Public Consultation on the preparation of a new Communication on an Industrial Policy for the Security Industry

Objective

The Commission intends to adopt a Communication on an Industrial Policy for the Security Industry in 2012.

Definition of security industry:
Security industry encompasses traditional security industry (based around the supply of general security applications such as e.g. physical access control), security-orientated defence industry (based on the utilisation of defence technologies in security applications or through acquisition and conversion of civilian technologies to security applications), as well as new entrants, i.e. mainly companies extending their existing (civilian) technologies to security applications, such as for example IT companies.[1][2][3]

Our society has become very dependent on our technologies and infrastructures, be it our electricity network, the internet, public transport, aviation, telecommunications etc. Man made accidents or natural disasters may easily disrupt basic economic infrastructures such as transport; energy and information networks. Moreover, they can cause major direct damage to human beings and the environment if they affect particular sensitive components of the industrial infrastructure such as chemical or power plants.

This dependency is being exploited by terrorists and organised crime. It is, therefore, not surprising that the fight against terrorists and organised crime have gained importance in our daily life.

As our society becomes more and more dependent on technical systems, new more resilient architectures are needed for the infrastructures we depend upon in our daily life. In other words, even though technology cannot guarantee security, there is no security without technology. With this understanding, we need a solid, competitive technological base for the EU security industry that is benchmarked against meeting the societal security needs.

The security sector has however never been the subject of an industrial policy initiative. The necessity to remediate to this void has been emphasized by the Communication of the European Commission: *"An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage"*[4], of which the EU security industry is an essential part.

*"The EU **security industry** faces a highly fragmented internal market and a weak industrial base. National regulatory frameworks differ widely and the market for security products is highly diversified, ranging from cameras to complex scanner systems. To provide a security system, manufacturers, system integrators, and service providers have to work closely together with clients. It is essential to develop a fast-track system for approval of priority*

[1] See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0691:FIN:EN:PDF

[2] It is worth noting that specific segment analysis have also considered the role and impact of security services when relevant, for instance, in the case of security service providers for the air transport security sector, as they are the main operators of screening and security equipment.

[3] Space and Defence products/services are excluded from this questionnaire.

[4] See: (COM(2010) 614 final)

technologies; to make substantial further progress on harmonisation, standardisation; to consider coordinated public procurement; and to accelerate research on security technologies including dual-use. On the latter the Commission will coordinate with the European Defence Agency."

Another major particularity compared to other industrial activities is the societal dimension of security emphasized by the Communication[5]: "all security solutions must be founded on the European values of freedom and justice and fundamental ethical principles and legal requirements mainstreamed through all security R&D and innovation activities."

This Communication will address the main hurdles the EU security industry is facing today and make recommendations on the appropriate policy measures to overcome those hurdles.

Problem Definition

The European Commission has identified three main problems that could require action, namely; the fragmentation of the EU security markets, the fragile industrial base and the adequate integration of societal aspects in security technologies.

The central challenge the European security industry faces today is the **highly fragmented nature of its markets**. Security is a highly sensitive area for national states and has therefore been mostly dealt with on a national level. This lead subsequently to a lack of harmonisation on security matters (inadequately defined regulations on security, no EU wide legal framework, lack of EU wide standards on security technologies etc.) on the EU level.

This, in turn, led the security industry to be nationally or even regionally oriented. Only a limited number of large companies are able to compete on a European level, small and medium enterprises, in most cases, do not have the necessary means to address markets other than their own national markets. Not only does this weaken the competition, it also leads to inefficiency and poor cost-effectiveness both for the industry and the end users.

This situation also weakens considerably the competition of the EU security in the world. This is especially true with regard to the US competitors, who have a large and harmonised internal market and an advantageous regulatory framework (i.e. US safety act)[6]. It is essential for the EU security in general and its industry in particular to be able to produce competitive and efficient in-house technologies and to have access to key third country markets.

This situation has a direct effect on the **EU security industrial base.** Even if a throughout mapping of the EU security industry has yet to be achieved, first indications clearly show that whilst there are some European champions at the system integrator level (these are large companies integrating technologies provided by smaller companies), the security industrial base seems quite fragile at the second and third tier level[7]. The financial stability of many SME's is endangered by the reduced access to markets and the lack of a harmonised EU regulatory framework. At the same time, a strong and industrial base is a prerequisite for a European security market.

Furthermore, the possibility of synergies between civil and defence technologies remain largely untapped. This is truer today than ever before, where certain technologies (e.g.

[5] See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0691:FIN:EN:PDF

[6] See: https://www.safetyact.gov/

[7] That is companies either providing Technologies to system integrators or providing themselves the market as specialized/niche equipment providers.

electronics, telecommunications, surveillance, intelligence) developed by the defence sector could also be of relevance for internal security and vice versa ("dual use").

An additional particularity of the EU security industry is **the societal/ethical dimension of security**. While security is one of the most essential human needs, it also is a highly sensitive area. Security measures and technologies often suscitate the fear of a possible endangerment of privacy. Any attempt to introduce a security solution that could violate ethical values would lead to fierce societal reaction. It is therefore necessary to fully respect the European values for security when it comes to improving the competitiveness of the European security industry.

Reference to the questions

Relevant policy areas to address the fragmentation of the EU security market;

- Many aspects of the EU security industry are still unclear today. No overview assessment of the regulatory framework identifying areas where the EU faces either a lack of harmonisation or where "over"-harmonisation exists. Whilst in some areas a large body of EU law exists (e.g. aviation security), in other areas there would seem to exist gaps which have lead to a variety of differing national requirements (e.g. port security). As regards **certification/conformity assessment procedures,** the creation of an internal market for security is hindered by the fact that no EU wide certification system for security technologies exists. Additionally, the national systems are differing widely from each other. => *Question 2.1.1 to 2.2.3, and 2.3 to 2.6.*

- Finally, there exist only a limited number of EU wide **standards**[8] in the security area. The absence of EU wide standards would seem to contribute to the fragmentation of the security market. => *Question 2.2.1. to 2.2.2.*

Relevant policy areas to address the fragile industrial base of the EU security industry;

- As regards **pre-commercial procurement**, pilot activities have already started in FP7. The Commission has also laid out its general policy on pre-commercial procurement, notably in the Innovation Union Communication[9]. However, these general policy guidelines and pilot activities still need to be translated into consolidated pre-commercial procurement schemes. Issues that need to be addressed concern: modalities to avoid a restriction of competition, modalities for IPR sharing, etc. => *Question 3.2.*

- Concerning **public procurement**, the existing Defence Procurement Directive[10] also covers security sensitive procurement, thus contributing to the establishment of a truly European Security Equipment Market, where European suppliers can operate freely in all Member States. The aim of this question is to gather additional information on the interest of security customers, regarding the possible pooling of investment resources. => *Question 3.3.*

[8] Standards as defined in Directive 98/34/EC which reads: "a technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory".

[9] COM(2007) 799 final, COM(2010) 546 final.

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:216:0076:0136:EN:PDF

- There have been numerous calls by the European Council[11] to further foster **synergies between security and defence technologies**. The European Commission and the European Defence Agency (EDA) have already started to cooperate in this field in the context of the European Framework Cooperation (EFC). This cooperation is focused on creating synergies between the civil security research of FP7 and the EDA's defence research activities. However, there is no systematic cooperation more upstream at the level of capability development. Therefore, research cooperation remains difficult, as long as there is not a more fundamental understanding between Interior Ministries and Defence Ministries in Europe about required capabilities in the years to come. Furthermore, such synergies appear to be hampered by the fact that more downstream the outcome of research projects is not used to undertake coordination at the level of standards. Such coordination would seem to be extremely useful and cost-effective in certain areas (such as for example UAS). => *Question 3.4*

- **Market access** is already an issue with regard to the US and in potentially important markets such as China, also. The Commission has already indicated[12] that it will produce from 2011 onwards an annual trade and investment barriers report for the Spring European Council as its key instrument to monitor trade barriers and protectionist measures and trigger appropriate enforcement action. => *Question 3.5.*

- An issue which is often raised concerns **Third Party Liability limitation** that is provided to US producers through the US Safety Act[13], whereby the liability of a producer of security technologies is being limited in case of a terrorist incident. This would seem to provide US manufacturers with a clear competitive advantage with the US Safety Act being clearly aimed at encouraging the development and deployment of new and innovative anti-terrorism technologies. => *Question 3.6. and 3.7.*

Relevant policy areas to address the societal/ethical aspects of security;

- Security is a sensitive field. It is crucial to ensure strict adherence to ethical standards and to ensure the societal acceptance of new security measures and/or technologies. Especially issues related to privacy and data protection are of outmost importance and need to be assessed carefully. Any security concept is only as good as its applicability. It would, therefore, seem crucial to take into account the ethical/societal dimension of security in an industrial policy for the security sector. The possible creation of EU **certification schemes (e.g. ‘privacy seals’)** for **'privacy-compliant'** processes, technologies, products and services could be envisaged[14][15] This could facilitate the acceptance of new security technologies in the EU and its citizens. => *Question 4.1.1 to 4.4.*

[11] See: http://www.ess-project.eu/news/83-the-european-council-insists-on-development-of-civil-military-synergies.html

[12] COM(2010) 612 final

[13] https://www.safetyact.gov/

[14] See: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[15] Examples for this privacy compliant processes are: "the right to be forgotten", "the principle of data minimisation", "privacy by design", etc.