EUROPEAN ORGANISATION FOR SECURITY

To Commissioner J. KING
Commissioner for Security Union

Brussels, December 5th, 2016

Dear Commissioner King,

On behalf of Andrea Biraghi, Chairman of the Board of EOS and of all EOS Members, we would like to thank you for the opportunity of our upcoming meeting on December 12th to discuss issues related to the contribution of the European security industry to the build-up of a Security Union.

EOS, as a trade organisation, has been working in this field for almost 10 years, but the activity on security of our industry members has started well before. Since 2002 our companies have supported the setup of European research in the security domain and, individually and through EOS, have contributed to the definition of the main EU security policies and measures.

Europe is facing increasing security challenges with internal and external threats, in the physical and in the "virtual" world. These threats are endangering our society, our citizens and our economy.

The European 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 the main security sectors: 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); and Hybrid Threats (focus on civilian - dual issues). All these areas are tackled both from the Research & Innovation point of view as well as the different aspects of industrial security policy issues (e.g. standardisation, certification, investments, SMEs, training, etc.).

For ten years we have advocated the need for an overall approach on security for Europe, a better strategy, developed in Public-Private cooperation and more focused investments, not only for research but also for deployments and use, as proposed in our two Flagships on Integrated Border Management and Cybersecurity. We are also looking towards an increased level of European autonomy in certain strategic / sensitive areas.

We believe that with the Security Union policy, there will be the opportunity to implement our suggestions and reinforce the European vision of a Europe protecting its citizens, its society and its economic growth. Our industry is ready to support this!

In the attached memo, we introduce the themes that we would tackle in our discussion. We provide some positions, drawn from our experience, to the different topics of the EC Security Union Communication. We introduce also some topics which are not in the Communication but that we consider as important to be tackled in our discussion, including a renewed EU industrial security policy supported by concrete and rapid actions.

We look forward to meeting you next week.

Best Regards

Luigi Rebuffi
Chief Executive Officer
European Organisation for Security (EOS)

MEMO - EOS Meeting with Commissioner King

December 12th, 2016

WITH REFERENCE TO THE TOPICS OF THE EC COMMUNICATION ON THE SECURITY UNION OF 20/04/ 2016

1 Integrated Boarder Management / Migration

1.1 Missing a public – private dialogue / cooperation

We started discussing solutions on Border Control and Migration with Commissioner Frattini in 2005, during the creation phase of EOS. Certain of these elements have been at the basis of the creation of EUROSUR. After several years of discussion, the EUROSUR regulation has been approved, yet it is hardly applied (or known) in Member States (MS). This situation, unfortunately, does not help solve the interoperability issue, an important technology challenge that should not be tackled "a posteriori". Indeed, border control and migration is not only an issue for public administrations and enforcement bodies, but it needs an adequate technology 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 been reduced, and only limited bilateral discussions are now possible. We hope for an improved dialogue and cooperation with the new EBCG structure.

Regarding cooperation with DG HOME, the dialogue has been always very open and with good common understanding at a high level; however, it is rather sterile when it comes to operational issues. Limiting discussions to "fragmented R&I" (Research & Innovation) is not sufficient to assure interoperable, efficient and competitive solutions that are effectively implemented in the market.

A wider and coordinated dialogue / cooperation with the private sector, which has been requested for years, is now urgent if we want to provide adequate solutions.

1.2 A Public – Private Flagship for an Integrated Border Management

Following discussions with M. Ruete in mid-2014, we proposed at the end of 2015 to the EC the creation of an Integrated Border Management flagship (we have had a similar flagship approach for cybersecurity and this led to the creation of the cPPP and ECSO), declined in the following topics:

Three Challenges / Threats

- *Massive migration*
- *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 needed):*
  - *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 Investments objective

- *Increase and optimize use of budgets, harmonising R&I and procurement of EU certified solutions in a coordinated EU strategy, targeting €6 bln over the next 10 years*

This suggestion is today supported and proposed also by BUSINESSEUROPE, after an analysis of the impact on the European economy of a too weak and fragmented response to border challenges.

The Commission was initially interested in this approach, but no decision has been taken to move forward. In parallel, we have started a discussion with Ministers of Interiors (MoI) in MS to establish a dialogue and consider the possible implementation of such a programme, starting from key EU countries and main security companies.

1.3 A Public – Private Platform

We have seen that the typical PPP model on R&I adopted in other areas by the EC is hardly applicable in this sector, as the market is mainly driven by public administrations. A more specific EU instrument should be found for effective coordination of strategy, resources and funds assuring a constant and open public-private dialogue / cooperation with effective use and focus of funds for R&I as well as capacity investments.
A first effective step of the proposed flagship could be the creation of a Public – Private Platform. This could serve for an initial dialogue and could be set up immediately in a voluntary mode.

1.4 Smart Borders / Entry-Exit

The appropriate technology to address this issue already exists. Our members, world leaders in this domain, have successfully participated in EC pilots, and solutions are ready for deployment. Technologies in this domain could well contribute to reduce 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. We hope that the finalisation and agreement of the Smart Border package, expected under the Slovak Presidency and foreseen to take place during the Maltese Presidency, should rapidly be implemented.

2 Cybersecurity

2.1 Cybersecurity cPPP

The cybersecurity cPPP has been set up in record time, in part thanks to the extensive preparatory work and support from EOS (who runs the Secretariat). The cPPP is targeting R&I activities, as usual in the EC approach. A specific association, the European Cyber Security Organisation (ECSO), has been created not only to support the cPPP and the definition of R&I priorities, but also to foster effective cybersecurity industrial policies activities in public- public cooperation to increase security and competitiveness. A specific meeting on the cPPP and ECSO could be envisaged with Commissioner King, as this would require tackling wide, specific and quite complex issues.

2.2 Digital Autonomy

The cPPP is not directly tackling sensitive issues as cybercrime, intelligence, cyberdefence, digital autonomy and other related topics, but EOS has the capacity to cover these issues in its Cybersecurity Working Group (WG).

2.3 Encryption

A sensitive political and technical topic, the EU industry (within the EOS Cybersecurity WG) could work on a common technical / political paper to assess the issue and provide suggestions for a European position, considering national sovereignty issues.

2.4 Digital Intelligence

Digital Intelligence should come not only from a public-public dialogue, but also from a stronger link with the EU 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 origin, even if largely present in Europe: this raises questions on the influence of external strategies in EU positions.

Questions that could be tackled in this area are:

- How the competence at national level (sensitive) of EU industry can be of use at EU level?
- How to build a European information sharing system?
- What kind of EU digital autonomy is possible in this sector?
- Can we create a big-data at EU level for security use?
- Etc.

2.5 High Level Expert Group on Information Systems and Interoperability

In his speeches, the Counter-Terrorism Coordinator suggested to create stronger links with private sector experts, in order to optimise the use of technologies (data quality of the systems, automatic fingerprint identification systems, PNR systems, intelligence systems, security of data stored, high quality biometrics, systems interoperability - all terms taken by the report of the first HLEG meeting). Today, unfortunately, industry experts are excluded from this dialogue and cannot provide an important support (experts should come from EU companies).

3 Research & Innovation

3.1 EU financed security research

Future research could better target terrorism issues, but the approach should be different (top down) with a comprehensive strategy and implementation measures (which is difficult under H2020 secure societies) in order to secure an effective commitment from industry. The strong shift from FP7 to H2020 towards “societal issues”

has somehow led to neglect in R&I projects the competitiveness aspects, so important for our industry in this "sensitive market".

3.2 Technology Autonomy (not only digital autonomy)

The present EC research approach does not focus on technology autonomy for strategic sensitiveness, 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. A structured Public-Private cooperation 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 the leverage factor is not applicable to "public markets". Without R&I "carrot funds" or coordination of other implementation funds, there is little chance to set up a comprehensive and strategic approach involving the different kinds of stakeholders.

3.3 Detection technologies and their use

Information on existing solutions not stemming from EU research is too sensitive to be shared. EC research is often too academic and too slow. Discussions with EU Institutions are watered down by diverging (public and private) interests.

The recently announced EU Certification of Civil Aviation Security Equipment took four years to be proposed. EOS supports the goals that the Commission's Proposal for a Regulation aims to achieve, yet we would hope the Commission could consider the modification of certain aspects. EOS considers the current proposal to be 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 trials to adapt existing technologies could be immediately set up.

4 Hybrid Threats

Hybrid Threats should be seriously considered in External (and their impact on Internal) Security in a public - private dialogue. Approaches should better consider dual use solutions. 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.

OTHER TOPICS (NOT IN THE EC COMMUNICATION)

5 DRIVER project

DRIVER is a 34M€ project started in FP7, on crisis management. The project is today in stand-by due to several issues. About 20 M€ remain still to be spent (possibly re-starting in 2017) if agreement is found on updated objectives.
We are discussing the possibility to link some of these objectives to those of the Security Union (crisis management / "urban catastrophes", including terrorism).
Political support from Commissioner King could help this renewed approach and recover the project. This could also be the possibility for an immediate use of already assigned EC funds to achieve the "low hanging fruits" of the Security Union objectives.

6 Industrial Security Policy

In July 2008 we proposed to the EC the creation of an Industrial Security 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 (after 4 years of discussions) to present such an industrial policy (yet, with a limited scope with respect to our requests). 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 the European industry.

We continue to believe that a strong European security industry is possible only in a better structured and supported environment, and a renewed industrial security policy could provide this support. It should not be limited to Research and Innovation, but tackle all aspects in a comprehensive approach.

TOGETHER WITH THE CREATION OF A STRUCTURED PUBLIC – PRIVATE DIALOGUE / COOPERATION POSSIBLY AROUND A FLAGSHIP APPROACH FOR FOCUSSED INVESTMENTS, A RENEWED EU INDUSTRIAL SECURITY POLICY IS OUR MAIN MESSAGE FOR AN EFFECTIVE SUPPORT OF THE EUROPEAN INDUSTRY TO THE SECURITY UNION.

The different aspect of a renewed industrial security policy should tackle:

- Standards, Regulations / Legislation and Certification
- Technology autonomy; supply chain
- Investments: link between R&I funds and investment funds (EU, national, regional)
- Better link of industry with SMEs and Research / Universities
- Training, Awareness, Simulation
- Dual use / Hybrid Threats
- Comprehensive R&I strategy

7 High Level Public-Private Dialogue

At our last meeting with Mr. Gilles de Kerchove (we have maintained a regular exchange of views with him for over ten years), he suggested to set up a high level meeting (a dinner or similar) between high level EC managers (possibly in presence of President Juncker, Commissioner King and relevant DGs, with CEOs of EOS members) to identify what will be the future Security Union, agree on common steps and commitments and in future, track its implementation.