EOS ‘White Paper’

Towards Holistic European Security and a Competitive European Security Industry

EOS support to the Comprehensive Assessment of the EU’s Security Policies

June 2017
Foreword

The European Organisation for Security (EOS) is the voice of the “European Security Industry” in Europe and beyond. Our goal is to assist in creating a secure Europe, develop a harmonised market and enhance the competitiveness of European security solutions.

With over a decade of experience advocating on behalf of the European Security Industry, successfully promoting a stronger, more streamlined dialogue with EU Institutional stakeholders, EOS is delighted to contribute to the European Commission’s comprehensive assessment of EU Security Policy.

The purpose of this paper is to outline the European Security Industry’s observations and recommendations towards achieving a strong European Industrial Security Policy and European Capacity R&I funding scheme, taking into consideration common threats and challenges. We aim to provide the European Commission with suggestions and feedback on relevant industry policies as well as the progress of research and development projects, but also elaborate on present and future capability and capacity needs.

The European Security Industry (including Research Centres and Universities) represented by EOS, has worked and is working in cooperation with National, European and International institutions and users to improve our security, while looking for an increased level of competitiveness and focussed investments.

At EOS, we cover all aspects of the security sector: Cybersecurity; Integrated Border Management Border (land, sea, check points) and Migration; Fighting Terrorism & Crime; Protection of Critical Infrastructure and Services; Crisis Management (including Civil Protection); Hybrid Threats (focus on civilian - dual issues); and Security Detection Technologies. Most of these areas are tackled both from the Research & Innovation perspective as well as with regard to different aspects of industrial security policy (e.g. standardisation, certification, investments, SMEs, training, etc.).

Since our inception, EOS has advocated for a comprehensive approach to European Security, and a better strategy, developed in Public-Private cooperation and with more focused investments, for research, deployment and use. EOS has proposed such a solution in two of its Flagship initiatives on Integrated Border Management and Cybersecurity, where potential joint actions have been identified as critical for improving the relationship between the European Commission and the European Security Industrial Base. EOS is the founder, and runs the secretariat of ECSO (the European Cyber Security Organisation, supporting the cPPP): thanks to this experience we have today a better view of the challenges and possible solutions for an effective public – private cooperation in security. This approach is all the more relevant today as we look towards an increased level of European sovereignty as well as technological and industrial autonomy in certain strategic and/or sensitive areas of EU security.

Luigi Rebuffi
CEO
European Organisation for Security
10 Rue Montoyer,
1000 Brussels.

www.eos-eu.com
EOS is registered on the EU Transparency Register: 32134385519-64
Introduction

Towards Holistic European Security and a Competitive European Security Industry

In recent years, Europe has considerably improved its security strategy, particularly regarding areas such as border management and cyber security, but major crises (terrorism, migration, cyber-attacks, natural disasters) have put a strain on its capacity for a collective and adequate response. Most of these threats are interdependent and require a comprehensive European approach.

We acknowledge the significant evolution of European security framework over the last ten years, but we urge policymakers to establish a more consolidated approach that would facilitate dialogue between national authorities, the EU, and industry to build more resilient societies. We believe that a strong European Security Industry can provide those solutions and processes to address current and future challenges in European security.

However, today, a comprehensive European capability for EU Security is still in its infancy and a European industrial policy for security has yet to be fully realized. In the current policy framework, we observe many gaps, which create a fragmented market and reduce industrial competitiveness. In most aspects, the previous “EU Security Industrial Policy” has not effectively addressed industry concerns, and most of the topics in its action plan have yet to be implemented.

Market fragmentation remains high at both the political and economic level. The European security industry is often more focused on the more attractive non-EU security markets, than the internal market, providing only a limited contribution to the development of common European solutions. Without an appropriate industrial strategy and incentives for industry, this divisive market approach will not change. There is a lack of strong partnerships between the EU and MS Institutions and the European security industry. A European security industrial base is missing, and efforts to build a stronger dialogue with EU Institutions has often received significant criticism from certain press and NGOs.

In terms of security research, H2020 has helped provide solutions to some of Europe’s emerging security challenges, but ensuring the competitiveness of EU industry has not been a priority due to evolving societal concerns. In February 2004, a Commission Decision was adopted “on the implementation of the Preparatory Action on the Enhancement of the European Industrial potential in the field of security research”. It was an ambitious first step. However, efforts to grow Security Research in H2020 have mainly been managed within the “Secure Societies” framework. This specific framework aims to strengthens the positive impact of technologies towards society, but at the same time challenges the economic and market impact.

The Commission has identified the importance of technology in security and the need for a competitive European security industry in:

- Communication on Security Industrial Policy, European Commission (2012): “We need to be aware of the fact that no technology will ever guarantee a 100% security, but at the same time, no security concept is thinkable without the adequate technologies. A competitive EU security industry is the condition sine qua non of any viable European security policy and for economic growth in general.”

- Cybersecurity Strategy of the EU (2013): “There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.”

- Interim Report by the Chair of the High-level expert group on information systems and interoperability (2016): “Technology and information systems for law enforcement, if implemented in compliance with data protection principles, can help public authorities to protect fundamental rights of citizens.”
The situation is different in the US, as we can see in the summary of the latest report of the US DHS on its R&D strategy (see below).

**THE S&T STRATEGY**

**A More Balanced Approach**

**The Strategic Framework**

**DELIVER FORCE MULTIPLYING SOLUTIONS:**
- Identify and Prioritize Operational Requirements and Capability Gaps
- Make Strategic Investments in High-impact, Priority Areas
- Partner with the Homeland Security Enterprise

**ENERGIZE THE HOMELAND SECURITY INDUSTRIAL BASE:**
- Optimize Markets by Pooling Demand and Developing Standards
- Engage the HSIB through a Deliberate, Continuous, and Transparent Approach
- Improve Programs Designed to Increase Collaboration with Innovative Companies

**ESTABLISH A STRONG AND HEALTHY LEADERSHIP CULTURE:**
- Empower the Workforce
- Provide Meaningful Leadership Development and Professional Growth Opportunities
- Engineer a Pipeline for the Next Generation of Homeland Security Professionals

**Implementation Plan**

To ensure European security, the European Agenda on Security needs to overcome the challenges faced by its stakeholders as they cooperate within the policy framework. Cooperation and joint action is necessary to promote security, but its prerequisite is an open dialogue for the construction of a viable agenda. We believe that only with a multi-stakeholder dialogue it is possible to progress and prepare an effective strategy for the future.

For the future, EOS would welcome stronger public – private cooperation, where EU and Member State (MS) institutions will support the creation of a strong European Security Industrial Base, as they are doing in the defence sector, where EU and national funds will be used to develop, deploy and use European solutions.

EOS ‘White Paper’ on Security

This White Paper draws upon the results of discussions held on 15th May 2017 at a High-level Meeting between the European Commission and the Security Industry, which addressed the priorities and implementation of the European Agenda on Security and of the Security Union, as well as a new “European Security Industrial Policy”. Furthermore, it sets forth recommendations for future actions, in the short term (to be implemented before the end of the present EC mandate i.e. 2020) and in the longer term through the upcoming MFF (Multiannual Financial Framework: budgetary and strategic assumptions for post-2020, the discussions of which are starting now).

The industry recommendations outlined in this paper also draw upon the results of an EOS survey conducted in early 2017, which gathered industry feedback on the EU Security Strategy, H2020 research activities and the 2012 EU Security Industrial Policy. EOS has also leveraged industry perspectives from previous White Papers shared with the European Commission in 2016, as well as findings from the implementation of ECSO, the European Cyber Security Organisation, for which EOS is providing Secretariat support.

The White Paper is divided into four sections:

- Section 1 establishes the European Security Industry’s Global Vision for the future and the objectives towards which is needs to work in order to ensure a viable future for itself;
- Section 2 outlines the Global Strategy we believe will be essential for providing a cooperative framework for EU stakeholders to deliver upon Europe’s security goals;
Section 3 provides an initial view on more immediate actions that industry and policy stakeholders might undertake in the short term to reinforce capabilities and competitiveness in specific European Security Sectors;

Section 4 provides a series of longer term approaches per security sector, based on a sector analysis.

1. Our Holistic Security Vision 2027

The feedback and recommendations presented within this White Paper are elaborated with a long-term vision for the European Security in mind. This vision foresees a series of key goals to be achieved by the end of 2027:

- In 10 years, Europe will have implemented the concrete objectives of its Industrial Security Policy and will have considerably increased its strategic autonomy in all security domains;
- A European Commissioner, dedicated to the EU Security Policy and supported by a dedicated DG, will coordinate budget spending in the transversal sectors;
- The European Commission will have significant investment capabilities, directly or via its agencies or bodies;
- The EU Security Industrial Policy will ensure the coordination of European Commission R&I funds as well as Structural / Regional funds and the ISF, focussing on few main European priorities (following agreement with the EP, Council and Commission). These priorities should include security for the digital transformation of society, integrated border control, the fight against terrorism and crime as well as resilience to natural catastrophes, and for the procurement of European solutions;
- A Public Private Platform on European Security, gathering committed security stakeholders (users and suppliers), will be created (leveraging upon the PPP experience of ECSO), tackling the different aspects of R&I, Security Industrial Policy and fostering dialogue and trust between stakeholders in those areas, which are still not covered by Public Private approach (see for example the issue of cybersecurity with ECSO and its potential evolution into a kind of Joint Undertaking).
- The FP9 (following H2020) will have adequate budget to cover future research, innovation and validation issues with tools and procedures better suited to the specific needs of Europe’s evolving security environment.
- The Union, together with its MS, will have identified a list of technologies / sectors to master and promote the growth of technological and industrial strategic autonomy at the EU level. The list will be regularly updated by a European observatory of sovereign security technologies.
- European regulations will promote procurement of sovereign security technologies and will control technology transfer as efficiently as done in the US or in China. Foreign (non-EU) investments in sovereign technologies will follow a regulation allowing a European technological and industrial strategic autonomy.
- A European NIST (National Institute of Standards and Technology) will be created, particularly for the protection of critical infrastructure and sensitive networks.
- A European Security Single Market will be created, leveraging European labels and a strong certification framework, to be recognised at international level (e.g. ISO).
- Some core common capacity building programmes will be created at European level around key priorities and supported by EU funds.

To achieve our Vision 2027, a strategic partnership needs to be established between users and solution providers, between the European Security Industrial Base, Member States and the European Union, within the framework of the European Agenda on Security and the current development of an EU Security Union. The European Security Industrial Base is the natural partner for the design, development and implementation of solutions to address user’s needs, for enabling technological advantage and guaranteeing strategic autonomy.

A potential mechanism to do so could be the adoption of an EU Security Industrial Development Programme.

Consequently, we ask the European Commission to trigger all necessary means to define a Security Industry Development Programme, the main goals of which should be:

- To develop strategic guidance for the adoption of common legislative measures based on Industrial competitiveness, which deliver effective and innovative insights, methods and solutions for the critical needs of the European Security Industry, and ultimately support the capability priorities as jointly agreed by Member States within the JHA Council.

- To define a technology-based capability development roadmap the EU should identify innovative technologies, standards, certifications, education, training, etc. It should also explore the potential synergies and similarities with the defence sector (funding mechanisms, shared technologies, etc.).

- To foster the Union’s strategic and industrial autonomy as a catalyst for more systematic internal security cooperation among Member States.

- To enhance the competitiveness and innovation of the European Security Industrial Base by promoting a collaborative undertaking to:
  - Set up innovative models of governance (security is a domain very different from commercial or professional markets) and give coherence to existing financial resources.
  - Maintain sustained investment in research and capability development, as well as fill the gap to market through new models of strategic innovation, supporting both foresight methodologies and operational capabilities that can respond to the changing threat environment and evolving risk scenarios.
  - Maintain sustained investment in capacity building for Member States to cover those security gaps that could affect the overall Security of the Union.
  - Provide support to operationalisation and harmonised use of technologies for higher security efficiency, while respecting human rights.
  - Analyse and develop all specific actions, such as the pooling of demand and development of standards and certifications, which should contribute to create a truly European security market that encourages a strong and stable industrial base in the long term.
3. Our Short Term Sectorial Recommendations

EOS and its members have identified a series of “Quick Wins”, or recommendations for action that could reinforce the EU’s Security policy framework and cooperation with a coherent and competitive European security industry. These actions could be rolled-out by the end of the current Commission’s mandate.

Integrated Border Management:

- Creation of a Public Private “Platform” for increased dialogue and coordination in research, deployment and use of innovative solutions with a comprehensive approach (e.g. EES), as well as for operational definition of new tools (e.g. ETIAS).
- Member States facing intense pressure at the external borders of the EU should continue being equipped with a full range of capabilities with flexible and mobile packaged systems and services in hotspots for:
  - Surveillance, and Search and Rescue
  - Identification, Screening and Registration
  - Capacity Building and Migration Management

The above solutions should allow fast decision-making to manage massive, mixed flows, with interoperable solutions (multi-national, multi-agency), clear procedures and immediate access to data from and to the hotspots (See recent adoption by the Council of the Regulation amending the Schengen borders code.)

Cybersecurity:

- Build on the successful beginning of the EU cybersecurity cPPP and the ECSO, increasing its representation and impact on the European market, in cooperation with Commission Services and ENISA.
- Definition and implementation of an EU Certification Framework, adapted to specific sectoral needs, to protect the growth of the EU Digital Single Market and the security of the Union.
- Creation of a European Network to foster and harmonise Education, Training and Awareness for citizens and professionals, to facilitate market growth and job creation, as well as informed procurement and use of trusted solutions and services.

Research & Innovation:

- Consider prioritising R&I into technologies that increase European strategic autonomy (not only digital autonomy).
- Establish pilots to validate existing detection technologies, including users / operators, particularly in the transport sector and urban environment (also linked to secure and smart cities) for improved threat / crisis management.
- Start preparation of a comprehensive R&I strategy for FP9 with closer links between the Programme Committee (Commission and MS) and the Private Sector (beyond the EC Advisory Group) in a PPP-like configuration, for all security R&I issues.
Specific rules for Security R&I in FP9 should consider:
- That the security sector is not a traditional commercial market in view of the sensitive sovereign nature of some of its technologies;
- That funding should be tied to the specific market conditions of the security sector;
- Efficient instruments should be developed to link R&I funds to procurement funds further.

Hybrid Threats
- Initiate a Public – Private (users and suppliers) dialogue for the identification of operational needs and possible solutions to hybrid threats, for civilian and defence issues (also including dual use technologies).

Counter Terrorism
- Creation of an EU Public-Private Platform for Information Sharing / Digital Intelligence for a more effective fight against terrorism and crime. The platform should leverage recent analytics methods and identify areas for effective cooperation and information exchange at European level, while avoiding national sovereignty issues, such as establishing dialogue with the European Counter Terrorism centre at EUROPOL.
- Harmonised EU communication tools for better informing citizens and relevant stakeholders about emergencies and crisis situations.
- More efficient use of social media in intelligence gathering, by creating guidelines for their use by security practitioners.

New Security Industrial Policy
- Creation of a new EU Security Industrial Policy more suited to the needs of the European Security Industry, rather than being submitted to political considerations. A renewed EU Security Industrial Policy should address a range of industry considerations:
  - Standards, Regulations / Legislation and Certification (for all security sectors)
  - Technology autonomy; trusted supply chain
  - Investments: link between R&I funds and investment funds (EU, national, regional)
  - Better links between industry, SMEs and Research / Universities
  - Training, Awareness, and Simulation
  - Dual use / Hybrid Threats
  - Comprehensive R&I strategy
- Creation of a European NIST, beyond the sometimes complex administrative approaches of the EC JRC or of EU standardisation bodies. This body would coordinate European standardisation and certification activities in the various security sectors, while also providing, in coordination with other EU Agencies and Bodies, better visibility on available and trusted solutions to current threats.

Public - Private Platform on Security (in general) and high-level Public-Private Dialogue to support the European Security Industry Development Programme
- Extend participation in the European Commission Task Force for the Security Union to representatives of the private sector - at least initially as observers.
Work towards the establishment of a Public - Private Platform on European Security by 2020 to better define R&I strategy, focus investments, harmonise education and training, facilitate implementation of standards and (certified) solutions according to EU legislations / guidelines.

Regularly (at least once per year) gather high-level representatives from the EU security industry together with EU and MS high-level representatives for a “Security Council” to review and advise on implementation of security policy and consolidate the commitment of EU industry towards priorities of the future MFF. Investments must focus on producing real market oriented solutions that concretely address Europe’s security challenges.

4. Our Long Term Sectorial Approaches

Based on a comprehensive series of analyses of key European security sectors, EOS and its members outline below the challenges faced by each sector in delivering against the goals of the EU Security Union framework, as well present some initial thinking on the most viable means to effectively address these challenges together with policymakers and other stakeholders over the longer term.

The ideas presented herein are a first step in the long-term development of Europe’s security architecture and the role of the security industry within it. EOS welcomes the opportunity to further shape these ideas alongside EU security stakeholders and jointly address some of the outstanding questions in European Security policy and practice.

A. Integrated Border Management / Migration

1.0 Sector Analysis

The Common External Border is a fundamental component for a smooth functioning Single Market as well as the resilience of our communities. External borders are the critical spot for data acquisition, retrievals, information sharing, analysis and checks. Knowing who is entering the EU and under which conditions is essential for effectively managing migration flows. Technology and information systems for border management and law enforcement can help public authorities protect fundamental rights of citizens – an issue that deserves more attention and emphasis. But these solutions can also be a second-to-none tool to enhance cooperation in the fight against terrorism and organised crime. Securing EU common external borders, however, can only be achieved through a common effort.

Systematic cooperation between authorities, comprehensive coordination between all stakeholders and a strong commitment from all layers of our society are key. The EU was created to cope with these challenges and to provide strategic added-value through European-scale projects, fostering cooperation, harmonization and information sharing.

The latest view on the specific challenges of this sector are defined in the COM (2016) 205 final on Stronger and Smarter Information Systems for Borders and Security1, where 3 main actions are identified:

- To improve the existing information systems
- To develop additional information systems
- Address the interoperability challenge

According to the Bratislava Roadmap (16 Sept. 2016) there are 3 strategic concrete initiatives in the Security / Border Management field (which align perfectly our proposed approach for an integrated border management outlined below):

- Operationalise the new EBCG (Frontex)
- Establish EES (Entry Exit System) for recording the movements of non-EU citizens at the EU external borders
- Create an ETIAS to determine who will be allowed to travel to the EU

Border management is one area where EU policies are overlapping. The most important are the migration and asylum policy, the internal security policy, the CFSP (Common Foreign and Security Policy), and the development and humanitarian aid policies, amongst others. Border management approaches have so far been reactive rather than proactive, but significant improvements in policies and solutions are currently ongoing, such as the ETIAS (European Travel Information and Authorisation System), the PNR (Passenger Name Record) and the tools these provide.

However, the coordination between relevant stakeholders, both inside and outside European borders, has not been sufficient. For several years, the European Security Industry has requested a stronger and more open dialogue between all stakeholders to maximise results. When national security needs and requirements are not sufficiently discussed in advance with industry, solutions cannot always address requirements effectively.

Recent events have increased awareness at both political and societal levels of the need for urgent collective action. To safeguard an area without internal border checks and a common external border, the implementation of a comprehensive common policy to integrate and modernise all capabilities for border security management is needed.

Such evolution of operational needs should be supported by continuous investment, yet investment in research and capacity building remains limited. Today’s priorities should therefore focus upon intensifying operational cooperation while using the full potential of technological innovation, and ensuring the EU receives the best value for money.

Only a European Integrated Border Security approach, leveraging innovative capabilities and with sufficient deployed capacities, will provide an adequate answer to today’s border security challenges and threats.

1.1 Smart Borders

The Smart Borders concept is the cornerstone of an Integrated Border Management Platform. It is logical that if the EU wants to secure its external borders, it needs to take advantage of the potential for digital transformation in this field.

The appropriate technology to address this issue already exists. Our members, world leaders in the biometrics domain, have successfully participated in European Commission pilots, and solutions are ready for deployment. Technologies in this domain could well contribute to mitigate certain issues linked to the migration crisis when used in hotspots. For years our industry has invested in these technologies, but political and administrative delays are negatively affecting the implementation.

Initiatives from the European Commission aimed at developing new IT systems, like EUROSUR, EES, ETIAS, ECRIS, a centralised Single Search Interface, Biometrics Matching Systems, Interoperability, Centralised Intelligence Analysis Platforms, etc... are either in progress or in the pipeline, and are setting the foundations of an Integrated Border Management System.

---

In this context, the European Security Industrial Base must be considered a relevant solutions provider for smart borders in the long term. By creating a stable and consistent policy environment, the EU can encourage stability for investment in emerging border security initiatives or the integration of best practices.

The European security sector is a natural partner for establishing technological autonomy for Europe. Ongoing dialogue and the opportunity to contribute to threat mitigation strategy development with policymakers will only enhance industry’s potential to deliver tailored and innovative technologies that respond to European border security needs.

The EU should energize this industrial base by investing in the design, development and deployment of information systems based solutions (infra + equipment + skills), and in those future capabilities that will enable and ensure the safety, security and resilience of the European Single Security Area.

A coordinated public-private approach to Smart Border R&D investments is essential if duplication is to be avoided across Member States. The EU High Level Expert Group on Information Systems and Interoperability should play a critical role in streamlining such investments. Future projects should be chosen strategically, ensuring that they are force multipliers that not only address critical end-user needs but are also aligned with the investments of European R&D organisations and industry.

### 1.2 The Missing Public – Private Dialogue / Cooperation

The EUROSUR regulation is hardly known by decision makers in the European Security Industry and has not often been recognised in EOS discussions with Member State authorities. This significantly reduces Europe’s ability to resolve interoperability issues, an important technological challenge that should not be tackled retroactively. Indeed, border control and migration is not only an issue for public administrations and enforcement bodies, but also one that requires adequate technological support, with solutions assuring security and privacy by design.

Over time, we have seen that the dialogue and cooperation between public administrations in charge of border control, and private companies from the supply sector has not improved. In fact, our dialogue with Frontex has significantly reduced over the last few years, and only limited bilateral discussions are now possible. We hope for an improved industry dialogue and cooperation with the new Frontex structure.

Dialogue with DG HOME has always been very open, with good mutual understanding at a high level. However, recently, channels of communication around operational issues have become more of a challenge. Limiting discussions to Research and Innovation funding is not sufficient to assure interoperable, efficient and competitive solutions are effectively implemented at the European market level.

A wider and coordinated dialogue / cooperation between European institutions, Member State authorities and the private sector, which EOS has been calling for over many years, is now urgent if industry is going to be able to provide adequate solutions.

### 2.0 A New Strategic Framework: An Integrated Border Security / Management Flagship Initiative

Following discussions with M. Ruete in mid-2014, EOS proposed creating an Integrated Border Security / Management Flagship Initiative to the European Commission at the end of 2015. (EOS developed a similar flagship approach for cybersecurity and this led to the creation of the cPPP and ECSO).

This Flagship Initiative links internal security issues in EU Member States, with external border security strategies, as well as with security challenges in Third Countries. Its structure is envisaged around several core topics:
Three Challenges / Threats
- Influx of Migration, internally and from third countries
- Terrorism
- Organised Crime

Three Operational Environments ("domains")
- Maritime Surveillance
- Land Surveillance
- Border Crossing Points

One Integrated Border Security
- Overarching layer for surveillance, information sharing and intelligence-led systems, exploiting and integrating complex data sets and real-time information across domains at the EU level

Two Step Approach
- Short term: immediate deployment of mobile packaged systems and services in hotspots with built-in cybersecurity capabilities (where necessary):
  - Surveillance and Search & Rescue
  - Identification, Screening & Registration
  - Capacity Building in Migration Management
- Medium / Long term: development and deployment of an EU Integrated Border Security

Two Roadmaps for the next 5 to 10 years
- Capacity Implementation Roadmap
- Capability / Technology Innovation Roadmap

One Governance
- Initial Stakeholders Platform evolving into a cooperative instrument with focussed investments

One Investment Objective
- Increase and optimize use of budgets, harmonising R&I and procurement of EU certified solutions in a coordinated EU strategy, targeting €10 bn over the next 10 years

Such an approach, based on effective information-sharing and focusing on priorities with an immediate and sustainable impact on European security, will improve the use of its overall capabilities, and encourage investment in a wide set of technologies and services.

Its specific objectives are:
- Deployment of capacities and services for the different border security domains: maritime, land and border crossing points and development of additional capabilities (where necessary)
- Development and implementation of a European Integrated Border Security overarching framework (capabilities and capacities) for surveillance, information sharing and intelligence-led systems at the EU level, respecting human rights and legal requirements.

To achieve these objectives, EOS proposes creating a Flagship initiative for an EU Integrated Border Security Investment Programme supported by adequate funding (updated estimate of approximately €10 billion over 10 years)\(^3\), which would be composed of:

---
\(^3\) The latest market report drafted by Visiongain estimated the global border security market in 2016 to amount to 18 billion USD. Since Europe is considered to represent 20% of the global market, one can estimate that the European Border Security market amounts to 3.5 billion EUR. If the Flagship Initiative were to incorporate approximately 30% of this annual market over a period of 10 years, investment during that time would amount to 10 billion EUR.
The definition and implementation of a Capacity Implementation Roadmap for capacity deployment across Europe and if / when needed in Third Countries, including short term focus on emergencies and longer term capacity building;

- The definition and implementation of a Capability / Technology Innovation Roadmap based upon a clearer strategy to support implementation of EU and Member State security policies and a Border Security Research and Innovation Strategic Agenda.

EU Member States should identify specific capacity and service needs and flag them in their priorities for EU funding as part of this investment plan.

The European Commission has initially shown interest in this Flagship Initiative, but no decision has been taken to move it forward.

In parallel, EOS has initiated discussions with Ministers of the Interior (MoI) in some Member States to establish a dialogue and consider the possible implementation of such a programme, beginning with key EU countries and key security companies. Such strategic dialogue, especially between Front-Line States, the private sector and EU Agencies aims to put in place a Private-Public Stakeholder dialogue that would foster an integrated border security dialogue at three different levels: European, regional, and national ones. The idea to develop this dialogue, and subsequent platform, at different levels is to assure that our objectives are more likely to be achieved.

A New Implementing Instrument: A Public – Private Platform on Border Security / Management

The European Security Industry should not be confined to the trivial role of “off the shelf supplier”, as the necessary innovative technologies should be developed in partnership with a clear vision on the evolution of needs to allow for effective investment planning both in the public and the private sector. The present bilateral approach between FRONTEX and the different technology suppliers, taken one by one, is not helping the growth of common and competitive European solutions.

We have seen that the typical PPP model on R&I adopted in other areas by the European Commission is barely applicable in this sector, as the market is mainly driven by public administrations. A more specific EU instrument is necessary for effective coordination of strategy, resources and funds assuring a consistent and open public-private dialogue / cooperation with effective use and focus of funds for R&I as well as capacity investments.

A first step to ensuring the proper implementation of the proposed Flagship Initiative would be the creation of a Public – Private Platform. This could serve as a structure for initial dialogue and could be set up immediately in a voluntary mode.

Such a Platform would broaden the current dialogue between public administrations to include the European Security Industry in a multilateral dialogue. This would be needed both for the definition of realistic objectives of the different phases of the Roadmaps, and for strengthening the commitment of the private sector to the implementation of this strategy. This approach would progressively improve the definition and harmonisation of needs for R&I and procurement across Member States in Border Security technologies by 2027.

By creating a better view of technologies and deployment by the public administrations, the Platform would establish trust between stakeholders, and allow the European security industry to overcome its present fragmentation, and better respond to needs through an effective architecture for integrated European border security. The Platform should develop the appropriate procurement processes for European certified solutions. With such a highly sensitive security challenges, public stakeholders, should prioritise the procurement of European certified solutions to guarantee the required security level.
The longstanding fragmentation of the European security market is one of the root causes of its inefficiency. This is hampering the development of a competitive and innovative security industry. For this reason, the endorsed Platform would combine different sources of funding in a more coherent and integrated way. The idea to build a forum wherein different stakeholders (public authorities, agencies responsible for border, and private entities) are engaged should also promote the crucial link between external and internal dimension of security by fostering a better coordination of funding through different mechanisms (like the provisions available also in IPA, EDI, EDF, as well as in the overall EU external action service like CFSP).

The activity of the Platform should not be limited to research issues or it will have a negligible impact on providing practical responses to urgent needs. The Platform would actually prepare all the necessary conditions for better implementation of research results, for instance via test and validation, certification, best practices and demonstration etc. of research results.

Wider objectives, linking H2020 with other funding, facilitating the protection of EU external borders, also with a view to cooperation with Third Countries should also be pursued, further stimulating the growth of the EU security industry. This Platform could eventually evolve into a Joint Undertaking-like initiative on Integrated Border Security, which would provide the most appropriate solution for the full implementation of the flagship recommendations by 2027, due to the challenges of an EU wide initiative leading to a deployable complex system and relevant services.

**EOS PROPOSALS**

- Adopt a Public – Private Flagship Initiative for Integrated Border Security/Management to provide a strategic framework for Europe’s approach to Border management.
- Create an Investment Programme to provide the Flagship initiative for an EU Integrated Border Security with adequate funding.
- Mobilise “Ready-to-Go” Smart Borders / Entry-Exit Technologies.
- Implement the decisions of the EU High Level Expert Group on Information Systems and Interoperability in streamlining and coordinating investment in R&D projects for Smart Border technologies.

**B. Cybersecurity**

**1.0 Sector analysis**

Digital transformation would be useless without Cybersecurity. Cybersecurity is recognized as a new global challenge / playing field with political, social and business implications. It involves serious economic, social, financial and reputational consequences.

The Digital Transformation of our societies, businesses and Single Market cannot be fully implemented without a Digital Union; and Cybersecurity is a precondition of a smoothly functioning digital union. It could not take plain effect if we do not adapt our capabilities to the nature and evolution of the threat. To cope with persistent threats, we need continuous investment and the scale of the threat will only be counterbalanced by delivering force multiplying solutions.
Within the EU single market, operators, utilities, businesses – including SMEs – and administrations must cope with increasing and evolving cyber security attacks & threats. To guarantee the normal functioning of our critical infrastructures and essential services we need technological support from trusted sources and an “informed” ecosystem.

Europe cannot lag behind in developing and retaining the core technologies and skills to feed its own strategic autonomy in this field.

The European Industrial Base should be energized, and strategic collaboration with innovative companies should be strengthened by means of joint technological roadmaps, from research to procurement for deployment and use.

1.1 Cybersecurity cPPP

The contractual Public Private Partnership, has reinvigorated cooperation between interested stakeholders (more than 200 members are currently participating in this initiative), strengthening European industrial potential on cybersecurity. The European Cyber Security Organisation (ECSO), supporting the cPPP, is a platform where European Member States’ public administrations, industry, practitioners and other stakeholder discuss and identify strategic priorities for Europe.

The cybersecurity cPPP was set up in record time, in part thanks to the extensive preparatory work and support from EOS (who runs today the Secretariat). The cPPP is focused upon developing R&I activities, as is usual in such European Commission initiatives. However, ECSO was created not only to support the cPPP and the definition of R&I priorities, but also to foster effective cybersecurity industrial policy activities in public-private cooperation to increase security and competitiveness.

A lot has been learned on effective Public Private cooperation in ECSO. These “best practices” in such a sensitive sector could be successfully applied in the creation and development of a similar Public Private Platform for European Security.

The cPPP on Cybersecurity was the first move towards a more complex Public Private approach (a Joint Undertaking style initiative could follow) and higher investments in the next MFF.

From an industry perspective, the cPPP should ultimately help EU policy bodies to foster and incentivize a leading industrial cybersecurity sector in our continent. We remain committed to promoting the cPPP and investing in our shared vision for the future. As such, we support ongoing public-private dialogue to define those cybersecurity domains in which European industry can become globally competitive leaders, a coordinated industry approaches to maximising current skills/competences, and the promotion of European cybersecurity industry’s strongest assets.

1.2 Digital Autonomy & Sovereignty issues

In parallel to the work of the cPPP, the EOS Cybersecurity Working Group (WG) has the capacity to initiate dialogue and develop recommendations on sensitive issues such as cybercrime, intelligence, cyber-defence, digital autonomy and other sovereignty-related issues. The aim of the WG is to foster public-private dialogue to address digital autonomy in terms of technology, policy solutions and intelligence sources. It focuses on delivering a European dimension for cyber-security related issues that are of strategic concern to the European security industry, and to the European economy as a who

As an example of a sensitive political and technical topic, the EU industry (within the EOS Cybersecurity WG) could work on a common technical/political paper on encryption to assess the issue and provide suggestions for a European position that takes into account national sovereignty issues.
1.3 Digital Intelligence

Digital Intelligence should come not only from a public-public dialogue, but also from a stronger link with the EU Security Industry. At national level, our industry belongs to those “trusted partners” supporting local governments in intelligence issues. Yet, at European level, information is drawn from industries that have non-European origins, even if largely present in Europe: this raises questions on the influence of external agendas in EU positions.

The moment is ripe for a more formal dialogue on the question of European digital intelligence and EOS would welcome the opportunity to contribute to this politico-technical debate with European policymakers. This dialogue should strive to define answer to some of the core questions around Europe’s ambitions for its digital intelligence capabilities and governance, including:

- How EU industry competences at national level (sensitive) can be of use at EU level?
- How to build a European information sharing system and what structure this could have?
- How progressively increase a trusted sharing of threat intelligence?
- Can we create a big-data at EU level for security use?
- What kind of EU digital autonomy is possible in this sector?

EOS PROPOSALS

- Develop an effective instrument to widen the dialogue and cooperation beyond the present cPPP approach, to better support competitiveness of the European cybersecurity industry.
- Identify and develop technologies that would increase a strategic European Digital Autonomy.
- Establish more formal public-private channels of communication to address questions around European Digital Intelligence.

C. Research & Innovation

1.0 Sector Analysis

Since its inception, EOS has been supporting European Commission funding programmes aimed at fostering innovation as well as the uptake of technologies. H2020 and its predecessors have improved European potential for innovation in many respects, especially by building synergies with National and Regional research programs. This has not only improved the efficiency of public spending, but has also created a wider network of stakeholders, ideas and projects.

Future research could better target terrorism issues, but the approach should be different (top down) with a comprehensive, long-term strategy and defined implementation measures (which is difficult under the H2020 Secure Societies programme) in order to incentivise an effective commitment from industry. The strong shift from FP7 to H2020 towards “societal issues” has resulted in R&I projects increasingly lacking a competitiveness component, which is so important for our industry in this “sensitive market”.

The simplifications introduced in H2020 (e.g. in the Participant Portal and in the reduced time to grant) should be recognized as a positive step for industry funding. Evidently, SMEs in the security sector have faced more challenging conditions for project financing. In fact, the closer to the market, the less funding they receive, and for SME’s and micro SME’s that is a sustainability factor. Before the simplification of the one rate scheme, SME’s could receive all the funding (100%) they had applied for. Nowadays, under H2020, the maximum funding for Innovation Action’s is 95%, that 5% is a considerable change. Consequently, we have observed
reduced interest in dedicating resources into EC projects by SME’s as well as large industry, for reasons linked to sustainability but from another perspective.

The introduction of stricter quality management by the European Commission has facilitated an increase in the quality of proposals. However, industry interest in participating in such collaborative projects has evidently decreased because of this new approach. The evaluation mechanism for project proposals is not clarified, and in most cases the description of calls does not match the evaluation results. Higher TRL initiatives demand a more focused concept in order to create a marketable solution; thus, higher quality is welcome. But higher quality and increased importance assigned to societal impacts have meant less innovation. For these reasons, H2020 rules and regulations have been received by industry with two very distinct opinions. With reduced interest from large companies in collaborative research, less innovation is being brought to market, as large companies remain the main vehicle driving the market inside and outside Europe.

While POV’s and PCP’s have proven more successful in bringing innovation closer to the market, problems still remain. Even if procurers are in the consortium, the uptake of the tool or technology solution is still undetermined and slow. This was also one of the main gaps presented in the security industrial policy. Industry, through specific policies aiming to boost their productivity, should be reassured that a market will exist and that their investments in innovation are worth.

Security is a very different sector from other European Commission R&I areas. If in FP9 preference will be given to loans rather than to grants, this lack of European incentives would reduce Europe’s attractiveness as a place to invest in innovation, especially from the side of SME’s. Adding this potential challenge to a weak approach to industrial competitiveness could lead to a total disaffection of the European industry for EC projects. This could have significant negative consequences, considering the sensitivity of security for Member States and Europe, where stronger strategic industrial autonomy would be essential.

2.0 EU financed security research: Topics for future research programmes

We reaffirm our interest in the topics of Critical Infrastructure Protection, Border Security, Disaster Resilient Societies, Fight against Crime and Terrorism and Digital Security. And for the future Secure Societies calls, we would envisage including the following:

- Cyber/Physical protection of critical infrastructures, especially regarding soft targets (link to work of the Task Force in DG HOME) as well as for urban security, energy, transport and innovative telecommunication networks (e.g. 5G);
- Intelligence / automated command and control centres including cyber-intelligence (analytics);
- Protection of strategic manufacturing areas (digitalisation of EU industry / Industry 4.0) and of important innovations for the society (e.g. autonomous vehicle);
- Development of test procedures for security devices;
- Analysis of social media content and automated exchange of data between law enforcement authorities;
- Network of standardisation and certification agencies throughout Europe and beyond.

Current and ongoing EU-financed security research programmes have been proving very successful in providing a springboard for industry not only to research new technologies but also move closer to deployment and implementation. A snapshot of these research programme success stories can be found in Annex I & II.

3.0 Technology Autonomy

The present European Commission research approach does not focus on technology autonomy for strategic sensitivity, security or competitiveness reasons. It is still very fragmented and dispersed, lacking a clear overall strategy. Despite the existing EC mechanisms, R&I still suffers from stovepipe approaches. Structured cooperation between industry and regulators could help to defragment the system and develop a
comprehensive approach. Yet, at present there is still no adequate EC instrument to accomplish this. The EC PPP model linked to a “leverage factor” is not applicable to "public markets" like the security. Without R&I “carrot funds” or the coordination of other implementation funds, there is little hope of establishing a comprehensive and strategic approach involving different kinds of stakeholders.

4.0 Streamlining Security Screening and Detection Technologies Certification

Information on existing security screening and detection technologies solutions is not originating from EU research in this area, as it remains too sensitive to be shared. The EU Certification of Civil Aviation Security Equipment took four years to be proposed. We support the goals that the Commission’s Proposal for a Regulation aims to achieve. Yet, the current proposal is overly complex and potentially bureaucratic. Additional costs will inevitably be incurred by the addition of complexity and bureaucracy, adding new barriers to entry into the security market and reducing the funding available to invest into research and development. In general, to support Europe’s security industry, the Regulation must be significantly leaner, with fewer administrative and financial burdens placed on manufacturers.

On land transport security, EU pilots to adapt existing technologies could be established immediately.

**EOS PROPOSALS**

- Maintain and possible increase, within future FP9 research funding calls, topics including cyber/physical protection of critical infrastructure as well as the use of social media as a cross-cutting topic.
- Consider from the beginning of future PCPs with commercialization aspects in mind. Incentivize EU technology autonomy through targeted funding for development or implementation of European security technologies.
- Further simplify the bureaucratic burden for SMEs and end-users.
- Establish EU pilots to adapt existing security screening and detection technologies to broader transport security modes (e.g. land transport) and encourage European industry participation.

D. Hybrid Threats

1.0 Sector Analysis
The past decade has seen the increased deployment of hybrid threats from both State and non-State actors aimed at harming and destabilising EU societies. The mixture of conventional and unconventional methods that define hybrid threats have further blurred the line between European defence and security strategies, requiring an ever more coordination and multilateral response. The EU’s Joint Framework to counter hybrid threats and foster the resilience of the EU goes someway to enhancing European capabilities, through cooperation between EU Member States, partner countries and NATO. However, the Framework’s holistic approach fails to acknowledge the role that the European security and defence industries might play in such threat mitigation initiatives, or provide a platform for integrating industry into the development process of European solutions to new hybrid threats.

2.0 Dual Use Solutions
The impact and mitigation of hybrid threats on both internal and external EU security should be seriously considered by public decision-makers and industry together. Furthermore, approaches should recognise the potential of dual use solutions to emerging hybrid threat. In general, defence and security should be better harmonised and not be the cause of antagonism between the different public and private stakeholders in Europe. Yet, it could be preferable to keep a distinction between the future Defence Research Programme and the Security Research Programme, in order to avoid budget reductions.

### EOS PROPOSALS

- Mobilise an EU forum for dialogue between regulators and industry to consider and encourage dual-use solutions to evolving hybrid threats.

### E. Counter Terrorism

#### 1.0 Sector Analysis

The past two years and multiple attacks on softer and critical European targets have revealed the polymorphous attitude of evolving terrorism strategies. Europe now has strategies on the financing of terrorism, on online propaganda, and the support of the Counter Terrorism Coordinator to propose updated strategies and actions.

#### 2.0 Information sharing strategy, process and implementation

The asymmetrical nature of terrorism however requires:
- consolidated sharing of information between Member States;
- better clustering of national authorities and emergency plans, a mapping exercise would be beneficial to understand the levels of preparedness, mitigation and resilience;
- innovative tools and solutions used in each Member State, and adaptation to more novel options.

The increasing threat of terrorism in Europe over the last few years has strengthened the belief by European intelligence bodies (and politicians) that stronger cooperation and dialogue is needed. Open channels of communication, both between Member States and with the private sector (operators), are essential for sharing immediate information on critical services / infrastructure, and soft targets. Cooperation with technology providers that own or develop innovative solutions using, for instance, big data analytics or artificial intelligence, should also be integrated. There is also a need for EU practitioners to better harness technologies that are already existing in the market. This can be achieved through better dialogue between users and suppliers.

It is also becoming very clear that counter-terrorism is a cross-cutting theme through some of the EU’s most critical security challenges. Foreign fighters, and their return to Europe alongside migrants crossing the Mediterranean, is a known threat, but trafficking has also proven to be a key source of terrorist financing too. In this regard, innovative technology solutions for the detection of such illicit movements in border regions, and preventing attacks against infrastructure or public areas is highly relevant.

Furthermore, innovative technologies will be essential in combatting the online presence and reach of terrorists. Online presence, however not only facilitates the above mentioned illegal acts, but it also helps intelligence services and border guards, track the movements of undocumented or illegal migrants, check their identity, but also check routes that they have taken through IP pinned in different locations. In addition to, anticipating boats coming into the Mediterranean from third countries.
F. Security Industrial Policy

1.0 Sector Analysis

Without the support of the European Security Industry there will be no security in Europe. One of the most important roles of the EU Security Industry is its contribution in protecting Europe. Yet, today dialogue between EU Institutions and the EU Security Industry is woefully lacking in many areas and industry is not in a position to contribute to formulation of the future of European Security.

- Without a dialogue with industry, industry is just a simple provider of COTS (Commercial Off the Shelf) and complex systems, so EU industry competes fiercely pulling down prices and letting non-European companies, sometimes not following security and privacy criteria adapted to our society, to deploy insufficient solutions in our market.

- Cooperation with industry could provide the needs-based technical input and advice through specific channels (e.g. EC / MS Task Forces) based on national / international experience and trying to foster trust and a synchronised action with an industrial perspective.

2.0 A renewed Security Industrial Policy

The European industry needs European references also to support its exports and a higher strategic technology and industrial autonomy to provide EU governments with validated and trusted solutions supporting European sovereignty, when necessary.

In July 2008, EOS proposed to the European Commission the creation of a Security Industrial Policy to support the development, implementation and use of adapted security solutions for Europe, as well as supporting the competitiveness of the European security industry.

The Commission issued a Communication in July 2012 presenting their view on such a Security Industrial Policy, but it proved quite limited in scope with respect to EOS recommendations. The 2012 Action Plan for an innovative and competitive Security Industry was conceived as a first step for the revival and expansion of relations between public stakeholders and the EU Security Industry. After an initial period of good dialogue between national and European public administrations and the private sector, the actions envisaged in such an Industrial Policy have almost disappeared or been further significantly reduced in importance in the eyes of European industry. Since the conception of this Action Plan, topics such as third-party liability limitation, became obsolete for Europe, while issues around societal impact monopolised valuable resources away from industrial capability-building initiatives. Societal impacts are in fact very important, but a solution, a concept or a method cannot be evaluated on softer issues alone.
We continue to believe that a strong European Security Industry is possible but it requires a well-structured and more supportive policy environment, and a renewed industrial security policy could provide this support. By taking a comprehensive approach, this policy should address the full lifecycle of the industry supply chain, from R&I to implementation, to retrofitting existing security infrastructure for improved performance.

Together with the creation of a structured cooperation between the public sector and industry, possibly around a flagship approach for focussed investments, a renewed EU industrial security policy is EOS’ key recommendation for creating a supportive policy environment for European industry to contribute proactively to the Security Union.

The renewed industrial security policy should tackle:
- Standards, regulations / Legislation and Certification
- Technology autonomy; trusted supply chain for security components
- Investments: link between R&I funds and investment funds (EU, national, regional)
- Better link of industry with SMEs and Research / Universities
- Education, Training, Awareness, Simulation
- Dual use / Hybrid Threats
- Comprehensive R&I strategy

Focus on standardisation

One of the main topics of the first Security Industrial Policy was standardisation. The aim was to “to ask the European Standardisation Organisations to establish concrete and detailed standardisation roadmaps”. Standardisation however, in the security domain, remains a challenge for the security industry due to market and company sizes compared to their Eastern and US counterparts. The EU supports the standardisation activities mainly through H2020 projects by either focusing on specific research areas or a specific solution. This however does not tackle everyday operational needs. Standardisation activities are thus dispersed and tackled by topic instead of holistically per security challenge. To help with the implementation of innovative technologies, in certain areas, we can follow the example of the CEF, which is the funding instrument with which air traffic management stakeholders work. CEF funds the deployment phase of the results from R&I performed under the SESAR program. Something similar could be envisaged for other sectors. Overall, the funding schemes could assist in the implementation of EU policies if aligned properly. The ISF could drastically assist in information exchange between law enforcement for example.

We suggest establishing minimum requirements for technologies and solutions which are not regulated by any standards or legislation, to protect European citizens from products that may infringe upon their Fundamental Rights.

Furthermore, a better harmonised certification system should be set up to tackle certification issues in all security domains, maybe supported by the creation of a European NIST. This could help innovative business models with the support of insurances via use of validated and certified solutions in a trusted supply chain.

Focus on information exchange

Information exchange amongst law enforcement authorities as well as between practitioners and procurers or industry remains an effective challenge. Several networks of law enforcement were funded through H2020 with aim of facilitating better dialogue with other stakeholder. Nevertheless, initiatives in the field of interoperability and information exchange have been for years defined and managed in a very fragmented way. Thus, we urge more engagement from the European Commission as a key facilitator in these projects.

Specifically, interoperability and information exchange initiatives have been lacking in the area of border management and counter terrorism. Member States tend in their purchasing methods not to involve the European private sector at an earlier stage. In some instances, Member States use solutions developed outside Europe, which increase discussions on privacy and protection of fundamental rights.
G. A Public - Private Platform on Security

1.0 Sector Analysis

Existing bodies (Programme Committee) and structures (PASAG – advisory group on Security Research to the EC) do not necessarily provide a strategy for security R&I, like PPPs are supposed to do.

Ten years ago, ESRAB proved to be a relatively positive experience but a closer link between R&I and capacity building (such as provided in ECSO) is needed. Without such dialogue, we will not achieve all the objectives outlined in the previous chapters. While there are commonalities between security and defence technologies, particularly at low TRL, their applications remain so different that R&I and capacity building initiatives should make the distinction between the two sectors.

2.0 High-Level Public Private Dialogue

In the short term, we envisage a Public - Private Platform on European Security will be established by 2020, which will already be supporting the European Security Industry Development Programme and better defining the R&I strategy, focusing investments, harmonising education and training, facilitating implementation of standards and (certified) solutions according to EU legislations / guidelines.

By 2027, EOS will be co-organising regular high-level meetings with senior European Commission decision-makers (including relevant VPs and Commissioners and their DGs, with CEOs of EOS members) to identify the future of the Security Union, agree on common steps and commitments. Working level meetings between our industry and the European Commission will become a regular feature of the work of the Public-Private platform to track the implementation of the development programme in the long-term.

EOS PROPOSALS

- Creation of a Security Industrial Policy to support the development, implementation and use of adapted security solutions for Europe, as well as supporting the competitiveness of the European security industry.
- A Security Industrial Policy should encourage the development of frameworks for standardization including minimum requirements for unregulated technologies, and a better harmonised certification system.
- EU facilitation of dialogue between industry and law enforcement/security services to address critical challenges around interoperability and information exchange.

EOS PROPOSALS

- Hold regular High-level EU-Industry Roundtables to share perspectives on the future of the EU Security Union by 2027.
- Hold regular and frequent operational meetings between the EU Industry and the different EC DGs to follow the implementation of a new EU Security Industrial Policy and other concrete security measures.