets. In this sense, a major success has been the commitment and involvement of both civilian and military bodies in common developments. The projects have served to develop and test a wide set of systems, assets and platforms and to improve the effectiveness of existing systems, but also have served as catalysers in the area of knowledge building and definition of programmes in border surveillance. As a result, these investments have created an optimum scenario for the Private and Public sectors to foster their cooperation.

In the FP7 framework a significant step forward was made by structuring research objectives to face a context of rapidly changing end user needs. Regarding maritime surveillance RDI initiatives, the three pillars projects namely PERSEUS, Seabilla and I2C have set the requirements for the first POV (Pre-operational validation) CLOSEYE in which most of the previous RDI achievements have matured. In parallel, the focus on CISE through which the other POV EUCISE2020 has allowed to progress data exchange aspects. CLOSEYE, coordinated by Guardia Civil (ES), developed systems and technologies (in some cases up to TRL9) in the field of Command, Control and Coordination, Communications, Sensors and Platforms, Data fusion and Exploitation or Resources Management, among others. Similarly, several Command and Control modules coming from PERSEUS are also in operation and are being exploited at commercial level, and MARISA is a coherent step forward in the improvement of the MSA capabilities of national agencies and EBCG.

Crisis Management, Soft Target & Critical Infrastructure Protection

Over the course of the programme, a large variety of projects have been funded. Some of them led to actionable results and technologies that are on use today. Examples of integrated projects helped to progress on both technological and industrial implementation for the benefit of the citizen. SMEs are among the beneficiaries. But one of the most prominent benefits of the programme is how it structured the European Security ecosystem, which is now less fragmented and more organised, leading to fair competition and active collaboration between Research and Industry stakeholders in the field of disaster management and beyond.

Funded projects like DRIVER+, Scintilla and SECURE-ED, have brought significant research results in the field of crisis management. Those projects not only have increased the operational capacity of end-users with their involvement on experimentation but have brought stakeholder communities closer to working together in crisis environments. This was achieved by bringing together end-users operating in the field and technology providers to address significant needs in the areas of disaster management as well as CBRNe threats.

Cybersecurity

Cybersecurity has evolved from mainstream cybercrime to targeting core critical infrastructures. Traditionally, critical infrastructures in the EU have been operated as stand-alone systems, with dedicated communication networks, thus protecting them from the outside world. However, extending these critical infrastructures with advanced services requires integrating them with an outside network, for example smart grids communicate with all other grids in the country/state to optimally export/import the required power. The necessity of many critical industrial control system applications to connect with other systems exposes them to new vulnerabilities, which can be exploited by cybercriminals, terrorists, or third countries intent on carrying out malicious attacks[5].

The most significant success story within the cybersecurity field has been the initiation of the cyber-security PPP (Public-private partnership) through the feedback of the NIS Platform and its WG on SRIA. The projects that supported these initiatives were predominantly CYSPA, CAPITAL and COURAGE. Significant results were extracted from the three projects and contributed to each of the NIS platform WGs and the SRIA WG. This was complemented by information from the Cyber security community created by NIS. SPARKS also developed security layers aimed at reducing the attack surface of smart grid systems, detecting cyber-attacks in real-time, and improving the resilience of smart grid infrastructure during an attack.

The European Organisation for Security (EOS) is the voice of the European security industry and research community. Operating in 15 different countries, EOS Members provide security research, solutions, and services across many security domains, including border, cyber, transport and crisis management. EOS Members represent almost two-thirds of the European security market, including major industry players, SME's, research centres and universities from across the whole business cycle: from technology R&D, equipment manufacturing, and system integration, to service providers, and end-users.

European Organisation for Security (EOS)
10 Rue Montoyer, 1000 Brussels, Belgium | www.eos-eu.com
EOS is registered at the EU Transparency: 32134385519-64

[5] D. Zhaoyang, "Smart grid cyber security," in Control Automation Robotics Vision (ICARCV), 2014 13th International Conference on, Dec 2014, pp. 1–2.