EOS contribution to the Public Consultation on the future of Home Affairs policies: “An open and safe Europe – what next?”

Introduction

An open and safe Europe guarantees fundamental rights and creates the optimal conditions for a European area of Freedom, Security and Justice. Therefore, it is vital to protect all citizens and enterprises, vital services and infrastructures from any form of hazard which could disrupt the normal functioning of democratic societies.

Security is a right for individuals and a key pillar for well-functioning organisations and economic sectors. Security should be embedded in social and business processes, rather than seen as a set of constraints impairing economic flows or endangering civil liberties. There might be cases where trade-offs are needed between the latter and approaches that are intrusive by nature, but Industry in combination with Research Technology Organisations (RTO) can provide technological solutions that fit in a proportionate strategy and, even better, can contribute to business facilitation and easier living.

A safe and secure environment is the very basis on which any stable society is founded. A competitive EU-based security industry, offering solutions for enhanced security can make a substantial contribution to the resilience of European society. Investments for economic growth and job creation will be increased in safe and secure environments: stability and security are crucial incentives. In Europe, it is evident that investments are growing in secure cities and territories, where the likelihood of achieving a return on investment is higher and where citizens, no matter what their nationality, feel safe.

Security is an enabler for a safe economic development, and technology is a driver for better security and sustainable growth.

1) Analysis of the present situation as seen from the security supply sector

Reflecting on the Stockholm Programme, we can see that many of the threats and priorities for European security defined in 2009 are still valid. Yet, five years have passed. The European Commission has built up and / or refined its policies in specific security sectors (e.g. cybersecurity) and developed a comprehensive Internal Security Strategy (ISS). A Security Industrial Policy has been proposed to face the technological and industrial challenges of the ISS implementation. Even though the actions foreseen by the ISS and its link with the External Security Strategy and the CSDP for protecting European interests in Third Countries are still under implementation, we recognize the considerable evolution towards a global approach at European level in the security sector. The role of Europe on the international scene has increased in the last years and European policies are now better supporting this role of stabilisation and increased global security.

The European security industry still faces several challenges to its competitiveness: a highly fragmented internal market, a gap between research and market and a lack of clear paths for societal acceptance of security technologies. The industrial security strategy set up by the Commission is trying to take care of these challenges. We think that DG HOME should also pay particular attention to these issues in their policy-making on security, for their high impact on European competitiveness.

Clear European security strategy and policy is an enabler to the security Industry and RTOs as it supports better planning of investments and provides a target for focusing technology innovation. It should also not be overlooked that solutions and services implemented in Europe can cite this fact as a reference, making them more exportable in the global (more dynamic and competitive) market.

The creation of a specific DG (DG HOME) within the European Commission to manage security issues as well as the creation and / or the progress of dedicated European Agencies (EU LISA, EUROPOL – with its EC3, FRONTEX) have been major steps forward in clarifying responsibilities and identifying dedicated interlocutors for the European security supply sector. And yet, continuous and trusted dialogue with industry (as in other EC DGs and sectors) is still limited and should further be deepened and focussed more on the whole innovation chain for security solutions. Moreover, new domains such as cyber security are still crossing over the remit of several institutions, both at European and national levels.

A significant effort has been made to include security as a specific topic in the European collaborative R&T programmes, which has contributed to the emergence of a security research community and provide a focus for innovation. However, priorities are still being defined without an end-to-end vision (and strategy) of the concept-to-product path, and according to national political agendas where common European interest should prevail. Even worse, keeping security as a specific theme in H2020 was not a given, and although achieved in the current Regulation, has been finally done without a sufficient increase in funding and subject to its being part of a more global set of societal challenges. Furthermore, the speed of funding allocation and requirements associated with H2020 research prevent it from being suited to the rapidly changing and IP-rich nature of cyber security technology development.

While understanding that enforcement of security measures is and will remain a sovereign prerogative of Member States, the implementation of European policies, regulations (when needed) and standards will help to harmonise the European security market (still very fragmented) and contribute to the competitiveness of the European security industry at global level, keeping highly skilled jobs in our countries. European solutions supporting European security policies will not only contribute to guaranteeing that our European specific view of privacy and respect of human values will remain at the heart of our innovations, but will also support European technological independence. This is key to avoiding possible security breaches, as we have recently seen.

2) Key security challenges and priorities in the next 5-10 years, as seen by the security supply sector

Present security priorities are similar to those mentioned in the Stockholm Programme, but operational needs and approaches have evolved in the last few years.
As derived from discussions with customers of our members, present and future security needs are:

- **Fight against (organised) crime:** organised crime is benefiting from the use of the latest technologies to increase its activity, without limit of borders and law. Smuggling of goods and drugs is helped by fast moving vehicles (particularly at sea). Fraud and crime are also facilitated by the increasing use of digital tools.

- **Terrorism:** intensified security measures in Europe have reduced (while they cannot be totally excluded) the risk of terrorist attacks originating in our countries. Yet terrorism remains active in Third Countries (due to instabilities, mainly in African and Asian countries) with a consequent threat to European interests (citizens, assets) and could give birth to threats propagating into the European Union.

- **Trafficking and smuggling of persons:** irregular migration is not only a societal problem but is also linked to criminal activities such as trafficking and smuggling of persons coming from unstable countries and difficult situations. Instabilities and poor societal conditions will further exacerbate this issue. Recent dramatic events in the Mediterranean have shown the situation is getting worse.

- **Citizens' protection:** citizens are largely benefiting from mobility: free movement of people, goods and information. Yet this mobility is also a source of threats, as transportation and communication are increasingly vulnerable due to interconnected networks. Key services for citizens are also increasingly interconnected and vulnerable in an urban environment.

- **Natural and man-made disaster management:** regulations and environmental rules are trying to limit man-made disasters and environmental crime. Yet there are natural disasters (also due to climate change) that cannot be avoided (e.g. earthquakes, large storms, flooding, pandemics) but only mitigated in their consequences. Populations must be prepared so that they prevent and/or react in suitable ways, and public forces should have the necessary processes and tools to cope with these events in a timely and cost-effective way.

in the different security sectors:

- **Border control**: The required capabilities and capacities for the implementation of EUROSUR should be progressively installed and their efficiency controlled, with operation across countries (e.g. maritime surveillance in the Mediterranean for law enforcement against goods/drugs smuggling or search and rescue operations to save lives of migrants at sea). Needs will continuously evolve as threats and criminal methods will continue to adapt (small boats, new migration paths, increasing numbers of refugees, etc.). Support to Third Countries (e.g. African) to better control their borders would reduce criminal risks (including piracy) to local European interests and citizens as well as proliferation of terrorism.
  The Smart Borders initiative, presented two years ago, still has a long way to go before its effective introduction. Implementation of the Entry-Exit System and Registered Travel Programme will help identify potential security breaches related to illegal transiting and over-staying of non-resident people in the Schengen area. It could also be a powerful tool for simplifying migration flows at EU borders. To achieve this goal, the implementation methodology and the governance for these systems should guarantee a more timely and cost-effective achievement than we have seen with the predecessor systems. A comprehensive view of border management, including the integration of regulated and unregulated borders on the one hand, and the integration of the monitoring of the flow of individuals and goods (incl. customs) should be targeted in the long run.

- **Protection of critical infrastructures:** EPCIP has made limited progress, although we recognise that some work has been done in the CBRNE domain at EU level. Member States have not been very forthcoming in identifying critical infrastructures and do not wish to face interference regarding the security measures they adopt. Operators still prefer to pay the consequences rather than invest to prevent potential risks. Political decision makers are not often keen on increasing the security level as long as they believe more demanding requirements would disrupt the economy of operators.
- We also must consider potential impact on privacy that these measures could bring, or at least the potential negative image that could be portrayed when presenting security solutions. The right compromise between security, privacy and economic advantage is still to be found. Areas like transport and energy are providing help in this learning curve, showing that security solutions can even lead in some cases to the global improvement of business process performance. Whereas other areas like ICT (Information & Communication Technologies), Finance, Administration or Health are for different reasons very sensitive as they have specific needs from country to country, which are difficult to tackle at an overall European approach. An increased use of a risk based approach should help better understand threats and develop common / harmonised measures and process that can benefit both users and operators, but also boost the competitiveness of security suppliers.

- **Cybersecurity:** during the 2010 – 2014 period, threats and crimes in cyberspace have significantly increased, becoming more notable in size than drug-related crime. This growth is likely to continue. Our society is increasingly based upon digital solutions and information exchange. This is creating a potential weakness in all sectors: financial, transport, energy, health, societal etc. The adaptability and rapidly changing nature of cyber threats to critical infrastructure, services and citizens in general is such that a complete elimination of these risks is totally out of reach. As a result, even more than in the other sectors, the agility of security solutions is critical to keeping on top of the risk.

- **Urban security:** protection of citizens and of vital services and assets in the urban environment is becoming a key security issue, since about 80% of the population in Europe lives in cities. The urban fabric is becoming more and more interconnected in all its services: food, water, transport, energy, health emergencies etc. Large cities are also nucleus of specific criminal activities, often enhanced by concentrated societal issues. Until recently, the different threats to security in an urban environment have been considered separately. Main cities are now considering all these issues together to find more suitable and efficient solutions for optimising resources and reducing potential risks. More coordinated measures aimed at protecting citizens, infrastructure, processes and assets within urban spaces from man-made and natural threats are needed. The involvement of citizens in this process is essential: they should organise themselves and become participants in achieving security. The creation of a specific EU policy for improving the security and resilience of urban spaces, firmly anchoring security as a fundamental pillar of the "smart city" should be envisaged as one of the objectives of the future Home Affairs Programme.

3) Technology can help by providing higher efficiency in the different security sectors related to Internal and External security, while respecting citizens' privacy and fundamental rights

Criminals are exploiting technology and divert innovative services to increase their returns. In which case, shouldn't law enforcement users and operators also use innovative technologies to prevent and mitigate crime, terrorism and disasters?

In the recent past, reactions of citizens towards privacy issues were not sufficiently considered. Yet, this is not a good reason to consider technology solutions and industry suppliers as a threat to citizens. The pendulum has now swung to the opposite side. Extreme considerations often result in the rejection of new technologies, when the better outcome would surely be better balanced.

Technology should not be unfairly perceived as a threat, and indeed can be of significant help against security threats. Yet this depends on the way it is used. Better training, correct behaviour of users and increased awareness of decision makers and the wider population are also needed. Legal frameworks should allow citizens and businesses to choose the level of information they accept to disclose without impairing the benefits technology can bring. Finally, pure law enforcement purposes should always benefit from the best technology can bring in terms of information gathering, provided that data collection is for the purpose of specific enquiries and duly mandated by democratically controlled authorities, which is, in principle, the case for European countries.

The Commission (DG ENTR) has realised the importance of the European Security Industry both for developing and producing high-level security solutions and services and for its role in the overall economy (direct and indirect jobs in Europe). The creation of a European Security Industrial Policy, even if still in its infancy, is a step towards a good direction to better support the competitiveness of our sector and contribute to providing better solutions to users and operators.

Another directorate of the Commission (DG HOME) should now take advantage of this industrial policy and consider the support from European security suppliers as a real asset in the implementation of its policies. This applies both to the quality of technologies available for preventing and mitigating internal and external security crises, and also for the close links our companies have with national / local administrations, along with the users and operators who have to implement and use these solutions. For years we have called for a stronger public – private dialogue and cooperation, not only at national level (where this is already happening in many sectors) but also at European level.

Attempts at cooperation between European Institutions and private bodies (Task Forces on some operational issues, like CBRNE; the NIS Platform on cybersecurity; the advisory groups on research priorities) are struggling to find consensus and their results are too often not sufficient to develop a comprehensive approach which could breathe life into a dynamic and harmonised EU security market, providing the needed competitive solutions that satisfy societal and operational needs.

Concrete examples of how technology can prevent and mitigate crisis are:

- in maritime surveillance: early identification and tracking of illegal goods smuggling; early identification of boats transporting irregular migrants, allowing a complete situational awareness of dangers and timely search & rescue operations (e.g. drones gained a misplaced generic reputation based on their use in Afghanistan, exacerbated by certain media. But they can also be used in entirely harmless ways that contribute significantly to saving lives)
- in smart borders: benefit in the smart border area should be obtained by the use of new mobile communication technologies and other biological identification means adapted to entry and exit scenarios at EU external borders for faster identification of bona fide travellers. Similarly they have applicability for random checks in the inner part of the European area, efficiently identifying irregular residents / overstayers.
- in cybersecurity: increased protection of citizens with respect to ID theft, child pornography, illegal internet content, viral and malware attacks, denial of services, protection of critical infrastructure and services of European and MS relevance (for which specific and ideally independent European solutions should be developed and implemented, supported by a true European cybersecurity industry)
- in protection of critical infrastructures: early identification of threats potentially causing disruption of services or harm to citizens (terrorist attacks, criminal events), via specific sensors for CBRNE, smart video-surveillance, intelligence and big data analysis, situation awareness for wide and populated environments / systems, etc.
- in crisis / disaster management: early identification of threats and situation awareness via imaging (e.g. satellite, drones), rapid reaction capabilities for search & rescue, advanced communication for crisis management and better decision making, training of population, better response tools for first responders, simulation for faster and adapted reaction, etc.
- in protection of citizens (specifically in urban environment): awareness, early warning and fast intervention tools can help law enforcement to prevent petty and large crime as well as vandalism in the urban environment; forensic tools and information sharing can help law enforcement to apprehend criminals and foster trust among citizens in the law and a liveable society. Urban critical infrastructure protection, command & control for intervention forces, and urban transportation security, to name just a few, can make valuable contributions to securing smart, sustainable and resilient cities and services for free, prosperous inhabitants.
- in threat reduction: the CBRNE threat can be reduced further by focussing on proactive measures as, for instance, improved EU regulations and guidelines on precursors for CBRNE. A further integration of detection technologies for fiscal goods and security substances will increase the chances that concrete threats are found in very early stages.

4) **Harmonised and focussed use of EU and MS funds for supporting capability development and capacity procurement are also instruments to promote a new dynamics to build a safe and open Europe.**

Public-Private cooperation is not only information exchange, as it is too often considered by public administrations, but also entails real operational measures and capacity building. Both parties are often reluctant to consider further steps, beyond dialogue, for public-private cooperation, as these would involve investments, both financial and operational. Without mutual trust and real and continuous dialogue between representatives from industry and public administration, it would be impossible to build sound and harmonised European security approaches. Competition will follow, but first it is fundamental to build a common comprehensive vision and a common programme.

A closer dialogue between representatives of private security suppliers and Member States is also urgently needed to identify common views for the development of future solutions adapted to national needs satisfying European policies. This would foster implementation of solutions and generate support for European programmes and harmonised procurement, thus allowing easier decision-making by the European Institutions. For that purpose, notwithstanding the prevalence of national sovereignty, the EU should also encourage MS to set-up specific procurement bodies for civil security. Such bodies could be organised at national levels or sectoral levels. Networking and cooperation with a view to elaborating common requirements and favouring economies of scale should also be promoted.

Thus, in the roadmap of such a common programme, we should set as key milestones the harmonised definition of operational needs, standards, adequate (in European coordination) risk assessment / management for each sector, security and privacy by design, specifications for system integration tools, solutions for harmonisation and interoperability between MS, certification procedures at European level, development of European capabilities and coordinated procurement of capacities (when possible). We think that one of the key objectives concerning security is the support to the future Programme for Home Affairs, which would result in a truly comprehensive approach.

The European Commission is funding research to develop capabilities to support the EU security policies. The positive outcome is evident in in the significant number of EU security policies in the main sectors. But there remains insufficient linkage between the developed technologies and the security European policies, in the frame of a sustainable (political, societal and economical) approach. Despite these many European security Policies, Security Research still lacks a clear strategy. Results are still reaching the implementation phase with great difficulty, and not only due to the often cited lack of defined needs by users. Stronger support to innovation closer to market (via pilots, demonstrations and large IPs in priority areas, such as border surveillance / EUROSUR, smart border initiative etc.) should be supported not only by H2020 funds but also the ISF (Internal Security Fund). ISF and structural funds should then be wisely used for coordinated or harmonised procurement of capabilities in Member States for Internal and external security as well as, when needed, in Third Countries for external security and CSDP missions. More transparency and / or early visibility of EU and MS investment strategies in security solutions would be needed to better plan industrial contributions and a sustainable market and job growth.