Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee — Security industrial policy — Action plan for an innovative and competitive security industry'

COM(2012) 417 final

(2013/C 76/07)

Rapporteur: **Mr PEZZINI**

On 26 July 2012, the Commission decided to consult the European Economic and Social Committee, under Article 304 of the Treaty on the Functioning of the European Union, on the

Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee – Security industrial policy – Action plan for an innovative and competitive security industry

COM(2012) 417 final.

The Section for the Single Market, Production and Consumption, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 8 January 2013.

At its 486th plenary session, held on 16 and 17 January 2013 (meeting of 16 January), the European Economic and Social Committee adopted the following opinion by 128 votes to 2 with 5 abstentions.

1. Conclusions and recommendations

1.1 The Committee considers it essential to have an integrated European policy for the security industry, underpinned by a coordinated approach to tackling the challenges of the industry, a common strategy and a shared vision of its competitive development, in a unified European market.

1.2 In order to competitively reinvigorate the security industry (understood as the traditional security industry and the security-orientated defence industry, as well as new entrants, i.e. mainly companies extending their existing civilian technologies to security applications and security service providers) with its vast and promising pool of employment and users, the EESC considers it vital to develop:

- **an internal dimension of full single market interoperability**: supporting, with a legal, technical, regulatory and procedural framework, an adequate level of dedicated resources, a unified development strategy and substantial investment in research and innovation;
- **priority actions per type of product** and service on the grounds of their ability to comply with harmonised rules and procedures;
- **the dimension of reliable access to international markets**, with enhanced international protection of industrial property rights (IPR), liberalisation of both commercial and public procurement markets, and an integrated industrial policy strategy;
- **equal access to maritime routes** for all European manufacturers to export their products to international markets;
- **integrated and joint actions across the various sectors of security and civil protection;**
- **the societal and ethical dimension of security-related technological applications**, right from the design phase, to ensure their **societal acceptance**, with full protection of the privacy of citizens; and
- **the training and professional dimension of human resources**, focusing on the design, installation, maintenance and operation of security technology applications, which should be centred around respect for human dignity and freedom and the right to have one's dignity safeguarded.

1.3 While the EESC endorses the initiatives in the action plan, it would like to see these underpinned by stronger cooperation and coordination, centred, inter alia, around product types, on the basis of relevant, detailed statistics, looking at the sector's companies in terms, not least, of their production, workforce and size.

1.4 The EESC recommends coordination and convergence of information management systems, and guarantees of interoperability.

1.5 The EESC strongly advocates bolstering the scope for managing and anticipating new competition scenarios and the prospects for accessing institutional financial resources, including through participatory foresight exercises at EU level.

1.6 The **societal and ethical dimension** must be interlinked in a transparent way and guaranteed at all phases, from design to standardisation and technological application on the ground. New technologies and rules should incorporate, from the outset, protection of the fundamental rights of citizens, especially regarding privacy and personal data protection.

1.7 An EU-level effort is needed, as well as the coordination of national efforts, to ensure training and support for human resources, so as to ensure the delivery of quality professional services, respectful of the individual and in step with the application of advanced technologies within a fully interoperable system.

2. **Introduction**

2.1 The security industry is a strategic sector with civil and military applications which are closely related and interlinked. It constitutes an ideal meeting point for scientific research, technological innovation and advanced applications.

2.2 This industry is inherently technology driven, with a constant influx of new technologies. Products and services in this sector are diverse, have high rates of obsolescence and require a high technical and scientific performance.

2.3 In the EU, the security industry has an estimated market value of up to EUR 36.5 billion and accounts for around 180 000 jobs. Globally, the market has grown over the last decade from EUR 10 billion to EUR 100 billion in 2011. The industry comprises the following sectors: aviation and maritime security and transport security in general; border security; critical infrastructure protection; counter-terrorism intelligence (including information and communications security and the cyber dimension); physical security; crisis management; and protective clothing.

2.4 In addition, there is the space-related security industry, with its many applications.

2.5 In Europe, the market for space-based security products is based on large multinational groups, which operate at European level, and individual Member States, in the civil and commercial spheres, with demand split 40 %-60 % between the commercial and the institutional.

2.6 Although market trends show constant growth, untouched by the economic slowdowns of the international crisis, the EU security industry is faced with a very fragmented internal market and an industrial base weakened by the considerable divergence between legal frameworks and technical and regulatory standards at national level, while research efforts and public procurement are still largely confined to individual Member States, despite EU action in this area, such as measures under FP7.

2.7 The EU is required to ensure the security of its citizens, businesses and society as a whole across a wide swath of activities, from civil protection against natural disasters to the protection of the food chain, from preventing and combating terrorism, to guarding against chemical, biological, radiological, nuclear and explosive risks.

2.8 The security industry is crucial for the future and is particularly representative of the challenges and opportunities facing Europe: thanks to their level of technological development, many EU companies are among the world leaders in various segments of the sector, but risk losing market share to their main trading partners.

2.8.1 Relevant, detailed and reliable statistics are needed with regard, looking at the sector’s companies in terms, not least, of their production, workforce and size.

2.9 The management of companies within the security sector is highly complex, hinging on a number of variables:

— the homogeneity, transparency and accessibility of markets;

— strategy and vision; access to financial resources;

— legal frameworks, technical standards, harmonised procedures and IPR protection;

— technological and operational performance; and

— the possibility of managing and anticipating new competition scenarios.

2.10 In order to competitively reinvigorate the European security industry, the EESC considers it essential that the European internal market ensures:

— an internal dimension of full single market interoperability, reducing the fragmentation of both domestic markets and investment in research and innovation;

— an external dimension of access to international markets, addressing the insufficient international protection of industrial property rights (IPR), the barriers to commercial and public procurement market access, and implementing also in this sector a more aggressive 'integrated strategy for the external dimension of industrial policy which ensures a leading role for the EU in the area of trade and a common approach in multilateral and bilateral trade agreements' [1];

— equal rights for European manufacturers in relation to the export of military equipment to third countries. There should be no discrimination in the single market against manufacturers from Member States without direct access to the sea, in the form of requirements to obtain 'transit licences' for the transport of their products to a seaport in another Member State;

— a societal and ethical dimension to security-related technological applications, right from the design phase, to ensure their **societal acceptance**, with full protection of the privacy of citizens and their fundamental rights, combined with the protection of confidential data; and

— products and services that do not intrude on privacy, but that enable winning approaches in terms of human resource development and international activities, supporting large companies, start-ups and SMEs, in part by harnessing networked consortia and districts, in order to obtain an adequate, competitive critical mass.

2.11 At global level, **the USA** is by far the biggest competitor. It benefits from a harmonised legal framework, common standards and strong public demand at federal level [2], with a consolidated internal market that accounts for over 42 % of global turnover and companies at the forefront in technical security equipment. **Japan and Israel** have leading companies in specific kinds of advanced equipment, especially in the IT and communications sectors, while **Russia and China** are highly advanced in the traditional sectors of protection of physical security.

2.12 In this global context, the EESC stresses the need for a proactive EU industrial policy for the security sector that better reflects the balance between the capacities of the sector and a technical and regulatory framework and IPR, and above all, types of products, services and systems that can comply with common standards and harmonised regulations and procedures, such as:

— access control systems;

— scanning hardware and software;

— protection systems and equipment;

— systems and tools for identifying and interpreting reality;

— systems and tools for surveillance and tracking; and

— alarm systems;

while for 'sensitive' products, the regulatory and access conditions are subject to assessments and agreements on a case-by-case basis, to maintain quality and safety levels.

2.13 The EESC has repeatedly highlighted the need to develop policies on network and information security, which is crucial to the Digital Agenda for Europe.

2.14 The EESC has also previously expressed its views on the crucial issues of aviation security [3], maritime security [4] and land transport security [5], as well as on the management of operational cooperation at the external borders [6], underlining the role of the Frontex agency and the need for a global approach to border security and to combating illegal immigration.

2.15 With regard to space-based environment and security monitoring, the Committee has stressed the importance of the Sentinel satellites and the GMES programme and the satellite navigation system Galileo [7].

2.16 Several studies have emphasised the importance of security-technology demonstration projects in the field of chemical, biological, radiological, nuclear and explosive risk (CBRNE).

[1] See OJ C 218, 23.7.2011, p. 25.

[2] See Homeland Security Act of 2002 and US Safety Act of 2002.

[3] See OJ C 100, 30.4.2009, p. 39, and OJ C 128, 18.5.2010, p. 142.

[4] See OJ C 44, 11.2.2011, p. 173.

[5] See OJ C 65, 17.3.2006, p. 30.

[6] See OJ C 44, 11.2.2011, p. 162 and OJ C 191, 29.6.2012, p. 134.

[7] See OJ C 256, 27.10.2007, p. 47 and OJ C 256, 27.10.2007, p. 73 and OJ C 181, 12.6.2012, p. 175.

2.17 The 7th Framework Programme (FP7) is the first to include a specific research programme on security. With a budget of EUR 1.4 billion, it is focused solely on civil applications and developing the technologies and knowledge to protect EU citizens [8], while respecting their privacy and other fundamental rights.

2.18 The EESC believes that the use of civil/military hybrid technologies should be facilitated, by developing suitable standards in cooperation with the European Defence Agency, while more resources and impetus should be injected into supporting the 'Security' strand among the enabling technologies of the new research and innovation FP [9], encouraging demonstration projects and pilot prototyping.

2.19 The Commission included the security industry among the essential elements of the Europe 2020 flagship initiative *An integrated industrial policy for the globalisation era*, on which the Committee has already outlined its views [10].

2.20 The EESC believes it is essential to launch a **single European strategy that takes an integrated approach to the security industry**, because security is one of the main concerns of today's society, is a cornerstone of growth and employment and requires joint efforts and shared vision among all the Member States in order to strengthen competitiveness.

3. **Gist of the Commission document**

3.1 The communication outlines the strategic importance of the EU security industry and the main actions required to make the industry more competitive and innovative, through which the Commission intends to accompany this process.

3.2 The proposed action plan sets out the following guidelines:

— overcome EU internal market fragmentation by means of harmonised certification procedures and technical standards for security technologies and mutual recognition of certification systems;

— make research and innovation more efficient and bring it closer to companies through *technical and regulatory mandates* in conjunction with the EDA for 'hybrid standards" applicable to both security- and defence-related R&D, use the new rules on IPR and pre-commercial procurement provided for in Horizon 2020, and employ funding under the future *Internal Security Fund* for rapid validation tests of security technologies;

— incorporate the social dimension and privacy; and

— market access: export rules to open third-country public procurement markets and overcome technical barriers, consider an EU security label for products; and carry out a study on third party liability limitation, as provided for under the US Safety Act (implementation: 2012/2013).

3.3 The Commission intends to set up a monitoring group to track the progress of the proposed measures within a specific timeframe.

4. **General comments**

4.1 The Committee believes that, for the benefit of EU citizens, companies, workers and European society as a whole and with a view to developing a competitive and sustainable economy, it is essential to define a comprehensive, coordinated approach at EU level to tackling security challenges and developing the EU's security industry, by devising an overall EU strategy on security systems that places individuals and their dignity at the centre, so as to meet basic requirements in terms of freedom and security.

4.2 In the EESC's view, greater consideration needs to be given to the added value of the existing agencies, such as the EDA (defence), Frontex (external borders), Europol (public safety), ENISA (information security), the EASA (aviation safety), the EMSA (maritime safety) and the EFSA (food safety), and the alert systems such as RAPEX (European rapid alert system for product safety) and the ECHA in Helsinki (system on chemical products/REACH).

4.3 The EESC agrees with the Commission on the need to take full advantage of the leading position of many European companies in the sector, **proactively** securing a truly unified and practicable European internal market, unhindered by fragmentation, and promoting a sector that constitutes a pool of products and services that is vast and promising from an employment perspective.

[8] At its halfway stage, FP7 had already funded more than 130 security research projects. The European Commission has published a catalogue of related success stories.

[9] See INT/651 Key Enabling Technologies

[10] See OJ C 218, 23.7.2011, p. 38.

4.4 However, the EESC thinks that the European action plan should go further and approach the launch of a fully-fledged common European strategy for the security industry with a shared vision, a European platform that brings together the various aspects of security and a system of governance capable of providing effective, unified coordination.

4.5 This integrated-approach strategy could take the form of a virtual platform, incorporating the ethical and governance issues, the inter-sectoral aspects and interoperability.

4.6 The EESC believes it necessary to bridge the gap of understanding between policymakers and the industry, including by strengthening initiatives such as the European Security Congress and through a permanent platform for dialogue, such as the Security Policy Forum.

4.7 Overcoming the fragmentation of the EU internal market requires:

— horizontal cooperation and coordination in the field of security, within and between the EU institutions and its agencies, to ensure full product and procedure interoperability, in tandem with vertical coordination between the various levels of action;

— a participatory foresight exercise, to define a shared, agreed vision; and

— a system of governance that involves the public and private sectors.

4.8 The Committee believes that, in addition to integrating the social dimension right from the design phase of products, services and systems, mechanisms need to be implemented that involve the social partners and organised civil society in monitoring compliance with the societal and ethical dimension of developing security and its technological-production applications.

4.8.1 The issuance of technical and regulatory mandates, in conjunction with the EDA, should be done in accordance with the principles of the new standardisation policy, with an open and transparent annual work programme, full participation of the social partners and organised civil society representatives, and the establishment of specifications for public procurement that respect the principles of openness, consensus, transparency, relevance, neutrality and quality [11].

4.8.2 The EESC endorses the proposed approach to the mutual recognition of certification systems, insofar as it achieves common levels of competence for accredited certification bodies, more stringent selection criteria and harmonised selection procedures for conformity assessment [12].

4.9 The Committee would stress the importance of regulatory recognition for **dual-use technologies** to promote hybrid technologies for joint civil/military use, while advocating even more strongly that this be bolstered both financially and in terms of content under the *enabling technologies* priority provided for in Horizon 2020, alongside actions under the future *Internal Security Fund*.

4.9.1 As regards intellectual and industrial property, while the innovative approaches in Horizon 2020 are certainly important, IPR protection under the WTO and under the bilateral and multilateral European association agreements needs to be strengthened, with a particular focus on the clauses regarding liability limitation and access to international public procurement.

4.9.2 The EESC shares the Commission's view on the merits of making full use of the possibilities provided by the *pre-commercial procurement* instrument within Horizon 2020.

4.10 The EESC fully endorses bolstering the societal and ethical dimension in the rules governing the security-technology industry.

5. **Specific comments**

5.1 **Overcoming market fragmentation on the basis of product type.** The EESC recommends setting priorities for action not by sector but by type of product that can most readily meet the requirements of the single market, through harmonised regulations and procedures, on the grounds of their high market potential, and their impact on a broad section of the public and workers, with particular regard to promoting SME development, in terms of both financial resources and research, and with respect to organisation.

5.2 **Research and innovation, IPR and procurement.** The EESC calls for EU funding for security technologies under Horizon 2020 to be stepped up, in tandem with a strong presence within the 'enabling technologies' strand; it also advocates bolstering joint interoperability projects on security under the ISA programme [13]; applying exemptions to the

[11] See OJ C 68, 6.3.2012, p. 35.

[12] See OJ C 120, 16.5.2008, p. 1.

[13] ISA – Interoperability Solutions for European Public Administrations 2010-1015.

sector, under the State aid for Innovation system; verifying the effective application of Directives 2004/18/EC and 2009/81/EC and of the pre-commercial procurement instruments to the security industry; more public-private and civil-military cooperation and the facilitation of cross-border company merger and grouping strategies; harmonisation of the rules on third party limited liability protection (TPLL); and better internal IPR rules.

5.3 **Access to international markets.** The EESC believes it necessary to step up integrated, common foreign policy actions within the security industry, strengthening IPR protection under the WTO and the bilateral and multilateral European association agreements, guaranteeing equal access to international markets and procurement on the basis of reciprocity, increasing the weight of the EU in international standardisation and launching a quality label (*euro security label*).

5.4 **Societal and ethical dimension.** All security systems, products and services must respect the fundamental rights and freedoms of citizens, especially the right to privacy, and contribute to economic and social progress, secure trade and people's well-being and safety. Technological developments should enable the protection of personal data and privacy to be enhanced, from the outset, providing – with the support of public-private dialogue – the means for transparent and accountable law enforcement that should be centred on human protection.

5.5 **Training, support** and employment of qualified human resources: in line with the requirements of security and the application of advanced security technologies, so as to ensure the delivery of high-quality professional services, within a fully interoperable system that is respectful of individuals and their dignity.

Brussels, 16 January 2013.

The President
of the European Economic and Social Committee
Staffan NILSSON