Position Paper

On the Future Program for Home Affairs

January 2014

Motivation of the paper

The present paper constitutes the response of Indra to the open Public Consultation by the DG HOME:

(http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2013/consulting_0027_en.htm).

Indra is a global consulting, technology, innovation and talent company. It is on the cutting edge of high value-added solutions and services for the Security and Defence, Transport and Traffic, Energy and Industry, Public Administration and Healthcare, Financial Services, and Telecom and Media sectors. Indra operates in more than 128 countries and has more than 42,000 employees worldwide.

Indra is one of the top European companies in its sector in terms of R&D&i, with more than €500 million invested in the last three years.

Indra is second-to-none in the design, deployment and integration of complex systems in the security sector, notably for critical infrastructure protection, border surveillance and automated control, and emergency & crisis management. Most recently, Indra has developed an ambitious R&D programme on cybersecurity as a strategic step for the company for the next years, with the aim to offer the highest quality in a fully competitive model, considering innovation as the added value. For this purpose, Indra has set up a Cybersecurity Operations Centre for the delivery of specialized services to protect critical infrastructures, cope with cybercrime and secure identity and individual privacy.

According to the high level of specialisation and references that Indra is able to offer in the security field, the contribution included in this paper is focusing on:

1. the suggested role of industry in the way to a safer, secure and prosperous EU, and

2. the technology challenges that the EU is currently facing in the area of maritime surveillance and cyber security, within the framework of the set of threats that lie at the origin of these challenges.

The role of industry in the program of Home Affairs

As it is clearly recognised by the European Commission in its document *COM(2012) 417 final* ***Action Plan for an innovative and competitive Security Industry:*** *"Security is unmistakably one of the central concerns of any society. A safe and secure environment is the very basis on which any stable society is founded upon. Citizens need to be free of security related preoccupations if they want to live their lives freely and contribute to the well being of our society"***.**

Security, as a characteristic and fundamental asset of the European society, needs to be continuously fostered and upgraded. To this purpose, the roadmap articulating the future Program of Home Affairs must necessarily include the resources required to continue to implement and develop effective systems that contribute to protect the citizens, combat law offenders, and save lives.

Accordingly, the role of industry is called to be central in the achievement of the following proposed objectives for the Program:

- ➔ developing, procuring and implementing **innovative solutions to cope with existing and evolving threats.** This first objective is naturally recognised as conforming the major expected role of industry in the security arena. The existing threats in the

particular domains of maritime and cyber security, and how technology can respond to those are described in the point below in this paper.

➔ **boosting the security markets and promoting new standards** along the whole chain of value, from research to procurement, in order to keep Europe at the global forefront of the sector. The Commission has recently addressed the development of a new standards through their agencies in a number of specialised areas (namely CBRNE, Border security and crisis management). Being a task of major relevance and impact, the effort is to be extended and reinforced to other security domains, such as the maritime environment. Not only the result of these processes are key to overcome the actual fragmentation of the security market. In this sense it is also important to remark that to be in the necessity to adopt a set of standards developed elsewhere would seriously limit the competitiveness of European industries in the global market for the sector concerned.

➔ **To lead the implementation of an EU model of public and private partnerships**, aiming to leveraging more effective use of funding instruments, and fostering a more competitive industry in the global market.

In the last years it has been sufficiently highlighted that the new policies on security need to contribute more efficiently to save the gap between research and procurement, to strengthen the link between the developed technologies and the European security policies, and to achieve a clear strategy for Security Research.

These goals will not be achieved by the mere introduction of new procurement tools and processes. A more substantial evolution of the policy decision chain is essential. The industry aims not to be considered only as a passive market player providing technology solutions and services, but as a pro-active partner able to create value for money. A cross public-private cooperation would foster a convergence of interests. It should be the result of a commonly defined strategy, focussing on the return of investment for each stakeholder, and the set up of a sustainable market for the medium and long term.

This analysis yields to the conclusion that a stronger dialogue between private security suppliers and public stakeholders from Member States involved in security policies is to be encouraged and facilitated by European responsible bodies such as DG Home Affairs. In this sense, the experience obtained from the projects and initiatives already adopted by the Commission in this direction (not only in the security sector); namely those implementing new forms of public-private partnerships, wherein the industry is playing a leading role, could be relevant lessons learnt for the roadmap under discussion here.

➔ **improved levels of acceptance** of security technologies by the civil society. Regarding this objective, it is frequently forgotten the obvious observation that the standards of safety and security and protection of fundamental rights achieved in Europe cannot be understood without the economic and technological resources needed for those to be maintained. Unfortunately sometimes the security technologies have been understood, as seen from some angles and perspectives, as a set of invasive tools contributing to undermine the principles of privacy, freedom and human rights. On the contrary, over the last years several systems have been implemented at European level that have contributed paradigmatically to the protection of those principles. For the latter systems, the industry has been a key enabler. The dissemination strategy containing the actions required to reinforce the awareness of this fact within society is not to be underestimated in the future Program of DG Home Affairs.

Major Threats and Technology Challenges

1. Maritime Surveillance

Although the main threats in maritime security have been identified for a long time, the specific manner in which these threats are accomplished have substantially evolved in recent years. In particular, at this moment there exists a vast experience in operating integrated surveillance systems in the maritime area, such as the one at Gibraltar strait (SIVE). However the mafias and offenders in general have changed their strategies (for example, departing in large mother-ships from further ports), so producing gaps in current solutions. The following threats have been identified, to still pose challenges to a surveillance system for the next future.

(T1) Irregular Migration

(T2) Drug Trafficking

(T3) Illegal Fishing

(*T4) Pollution impact on coastal environment*

(*T5) Fight against Mafia networks*

(*T6) Terrorism*

(*T7) Accidents at sea and natural disasters*

(*T8) Piracy*

(*T9) Criminal acts against critical facilities/infrastructure*

The set of threats above imply first of all a number of technological challenges that are mainly related to the surveillance technologies available. In some cases these exist but are not yet standardised as European solutions, or are restricted to particular conditions, or simply are too costly to be considered as a feasible response to the extension or nature of the threat. In some other cases, the technology is exploited to the edge of its performance and the threat opportunity comes mainly from this technical limitation. However, it is important to mention that in some cases the technical challenge arrives from the know how and conditions required to implement existing best practices and techniques, which are already available in the market and in other areas of operation.

Below follows a description of the technical challenges in maritime surveillance and the security threats most directly associated to each.

- **Detection of small targets:** Detecting small craft in vast areas as well as in closed waters of archipelagos. These comprise mainly pateras (Wooden, rubber or fibre vessel from 5 to 7 meters long, about 2 meters wide); cayucos (wooden or fibre vessel from 6 to 15 meters long, from 2 to 5 meters wide) and rubber boats (rubber/fibre vessel, from 5 to 8 meters long, about 2 meters wide); and more recently, other kind of smaller vehicles such as water bikes. As a most extreme example observed in the later times, the use of inflatable tyres at open seas as the only floating device has reduced the radar echo of the target to nearly that of the human body on the water. This challenge is already well recognised by the European Commission (see ref. COM(2011) 873 final *Establishing the European Border Surveillance System (EUROSUR*)). Related threats are T1, T2, T3, T5, T6 and T8

➔ **Detection of Low flying aircraft:** Small aircraft flying at low altitude are not detected by wide area air surveillance radars (typically operated by the air force), and neither by coastal radars optimised for sea surface monitoring. It comprises typically CESSNA 152 or Ultra light type airplane; and twin engines type airplane. Related threats are T1, T2, T3 and T5

➔ **Routine, secured and innovative uses of aircraft for monitoring and surveillance efforts:** while it is foreseen that Unmanned Aerial Systems (UAS) will have a major impact on the surveillance of remote areas, it is necessary to extend the portfolio of piloted light surveillance platforms with a reduced operational cost. In this way the surveillance time will be increased in high seas. This type of platforms shall effectively cover surveillance gaps in a short period of time avoiding legislative constrains.

On their side, the using of UAS would increase dramatically the surveillance capability of the maritime border surveillance forces using on board deployable sensors for prevention and detection of real menaces for the community. To unlock this true potential of the UAS, stakeholders need to break a series of entangled challenges. Today, in the absence of UAS regulations, the development of solutions is risky and expensive for industry, and essentially aimed at military applications.

This challenge relates to all threats.

➔ **Fusion of data and generation of relevant Information and regional/transnational situational picture:** It relates to the fusion of information coming from different and/or heterogeneous sources (satellite, in-situ, models, etc.) and establishment of a common situational picture across Member States; integration of information coming from real time national situational pictures and intelligence sources, building pre-border situational pictures, and integration of information from open sources. Not only does data fusion have a great importance to identify and fuse tracks from different acquisition resources, but also it is vital to use the available technology to envision future undesired actions or manoeuvres from the current scenario.

This challenge relates to all threats.

➔ **Analysis and presentation of the information:** development of tools for decision support, so as to enable and facilitate the corresponding risk assessment and the impact evaluation of measures to be taken in a specific critical scenario.

Presentation of the presentation of the information relates to measures to present the maritime situational pictures and the different layers of supporting information in order to:

- detect abnormal vessel behaviours
- continuously track suspicious vessels
- progressively understanding and identification of threats and extraction of risk analysis from the surveillance data,
- provide operators and decision makers with decision support tools on multi touch, multi user and intuitive interfaces

This challenge relates to all threats.

➔ **Interoperability:** There is also a need to secure and make more robust communication platforms, supporting seamless connectivity, communication and interoperability, defined in a secure way, with relevant APIs for enabling the connection between the data collection tools and the communication platform as well as the connection between front end sensors, devices and control elements to the fusion system. This approach

will facilitate the efficient and transparent transfer of data and information between the various system entities and layers. Related threats are T1, T6, T7, T8

➔ **Detect, track and identify oil spills, and other polluting substances:** Due to the growing concerns about the future health of our oceans (as well as the associated risks to the human health), and the sustainability of marine resources, new tools for effective decision taking are needed, according to the results of real-time monitoring status of marine water quality, including prediction models and the provision of early warning systems. Real-time in situ detection and spill monitoring of marine chemical contaminants (oil pollutants, algal toxins, etc) should be used for immediate reaction. Existing and different platforms and sensors, technologies and capabilities, new and existing ones, such as wave and tide gauges, radar based solutions, UAVs, OPVs, satellite SAR images and other surveillance technologies must be combined in a more efficient way in order to be able to widely deploy pollution monitoring systems. Particularly to reduce the risk of potential accidents in port areas, all these improvements can be applied also to the development of more efficient and coordinated monitoring systems for ships carrying dangerous goods (HAZMAT). Related threats are T4 and T7.

➔ **Prevention protocols associated to disasters (e.g. human, natural, etc.):** Forecast and early awareness systems are a critical area of development for Maritime Surveillance. Even if useful technologies are already available for the related capabilities, the maritime environment poses specific challenges in terms of coverage, communications and maintenance.

Regarding natural phenomena, it's worth mentioning the flood prevention and resiliency management to minimize negative impacts on port infrastructures, vessel traffic conditions and their impact in quality of water. Forecasting and preventing flood and draught impact will be considered on the prevention protocols.

Related threat is T7

➔ **Maritime communications:** Provision and/or improvement of:

- Long range communications between ships, aircrafts or coast control centres by using maritime frequencies (VHF, HF), broadband radio or SATCOM communications.
- Wideband inter-communication infrastructure for a fleet of ships.
- Opportunistic wideband communications of maritime platforms when approaching coast.
- Ship data-links to enable communication with aircrafts (UAVs, OPVs, helicopters, etc).
- Inner wideband communications coverage for ship deck.
- Integrated sensors on different surveillance platforms (aircrafts, ships and ground vehicles/places) able to communicate their detected data to the corresponding control centre and/or relevant stakeholders.

This technical challenge relates to all threats.

➔ **Critical Infrastructure Protection:** It consists of the protection plan for ports areas and off-shore infrastructures in case of emergency situations, intentional damage, sabotage, natural phenomena, burglary or terrorism.

Given the complexity and extension of some of the particular infrastructures, the nature of the materials stored (e.g. oil/gas terminals and repositories), and the amount of daily traffic, effective methodologies of risk analysis are required. For the threats mentioned above (see T9) the risk analysis should provide impact quantification in terms of port operation, reparation of the damage, social or psychological impact, extension or amplitude of the impact, probability of occurrence, and probability of damage after the occurrence. The appropriate methodologies should be capable of being dynamically updated according to the information provided by port surveillance systems in a continuous basis, and at the same time be able to tailor these systems to the updated outcomes from the risk evaluation.

Regarding off-shore infrastructures, it is essentially a plan to protect wind farms, oceanographic platforms, employees and any kind of off-shore energy production system. It will also cover all measures adopted to avoid blocks of operations and includes measures as response against security violations.

Another aspect that should be addressed is the observation of critical maritime infrastructures based on surveillance systems for the ultimate security covering ports, passenger transport and energy supply to avoid them being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour.

This challenge relates to all threats.

2. Cyber security

In the 90s computer attacks were mere anecdotes of people seeking notoriety creating annoying virus without any benefit. In the past decade, the cybercrime made his way through complex programs in order to steal large sums of money. In the last years we have experienced attacks on different critical infrastructures as nuclear power plant control systems, or government organizations. We have gone from computing vandalism two decades ago to Cybercrime and everything suggests that in the coming years we must prepare our infrastructure against cyber terrorism and cyber war. Digital control systems are a critical component of the energy plants. Nowadays, users need to increase the availability of process data and thereby to define Facing Digital Threats connections to the processing network. The technology used is changing and the design of the plant evolves from isolated proprietary systems, to systems based on open technologies of common use and well documented in Internet as well as to an increased system integration. This situation has produced the emergence of new risks.

The number of incidents has grown, which have been committed not by mere individuals seeking notoriety and personal satisfaction but by organized groups that have big budgets and even interests in governments of some countries. Cyber security is not an just a technical issue. It requires engaging the organization and the definition of new activities and responsibilities.

To achieve an acceptable level of cyber security in an organization, it is required to have knowledge and experience on Industrial Control Systems and Security for traditional Information Systems. IT security processes cannot be exported directly to control systems processes. Neither safety requirements are the same nor is security technology applicable.

Below follows a description of the technical challenges in cyber security:

- ➔ **Protection of ICT Infrastructures**
  a. Plans and solutions for Critical Infrastructure Protection.
  b. Business Continuity.
  c. Secure Control of Business Processes
  d. Vulnerability analysis using static and dynamic techniques

- ➔ **Identity assurance**

a. Identity and biometric systems. Identity management and authentication.
b. Electronic signature, digital certification and corporate PKI.
c. Generation and validation of secure identity documents.

➔ **Information Assurance**
a. Secure data storage, both in short-term and long term documents.
b. Data, files and repositories encryption.
c. Data integrity and resilience
d. DLP / DRM

➔ **Secure Activity**
a. Signature generation and verification platforms.
b. Research and Intelligence. Data mining and trends.
c. Forensic analysis.

➔ **Security governance models and risk management**
a. Adaptation to current legislation.
b. Norms and standards compliance.
c. Security incident and event management.