- Non Paper -

Towards a Stronger Security Union:

Current state of play and future trends in EU Security Research

(Paper produced by the European Commission services to stimulate the discussion in the frame of the 2017 Security Research Conference in Tallinn)

November 2017

SRIEE 2017
SECURITY RESEARCH, INNOVATION & EDUCATION EVENT

A. INTRODUCTION

As highlighted in the European Agenda on Security, research and innovation is essential if the EU is to keep up-to-date with evolving security needs[1]. Criminals and terrorists exploit technological developments and devise more and more sophisticated ways to act and elude investigations. Moreover, the EU is facing new challenges related to cyber-crime attacks on critical infrastructures, companies or public administrations amongst others. In addition, the severity and impact of extreme weather events, partially due to climate change, such as floods or forest fires have dramatically increased over the last years. Other natural disasters, such as earthquakes, also have devastating effects on the lives of EU citizens and EU economy. All of these events call for appropriate action to be taken up at the European level.

As stated in the first Security Union report: *the complex, cross-border threat requires a concerted and multi-layered response. This can only be achieved through trust and joint work by all institutions and Member States*[2]. Only through EU-wide, or even global cooperation, can solutions be found to safeguard the security of our citizens. The need to (re)act is a broadly perceived requirement by society at large. For the first time, the spring 2017 Eurobarometer survey indicates that terrorism is now on top of the issues that citizens cite when it comes to challenges that the EU is currently facing (44%, +12 percentage points since autumn 2016)[3].

Security research plays an important role in the development of innovative security solutions and in ensuring that the EU's research effort is well targeted and tailored to the needs of end-users, such as law enforcement authorities by involving them in all stages of the process, from conception to market. In addition, security research not only helps identifying new security threats and their impacts on European societies, but also contributes to creating trust in new security policies and tools.

Moreover, a strong and competitive EU security industry contributes to meeting the EU's security needs. Whilst technology cannot guarantee security, it is a principal enabler for security in today's society. Furthermore, a strong EU-based security industry ensures that Europe does not have to depend on third countries' technologies in highly sensitive domains.

In this context, Horizon 2020 – the world's biggest multinational research programme – is already significantly contributing to enhancing security in the EU and strengthening the competitiveness of EU security industry.

Against this background, the EU security research is facing two major challenges: the constantly evolving nature of threats and the difficulty to bridge the gap between research and market. The latter is related to the fact that during the research cycle it is often difficult for industry to predict whether there will be sufficient market demand to justify the investment in the development of products that would make use of research outputs. This leads to situations

[1] COM(2015) 185 final.
[2] COM/2016/0670 final.
[3] Standard Eurobarometer 87 – Spring 2017

where potentially promising research outputs are not explored any further and, as a result, certain technologies which could improve security are not made available to end-users. To be effective, security research must on the one hand focus on the concrete requirements of practitioners and on the other hand enable, by design, the effective commercialisation of research results.

This paper sets out the strengths of the EU security sector, identifies the different challenges and illustrates the most prominent actions in addressing them, highlighting how the overall effort can contribute in effectively bridging the gap from security research to the market. Furthermore, it points to future actions and tools to further optimise the process and provides an update on progress made on key legislative and non-legislative files.

B. A STRONG SECURITY SECTOR

Thanks to EU companies' technological advantage and high quality manufacturing European industry is among the world leaders in many segments of the security sector, such as critical infrastructure protection, border control systems and identity management.

The growth prospects for Europe's security sector are promising. According to a study carried out in 2015 at the request of DG Migration and Home Affairs[4], the sector employs 4.7 million people and accounts for an annual turnover approaching EUR 200 billion across more than 20 sub-sectors of the European economy. Most companies in the security sector reported growth over the last five years and a majority of these companies expect this trend to continue in the future. In terms of client groups, market demand for security products and services is also expected to show significant growth, especially in the area of critical infrastructure protection.

One of the major challenges in achieving a competitive EU security industry is the industry's focus on national or regional markets. This is mainly due to the type of products and services that are offered (often niche products), and to the public nature of purchasers which often leads to technical (and at times legal) specifications for the different products to vary considerably from country to country.

As a consequence, if on one side security research is helping industry in Europe to stand its ground against strong competition from the USA and Asia, which obviously also contributes to EU autonomy when it comes to facing security threats and challenges, more can still be done in this area to support the establishment of a security industrial base with a clear European connotation.

C. ADDED VALUE OF EU FUNDING

The security research funded by the European Union brings both improved security and better industrial performance. As already stated, focused research allows the development of technologies and tools that meet the needs of the practitioners dealing with security threats,

[4] Study on the development of statistical data on the European security technological and industrial base (2015)

such as terrorism, cyber-crime, trafficking of firearms and trafficking in human beings, as well as responding to natural disasters. Some examples:

- Supporting EU border management policies: The adoption of the European Border and Coast Guard Agency regulation defines Integrated Border Management as a shared competence between the Agency and Member States. The EUROSUR framework for border surveillance will also evolve to support further integration of enhanced border management systems. Innovative technological solutions will be requested to support these changes. A number of EU funded projects already cover this dimension. Among these, the CLOSEYE[5] project has validated novel solutions for maritime border surveillance in the Mediterranean, thereby also contributing to improve the EUROSUR Fusion Services managed by the European Border and Coast Guard Agency. For example, the Spanish Guardia Civil has taken over some of the validated applications for purposes of Spain's national EUROSUR control and is implementing a joint initiative (ESPIAS) with Portugal funded through the Internal Security Fund

- Supporting EU policies against radicalisation: A number of EU funded projects[6] produced scientific tools and policy recommendations that could be directly implemented by law enforcement agencies and security policy makers, including the Radicalisation Awareness Network (RAN). In addition, other ongoing projects[7] are researching the root causes of radicalisation. The results of these projects could potentially lead to the identification of efficient measures to prevent or mitigate such phenomena.

- Preventing the marketing of explosive precursors: In the light of ongoing efforts to promote the dissemination and market uptake of research results, the Commission is currently examining how the outcomes of the PREVAIL and EXPEDIA research projects (funded under the previous Framework Programme for research - FP7), which produced promising results on the chemical inhibition of explosives precursors, could be appropriately reflected in the revision of the Regulation on the marketing and use of explosive precursors. This could help to make the production of improvised explosives devices more difficult and facilitate the detection of illegal bomb factories.

The strong added value of EU security research is also explicitly mentioned in the "Lamy" report[8]:

*"Investing in research and innovation at EU level will address global challenges (e.g. migration, **security**, climate change, health) which facilitates finding solutions much faster and more efficiently compared to what can be done at national level."* (emphasis added)

In general terms, EU-funded research represents between 8-10% of total public funding for research. The situation is very different in the area of civil security research, where EU-funded research represents 50% of the overall public funding in the EU. The majority of the

[5] http://www.closeye.eu
[6] SAFIRE, PRIME, VOX-POL and IMPACT-EUROPE
[7] PERICLES, MINDb4ACT, PRACTICIES and TRIVALENT
[8] ("LAB – FAB – APP Investing in the European future we want" – Report of the independent High Level Group on maximising the impact of EU Research & Innovation Programmes – July 2017

EU Member States depend entirely on EU security research as only seven Member States (AT, DE, FI, FR, NL, SE, UK) have national security research programs. This dependency on EU research is increasing ever more due to the evolving security threats in the EU and the cuts to national research budgets. This has led to an increase in the added value of the activities conducted at European level as well as in a strong case for increasing EU spending in this domain.

Moreover, the cross-border collaboration inherent in EU funding prevents fragmented approaches and dissimilar standards of knowledge and capacity between different Member States, paving the way for establishing a European single market that would also encompass the security dimension.

To ensure that EU funding for research delivers maximum impact when it comes to strengthening security in the EU, the Commission has launched a dedicated Focus Area on 'Boosting the effectiveness of the Security Union' as part of the Horizon 2020 Work Programme for 2018 to 2020. It has a total budget of one billion euro and brings together different relevant parts of Horizon 2020 (Security, Health, Energy, Space, Inclusive Societies) in order to foster coherence and synergies among them, to improve the quality of projects and their impact, and to make the strength of common research funding in support of the Security Union visible.

In this overall context a special mentioning needs to go to the relation between civilian security research and defence related research since the future Multi-annual Financial Framework will provide for EU funding covering also the latter dimension. While fully taking into account their different specificities (e.g. in terms of end-users, scope and objectives) and affirming the need for a clear separation between the two budgetary lines, synergies need to be further explored between the civil security and defence dimensions both to ensure the necessary complementarity as well as to avoid any possible double funding in areas of potential overlap.

D. CHALLENGES AND HURDLES

While the situation depicted above indicates the strength of the EU security industry and the relevance of EU funding support, the same sector also faces a number of difficulties. These challenges and hurdles, which are outlined below, all contribute to the broadening of the gap from research to the market, hence limiting the EU's ability to effectively tackle security threats.

- **Market fragmentation**: the security market is a highly fragmented market divided along national or even regional boundaries and is also characterised by a high percentage of small and medium sized enterprises (SMEs). Member States are reluctant to give up their national prerogatives, because of the sensitivity of the security policy area. This is even further exacerbated by the current lack of EU-wide provisions for conformity assessment of products and services, industrial standards and technical certification. SMEs typically suffer more from these hurdles than larger companies do.

- **Institutional nature of the security market**: even in areas where there is a broad commercial market, the security requirements are largely framed through legislation. As such, demand is mainly driven by requirements of the national public authorities (e.g. police forces, customs authorities, etc.) that are the main if not sole buyers of end products. In addition, the development of tools to be used by practitioners is on the one side subject to a 'technology push' model and, on the other, limited by standards defined again at national level.

- **Limits of the existing funding schemes**: whilst security threats evolve rapidly and often require urgent responses, innovation cycles in the area of security are quite long and thus offer limited flexibility. As a result, security practitioners might not have immediate access to the tools and technologies they need to address evolving threats adequately.

- **Misalignment between demand and supply:** the needs of buyers and users on the one hand and the offer of tools and technologies available on the market on the other do not always meet due to various factors such as fast evolving security threats and specificity of operational/technical requirements.

- **Competition from third countries:** in the long-run, Europe's place in the world will be shrinking, not only in demographic but also in economic terms. In this respect, the EU security industry will be increasingly faced with competition from third countries, which will affect the EU's competitiveness on the global market. In comparison, US competitors benefit from a stable and strong internal market, as well as recognised US labels, such as the Transport Security Agency certification system for aviation screening equipment. Asian competitors have increasingly caught up on a technological level and benefit from lower labour costs. It should be noted that the highest growth on the demand side is expected to come from outside the EU, in markets such as China.

- **Communication and dissemination of security research results**: this challenge is not exclusive to security research as it is a commonly experienced challenge in the wider area of research. However, in the field of security, the sensitivity (and at times classification) of certain research results further complicates the issue. Nonetheless, without effective communication and dissemination of project results, policy makers and practitioners remain sometimes unaware of very promising research findings. For instance, all radicalisation-related projects have been producing scientific tools and providing policy suggestions directly usable by law enforcement agencies and security policy-makers, such as the experts of the Radicalisation Awareness Network. However, there is still a lot of room for improvements especially regarding the uptake of project results.

E. EXISTING TOOLS AND ONGOING ACTIONS

Addressing these internal and external challenges requires a holistic response that combines both research and industrial policy tools. Annex 1 provides an overview of the tools and actions used to address the different hurdles that contribute to reducing the gap between research and market. The 2012 Communication "Security Industrial Policy – Action Plan for

an innovative and competitive Security Industry"[9] announced a set of priority actions, ranging from standardisation and certification to the use of pre-commercial procurement. Most of those actions have already been implemented or are currently under implementation.

Standardisation and Certification

With the particular objectives of overcoming market fragmentation and strengthening the competitiveness of the EU industry, the Commission is currently involved in a number of standardisation initiatives, primarily in the areas of privacy by design, disaster resilience and CBRN-E (Chemical, Biological, Radiological, Nuclear and Explosives with European Standardisation Organisations (CEN, CENELEC and ETSI)) or through the introduction of standards in relevant legislation.

The pre-normative actions that may lead to improved standardisation for detection of chemical and biological risks to drinking water, radiological-nuclear threats, and/or explosives and weapons are examined by the European Reference Network for Critical Infrastructure Protection (ERNCIP) at the Joint Research Centre (JRC) of the European Commission

In this context, the FP7 research projects CRISP and HECTOS addressed standardisation, evaluation and certification approaches for **security products and systems**. This has led to guidelines for the certification of installed security systems and to the development of innovative products.

In addition, Joint Research Centre is currently developing test materials and kits to enable security practitioners to measure and benchmark the performance of their **explosive detection** equipment. These have potential to become de facto standards. Outside aviation security there are presently almost no performance standards for equipment. A new standardisation action on explosives detection equipment in these areas is foreseen in the **2018 Annual Union Work Programme: for European standardisation[10],** adopted on 25 August 2017.

On **Hybrid Standards** (standards which apply both to civil security and to defence technologies), Software Defined Radio[11] was chosen as a first area for cooperation between the European Commission, the European Defence Agency (EDA) and the European Standardisation Organisations (ESOs). Continuous progress has been made since and work is still ongoing in order to ensure the needed synergies between defence and security sectors.

The Commission has also proposed a European Information and Communications Technology (**ICT) cybersecurity certification** framework that enables the creation of individual EU certification schemes for ICT products and services. Certificates resulting from

[9] COM(2012) 417 final.
[10] COM(2017) 453
[11] Software Defined Radio (SDR) is a radio communication system in which typical hardware components (e.g., filters, amplifiers, modulators.) are managed through dedicated software installed on a personal computer or embedded system.

future EU schemes will be recognised in all Member States. The proposed measures would therefore help addressing the current fragmentation in the field of ICT certification where national initiatives are already in place or emerging without being mutually recognised. Another issue that is being explored is ICT security certification within critical infrastructure protection, building on internationally recognised standards and schemes in this domain.

Finally, a Commission major initiative is the proposal to establish a single EU certification system for **aviation security screening equipment** that would allow ensuring a minimum commonly agreed security level in all European airports, that would contribute to the proper functioning of the EU internal market of aviation security and would increase the global competitiveness of the relevant European industry.

Public Procurement

Most demand for security products and systems comes from the public sector. Different actions in public procurement could stimulate the demand for innovative security solutions, contribute to increased uptake of research results and finally lead to better value for money in the procurement of public services. Actions in security procurement may also lead to a "*de facto*" standardisation (or at least harmonisation) of the currently scattered security market (in Europe) if several Member States were to then jointly finance the development of security products.

The Public Procurement Directive 2014/24/EU aims at facilitating the procurement of innovative products, services or works. Under that Directive the "**innovation partnership**" is an opportunity for public procurers to build innovative products, services or works that respond to a need that cannot be met by what is available on the market. Procurers can structure the innovation partnership in successive phases, following the sequence of steps in the research/ innovation process. The Directive helps institutional buyers to procure security solutions that meet their specific requirements, hence matching demand and supply.

The Defence and Security Procurement Directive (2009/81/EC) established a specific procedure for the procurement of security products, works and services, as well as for R&D&I services. The aim of this directive is to open up the national markets for defence and security procurement by giving the Member States the possibility for a more tailored approach than under Directive 2014/24/EU. There is a need to further explore if and how the implementation of this directive could be further promoted in the framework of civilian security.

Making optimal use of the existing research schemes

The Commission adopted on the 27th of October its work programme for Horizon 2020's final two-year period (2018-2020). Security research will receive more than €200 million in funding for each of these two years. Money will go to projects involving infrastructure protection, disaster resilience, the fight against crime and terrorism, border management and digital security. There will also be a research strand on emerging security challenges such as the protection of people in public spaces or the exploitation of big data to fight criminal activities.

A cross-cutting "focus area" to boost the effectiveness of the EU's Security Union will bring the security research programme together with relevant activities from other parts of the Horizon 2020 programme (ICT, space, health, energy, inclusive societies). This will benefit from €1 billion in research and innovation support during 2018-2020 to help develop a genuine and effective Security Union.

The Work Programme contains a number of features that allow to coherently build on the work done so far, such as:

- A number of open topics calling for pre-commercial procurement according to modalities which have proven to be attractive to the different stakeholders.
- The mandatory participation of practitioners in most topics and additional support for networks of practitioners.
- The support for the creation of networks of procurement agencies and of clusters to bridge the gap between research and industry uptake.
- A built-in flexibility (with many "Open" sub-topics) that should allow applicants to adapt to fast emerging and diversified threats.

Pre-Commercial Procurement and Public Procurement of Innovation:

As already stated, one of the key challenges for security research is to promote the effective uptake of research results in order to develop solutions tailored to the needs of practitioners. While the previous research funding scheme (FP7) allowed for research to go up to the testing of prototypes, they did not allow the development of actual systems proven in operational environment, which is the last step before the commercialisation of a solution. Under Horizon 2020 two new tools have been introduced to aim at closing this final gap: Pre-Commercial Procurement (PCP) and Public Procurement of Innovation (PPI).

PCP research projects are run by the entities which are the final procurers of the solutions to be developed. Within a PCP project the procurers support the development of a solution meeting the customers' operational requirements in close collaboration with industry.

More specifically, PCP enables public procurers and suppliers to:

- Facilitate the access of new innovative players (e.g. start-ups, SMEs) to the public procurement market.
- Share the risks and benefits of designing, prototyping, and testing new products and services between procurers and suppliers.
- Create optimum conditions for wider commercialisation and take-up of R&D&I results.
- Reduce market fragmentation by decreasing costs for procurers and creating wider markets for companies.
- Create highly qualified jobs in Europe in the research, development and innovation domains.

PPI projects are the ultimate step to commercialisation foreseen under Horizon 2020. In PPIs, public authorities, supported by EU funding, invest in the actual commercialisation of

an innovative solution. PPIs are launched when the solution has proven, possibly through a previous PCP project, to be mature enough and ideally suited to the needs of the end-users.

Through PPIs, the Commission aims at modernising public services with higher quality and more cost efficient solutions as well as boosting a particular new market for innovative solutions and helping innovative companies reach economies of scale to grow their business.

An example for such a level of technological maturity and market interest is the field of secure communication. In the EU vast majority of police forces, firefighters and border guards depend on secure communication tools for their work. Due to interoperability issues, cross-border communication is hindered between many countries, potentially jeopardising efficient joint search and rescue operations, joint criminal investigations or joint response to natural disasters.

The Commission has invested over 70 million euro over the last ten years in security related projects that paved the way towards the establishment of PCPs/PPIs. Based on the results of these activities, the maturity of the technology and the interest of the Member States, a number of PCPs will be now launched as of 2018. Among these will be an initiative on secure communications aimed at developing a new interoperable standard solution for secure communication in the EU, which should facilitate cross-border cooperation and support the daily work of the practitioners that are safeguarding the security of the European citizens.

The post-2020 EU research programme will constitute the playing field for further exploring and maturing these strategic instruments.

Mandatory participation of practitioners and security practitioners' networks

Security practitioners are critical actors in the research process since they are able to identify security needs (the capability gap), steer research projects, monitor their output and promote the uptake of project results among their peers across Europe. In this respect, the Commission strongly promotes the participation of end-users in EU security research projects to ensure that the pre-commercial design of various solutions addresses their operational needs. For example, in the area of border management and control innovative detection technologies are needed by the practitioners to effectively combat the wide range of dangerous and illicit goods moving across borders, using legitimate trade as cover loads. End-user support can also contribute to the decision making process when it comes to choices regarding procurement of technologies.

In this context, the Commission launched in 2017 five networks of practitioners (two of police forces, one of firefighters, one on CBRN testing centres and one specifically related to the Danube region).

Furthermore, in order to facilitate and to promote interaction between practitioners, academia, policy-makers and industry, the Commission established the **Community of Users on Secure, Safe and Resilient Societies (CoU)**. It now has **over 1500 registered members** and meets three times a year**.** The CoU constitutes a general (multi-dimensional) umbrella which aims at (1) ensuring that research programming takes into account practitioners' needs, (2) and at identifying the most promising tools and methods, derived from research projects, that could be taken up by practitioners. The CoU also facilitates policy development and implementation and supports the competitiveness of EU industry by ensuring that the expertise of practitioners is made available to policy makers. In this context, a special role is played by the Commission's Disaster Risk Management Knowledge Centre (managed by the JRC) that, by aggregating existing knowledge on disaster risk management activities (both policy and projects), facilitates a better alignment of research activities to practitioner needs and public policies and contributes to the overall effort under the CoU.

To take this action-oriented network a step further, the Commission is now working on the creation of communities of practices gathering practitioners and end-users in thematic clusters under the umbrella of the general CoU. This could leverage the implementation of research output into capability development and enhance the security industry sector. In this respect, following a bottom-up approach, the Commission has started a discussion with Member States on forming such communities of practice. A first such (pilot) platform has covered resilience of the urban built environment and critical infrastructures with a focus on safety and security threats, including counter-terrorism related actions. The main advantage of a 'cluster' approach include a structured approach to short, medium and long term capability development in specific fields, through accelerated innovation, prompt responses to unexpected threats (by calling in the support of an expert community) and tracking the progress of the results of EU-funded research projects.

The role of EU Agencies in research and procurement

EU Agencies, such as the European Border and Coast Guard Agency (EBCG) and the European Agency for the operational management of Large-Scale IT Systems in the area of freedom, security and justice (eu-LISA), are in an ideal position to keep security research close to the experts. These agencies can build bridges between practitioners on the ground and the innovative solutions they need and, as a result, contribute to (cross-border) deployment through procurement.

The EBCGA Regulation (2016/1624) gives the Agency the legal basis to implement part of the "security research" programme of Horizon 2020 that relates to border security. The new eu-LISA proposal for a Regulation follows the example of the EBCGA Regulation.

The delegation of such responsibility to EU Agencies does not indicate an intention to transform such bodies into new research executive agencies. On the contrary, such delegation would be implemented on an exceptional basis and be limited to a selected number of projects in which the transfer of responsibility would clearly provide an added value in relation to the Agency's mandate. The Agencies, as such, are best placed in terms of identifying

practitioners' needs and operational requirements, contributing to the drafting of the research work programme, managing relevant research projects and finally, leveraging the research output by helping to aggregate demand and enable joint procurement by various Member States or, as appropriate, by the Agency itself. Such process would, in essence, efficiently bridge the gap from research to market.

International Forum to advance First Responders Innovation

In early 2017, the Commission joined the **International Forum to Advance First Responders Innovation**. The goal of this Forum is to assist First Responders across the globe in conducting their missions more safely and efficiently. This is done by providing information that may influence the global market in order to develop affordable and innovative technology. The objective for the Commission is twofold: (1) to support the competitiveness of the EU Industry in the First Responder area and (2) to ensure the coherence of EU security research in the field of First Responders at international level. Following the college decision taken at the conference of the Forum on 23 October 2017 in Tokyo, the Commission formally confirmed that it would take over the secretariat and chairmanship of the Forum. The activities of this platform are very closely related to the activities of the Community of Users and thus appropriate synergies will be progressively established.

Smart Specialisation Strategies

Smart specialisation has contributed to putting in place reforms in many Member States and helped to address numerous research and innovation challenges. Smart specialisation strategies are about enabling regions to turn their needs and competitive advantages into marketable goods and services.

The recent Commission Communication "Strengthening Innovation in Europe's Regions: Strategies for resilient, inclusive and sustainable growth"[12] proposed a new set of actions to further help Europe's regions invest in their niche areas of competitive strength and generate the innovation, resilience and growth needed. This includes aligned and simplified rules to allow the combination of funds from Horizon 2020, the cohesion policy and the European Fund for Strategic Investments in a single project. This can be of high interest for the security sector and should be further explored to generate the innovation, resilience and growth needed.

Dissemination of security research project results

In order to enhance the outreach of research projects, the Commission launched a pilot corporate tool - 'the Common Dissemination Booster' (CDB). It includes guidance in identifying portfolios of research results stemming from complementary projects, for which a

[12] COM(2017) 376 final

common dissemination approach offers an added value, or guidance in mapping the relevant stakeholders for a specific thematic portfolio of research results, combined with the use of the most appropriate dissemination tools. This horizontal tool could contribute, as appropriate, to the dissemination of research results in the field of security, taking into account the specificities of this policy area related to EU classified information.

Aiming at better communication of the research results, as recommended by the already mentioned "Lamy" report, the Commission already launched on 22 May 2017 a call inviting tenders to track research results. The project is aimed at designing methodologies for tracking research results after the end of the contractual period of EU-funded projects.

Dissemination of security research project results will also be at the heart of the **Security Research Events** regularly organised by the Commission that will, among others, enable better networking between the different security communities and promote the uptake of research results. Beneficiaries of selected EU funded research projects will present to industry and end-users the systems and solutions they developed setting the conditions for possible implementation in end user products.

F. FUTURE ACTIONS AND TOOLS

In addition to the existing tools and ongoing actions, the EU is assessing the possibility of making use of additional and new instruments to better ensure the impact of security research activities. These initiatives will build on the work already done in the area of security research by complementing them and targeting challenges that have not (yet) been sufficiently addressed.

The post-2020 EU research programme

The Horizon 2020 “Secure Societies” programme has delivered better value for money, improved research outcomes, better cross-border and cross-sector coordination and integration of research and innovation efforts compared to what could have been achieved at national or regional level alone. This trend needs to be continued in the EU research programme that will follow Horizon 2020. In this context, synergies with complementary programmes will need to be further sought and innovative tools such as PCP and PPI will need to be further explored to identify best practices and processes that can overcome the gap between research and the market.
In the discussions that will lead to the adoption of the future programme it will be necessary to guarantee an appropriate level of flexibility of the different tools in order to allow appropriate responsiveness to evolving security threats. The importance of mission driven research funding and the consequent necessary involvement of practitioners to ensure a capability driven approach will be also key features to be maintained in the next Framework programme.
Finally, appropriate consideration will need to be given to the follow up of research projects after their life time, so to ensure their envisaged uptake as appropriate.

Leveraging Private Sector Investment

Private sector investment should be leveraged as much as possible with Member States exploring measures that fit their national policy toolbox, such as tax credits and innovative procurement, and through the use of the guarantees offered under the **European Fund for Strategic Investments** (EFSI). EFSI is a joint initiative from the European Commission and the European Investment Bank (EIB) Group which aims to address the lack of investments in the EU by providing guarantees to economically viable projects with a higher risk profile requiring funding. Through these guarantees, EFSI helps to unlock the additional investments needed to fund promising projects in key economic sectors. Dedicated initiatives will be taken to inform project coordinators and relevant stakeholders of the EFSI portal and hub and of the opportunities that the fund offers also for the security dimension.

Identifying and exploiting synergies and complementarities with national programmes

National programmes under EU funding, such as **ISF Police or Borders**, or **European Structural and Development Funds** (in particular the European Fund for Regional Development - ERDF) could be appropriate instruments to be used by the Member States to further develop and/or procure tools enabled by EU-funded research. Presentations at the Asylum Migration Integration Fund/Internal Security Fund committees of research projects will, among others, be also considered to support Member States to identify possible complementarity and sequential funding vis-à-vis the actions launched under Horizon 2020.

Creation of a European Cybersecurity Research and Competence Centre

In its Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", the Commission announced the intention to create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. This initiative aims, among others, to reinforce EU cybersecurity capabilities, protect critical hardware and software, and to stimulate development and deployment of technology in cybersecurity. It was also announced that the Commission will propose a pilot phase under Horizon 2020 to help bring national centres together into a network in order to create a new momentum in cybersecurity competence and technology development.

Establishment of a European Innovation Partnership on Security (EIP)

European Innovation Partnerships on Security (EIPs) are tools foreseen under the "Europe 2020 Strategy for smart, sustainable and inclusive growth" (within the Flagship Initiative 'Innovation Union'). As previously highlighted, this instrument provides favourable conditions for research and innovation partners to cooperate. Consideration will be given in the framework of the CoU to set up a dedicated European Innovation Partnership on Security. Such a security EIP would build on the CoU activities and in particular on the roadmap developed under project ENCIRCLE which is a common support action funded under

Horizon 2020 with a focus on CBRN. This initiative could support national CBRN action plans and the EU CBRN Action Plan with regard to detection, preparedness and response. ENCIRCLE aims to improve and facilitate European CBRN technology dissemination and exploitation by Member State authorities, international organisations, operators and other stakeholders of the supply chain, including SMEs.

Creation of a RegioStars Award on Security

To identify good practices in regional development and highlight original and innovative projects, DG REGIO created the RegioStars Awards. Many RegioStars winners address common challenges, such as climate change and gender equality, through cross border cooperation. Since security affects the lives of citizens everywhere and should be addressed at all levels (European, national, regional, municipal), to recognise ongoing efforts and to promote good practices, the Commission could select security as an award category in a following edition of the RegioStars Awards. The possibility to have a "Security RegioStar" (for example on forest fires, secure cities or public spaces) will be further examined in this context.

Setting up a dedicated security Knowledge and Innovation Community (KIC)

The Commission will assess the feasibility of launching a KIC focused on security. A decision in such sense will be based on stakeholder surveys and internal analysis that will be carried out by the European Institute of Innovation and Technology (EIT) and should be concluded in spring 2018. Furthermore, the synergies between the existing KICs and the Horizon 2020 Focus Area on "Boosting the effectiveness of the Security Union" will be promoted, in particular the mainstreaming of security concerns in the KICs "Digital" and "InnoEnergy". An example for such synergies could be in the domain of the protection of critical infrastructure. As such, the InnoEnergy KIC is fostering innovation on critical infrastructure protection in the context of smart and efficient buildings and cities while the security research programme will finance a dedicated action on smart cities within the 2018-2020 Work Programme.

G. CONCLUSIONS

This report outlined the strengths of the EU security research sector and the added value of EU funding. It further identified the existing challenges and provided an overview of the measures the EU has already taken, or is planning to take, in order to address these challenges. Such measures represent a diversified set of instruments falling under three broad categories: (1) financial support, (2) policy initiatives and (3) legislation, but each of them contributes in a specific way to the overarching objective of closing the gap between research and market. The table in Annex 1 visually illustrates such comprehensive approach.

To date, the Commission has invested nearly two billion euro in over 400 projects which have brought tangible results. At the same time, the EU is currently facing unprecedented security threats. In order to fight terrorism but also the other not less relevant security challenges in an

effective and efficient manner, Europe needs to consolidate its research efforts and harmonise national security industrial policies to enable the development of technologies, tools and methodologies needed to strengthen its security related capabilities and build resilience.

Notwithstanding the high level of competence of the European security industry, a number of challenges have been identified that prevent a seamless uptake of security research results that are finally made available to security practitioners.

Through a **seamless transition from research to market**, security research should lead to the creation of **a true internal market for security**, based on a strong EU security industry, which could ultimately lead to a **joint procurement of security solutions** by Member States. In the long run, this will require a significant strengthening of the allocated budget.

In a society where the threat is constantly evolving and technological development is fast-paced, Europe needs security research and security industrial policy to constantly support the development and upgrade of the toolkit it needs to effectively counter the threat itself and make Europe a more secure place to be.
Taking into account that both the next financial perspective of the EU as well as the next framework programme for research and development are currently being defined, it is important to acknowledge that such a critical objective can only be met by maintaining a dedicated security research programme which, in addition to being adequately resourced, needs, on the one hand, to maintain a certain degree of flexibility in order to constantly adapt to the evolving situation and, on the other, to be managed by establishing appropriate synergies with other complementary programmes such as the one related to Defence.

Finally, this paper has the purpose of stimulating the discussion on the structuring of the European security research effort. Given the long term perspective of implementing research output in products and services that support the end-users, it is important that relevant stakeholders on all levels are appropriately engaged in the process so to guarantee a coherent and efficient approach to capability development in the civilian security dimension.

*Annex 1: Overview of the different instruments and their effects (+ direct or * indirect) on the different challenges that contribute to the gap between research and market*

Challenges / Instruments	Market fragmentation	Institutional nature of the security market	Limits of the existing research funding schemes	Matching of user needs with research output	EU competitiveness on the global market	Ineffective communication and dissemination of security research results
Standardisation and certification	+				+	
Public Procurement Directive		+		+	*	*
Pre-commercial procurement and public procurement of innovation	+	+		+	*	+
Role of EU agencies in research and procurement	*	+		+	*	+
Mandatory participation of practitioners and networks	*	+		+	*	+
Community of Users and other fora		*		+		+
International forum to advance first responder innovation		*	*	*	+	+
Smart specialisation	+	+		*	+	

Challenges / Instruments	Market fragmentation	Institutional nature of the security market	Limits of the existing research funding schemes	Matching of user needs with research output	EU competitiveness on the global market	Ineffective communication and dissemination of security research results
Dissemination of security research project results		*				+
Making optimal use of existing research funding schemes	*	+		+	+	
Leveraging private sector investment	+		+			
Identifying and exploiting complementarities with national programmes		+	+			
FP9	*	+	+	+	+	+
Creation of a European Cybersecurity Research and Competence Centre	+	+		+		
Establishment of a European Innovation Partnership on Security	+	*		+		+
Creation of a Security RegioStars Award			+		*	+
Setting up a dedicated security KIC		+	+	+	*	*