EOS
EUROPEAN ORGANISATION FOR SECURITY

Attachment to the letter to the President of the European Council,
Mr Van Rompuy and the President of the European Commission, Mr Barroso

Maritime Surveillance / Security

Maritime security issues are not only concentrated in the South Mediterranean but can be found in all seas, from the North and the Artic seas, to the Indian Ocean, for the protection of significant European economic interest in those areas. Indeed, maritime security strongly links civilian and military aspects as well as public and private needs and resources.

What happened recently at large of Lampedusa is just an example of the urgency of providing more and better tools for early detection and identification of critical situations and immediate response at sea. Effective implementation of EUROSUR, more resources at EU level managed by Frontex, for instance in the frame of a EU Coast Guard Force, better coordination of civilian and military efforts, are only some of the possible measures to be taken.

EOS and its members strongly supported the EUROSUR Programme from the beginning. However, to reach the needed level of collaboration between all Member States and implement the EUROSUR programme efficiently with the deployment of specific capabilities, we believe that a continuous and extended dialogue and cooperation between public-private stakeholders at national and European level would greatly benefit the whole European security and economy.

Specific capabilities based upon innovative technologies can be used for:

- Migration surveillance and emergency response (including search & rescue)
- Enhanced surveillance capabilities (RPAS, Space, etc.)
- Crisis management
- Fight against crime (smuggling, trafficking, illegal fishing, etc.)
- Piracy

The European industry is particularly active in the maritime security sector, and members of EOS have already shown, via projects funded under the 7th Framework Programme for Research and Development like PERSEUS, I2C and SEABILLA, the effectiveness of many innovative technologies and capabilities needed for European-wide maritime surveillance systems to overcome major gaps at National and European operational levels. These successful projects show that the European security industry, working with various research organisations, has much to offer in terms of cutting edge technology / services and providing EU decision makers with concrete, flexible and cost-efficient solutions worth investing in. We should now put these results and solutions into operation.

Research and deployment should be considered in the context of a global strategy, wider than EUROSUR, tackling all the issues of the maritime area, in order to allow EU industry to better envisage investment and increase its competitiveness.

Parallel to EUROSUR, the European Commission has set guiding principles on how to achieve integration of a wider maritime surveillance and awareness with the creation of a Common Information Sharing Environment (CISE) to increase and facilitate services and the exchange of data in all maritime sectors. We think that the CISE should be extended to a more sustainable model of data-sharing across sectors (public and private), operating in maritime environment with the appropriate level of confidentiality. If supported by adequate European policies and common standards, this will then provide a long term strategy to foster security, prevention of loss of lives at sea, as well as economic growth and environmental protection in the Mediterranean.

To support the development, validation and procurement of the needed capabilities for maritime surveillance / security and in view of the December European Council, we would suggest:

- *The establishment of a closer Public – Private dialogue with the EU and MS public administrations, leveraging upon the conclusions of the December Council and in particular building upon the work of the next two EU Presidencies, the Greek and the Italian, so sensitive to issues related to maritime security, to harmonise requirements for a faster implementation of technical security solutions at sea, also in the light of the European Maritime Security Strategy currently under development by the EU Institutions.*
- *To allocate specific European funds and financial incentives to set up operational services, also with the support of the industry, which may be coordinated by European Agencies in case of emergencies, while respecting sovereignty issues of each Member State involved.*
- *The creation of a specific programme, in Public – Private cooperation, to deal with maritime surveillance / security (and in particular to support the deployment of EUROSUR and build up the CISE, seen as a way to create a "Single Sea") for the development, validation, procurement and use (end – to end approach) of innovative technical / services solutions. In particular, the continuation in H2020 of pilots and large demonstration projects is important to keep consistency of the developed approaches and consolidation of investments and efforts.*

Cybersecurity / defence, protection of data and infrastructure

The security of networks, of communication and information systems and in general, the protection against the threats to infrastructures relying on ICT (Information and Communication Technologies) have become a vital issue at global level, not only considering the extension of cybercrime, which today is estimated to be wider than drug smuggling, not only with respect to the attacks on citizens' privacy, but also for guaranteeing stability of our societies and the protection of our economy and national security. The recent PRISM revelations show that an appropriate level of security and privacy is needed.

Many European industries are working with national Member State administrations to build a safer cyberspace in line with the most important European principles of justice and freedom, within trusted partnerships. Yet, more remains to be done to foster European competitiveness in this area.

The European Institutions are working on the implementation of the EU cybersecurity strategy and a project of NIS Directive. The effective growth of a competitive European industry could be one of the means of ensuring a better control of data and the protection of critical infrastructure.

To support the development and implementation of the necessary cybersecurity capabilities and looking ahead to the December European Council we would suggest:

- *To elaborate in a public / private dialogue concrete actions for stronger synergies between security solutions for cybersecurity in the civilian and military domains, define harmonised requirements for the development of capabilities in H2020, while envisaging detailed objectives and a Roadmap (ways and means) for their implementation.*
- *To create a Cybersecurity Industrial Policy with concrete measures to stimulate the EU market and support the development of a competitive European cybersecurity industry which could leverage upon competence and trusted relationship developed at national level.*
- *To create a Public-Private European Initiative on cybersecurity (beyond the present NIS Platform, which is providing an initial dialogue) to gather all the main European actors in the domain, to focus resources on concrete actions, also with the support of EU funds for capability deployment (e.g. structural funds), starting for instance from the protection of infrastructure and services of critical European relevance (e.g. electricity and transport networks, Galileo, Single Sky, a possible future European Cloud, etc.).*

Security Industrial Policy

Considering the relevant sovereignty and economic interests linked to its security, Europe should be able, when relevant, to develop its own solutions, adapted to its environment. Only public – private cooperation could efficiently gather all the needs and competences and develop a competitive European Security Technology and Industrial Base, essential to Europe in achieving its strategic objectives.

Results from the European Security Industry Policy launched in 2012 are still not sufficiently visible and certain priorities could be reviewed, not only in the light of users' needs. A closer dialogue with the European supply industry could better precise which are the most urgent areas and topics that an industrial policy for this sector should support to increase industrial competitiveness and the EU economy as a whole.

A structured public-private dialogue could also tackle the delicate interface between technologies which could be of dual use, better exploring priorities and exploiting, if possible, synergies.
EOS's remit is to consider only technologies for civilian security applications, yet, the borderline between internal and external security is blurring and the European security industry is concerned by the use of certain security technologies and services in the civilian and military world for joint or specific operations (e.g. Maritime Surveillance; Border Security; Cybersecurity; Crisis / Disaster Management - including CBRNE and RPAS) as envisaged by different European policies (e.g. Internal Security Strategy, cybersecurity strategy, border control / EUROSUR, CSDP etc.).

Considering these issues, to support the development a competitive European Security Industry and in view of the December European Council, we would suggest:

- *To review the European Security Strategies, considering the long standing threats and the new threats (internal and external) in order to identify detailed actions / objectives of this strategy and harmonised capability requirements.*
- *To review and update effective actions for the Security Industrial Policy of this sector to support and increase the competitiveness of the EU security industry, especially through the following key themes:*
    - *harmonisation of requirements and consolidation of demand in a public – private dialogue;*
    - *standardisation and interoperability; mutual recognition at international level of security procedures;*
    - *strategy-driven Research & Development (not limited to low TRLs – Technology Readiness Levels - but also targeting operational issues: pilots & trials);*
    - *harmonised testing and validation towards an EU-wide certification system acting as a European Quality Mark for Security, thus driving research results and innovation to the market;*
    - *support to the development of the full supply cycle, including legal and societal issues, training, support to SMEs etc, for a larger technology independence of Europe in critical areas;*
    - *focus resources into main programmes / platforms (in Public – Private Cooperation), that help supporting the implementation of European and National Security Strategies and the competitiveness of the European security industry;*
    - *use of EU funds and financial incentives for coordinated development and procurement of needed capabilities using European solutions.*
- *To analyse, via a structured Public – Private dialogue, possible synergies and needs in the development and use of technologies and services which could be used in civilian and military capabilities, without entering in defence related issues, providing EU Institutions and Member States with industrial views and priorities (economic and technical constraints) for more informed decisions.*