statewatch

Analysis

The visible hand: the European Union's Security Industrial Policy

Chris Jones, August 2016

List of acronyms used in this report

ASD	AeroSpace and Defence Industries Association of Europe
ASSA	International Aviation Security Services Association International
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CoESS	Confederation of European Security Services
CR	Cognitive Radio
EOS	European Organisation for Security
ESOs	European Standardisation Organisations
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
ESRP	European Security Research Programme
ETSI	European Telecommunications Standards Institute
FP7	Seventh Framework Programme for Research and Technological Development
GPS	Global Positioning System
IPR	Intellectual Property Rights
ISF-Borders	Internal Security Fund - Borders and Visas
ISF-Police	Internal Security Fund - Police
PASAG	Protection and Security Advisory Group
PCP	Pre-Commercial Procurement
POV	Pre-Operational Validation
PPI	Public Procurement of Innovative Solutions
QATT	Qualified Anti-Terrorism Technology
R&D	Research and Development
RPAS	Remotely Piloted Aerial System(s)
RRS	Reconfigurable Radio Systems
SAFETY Act	Support Anti-terrorism by Fostering Effective Technologies Act
SDR	Software Defined Radio
SIP	Security Industrial Policy

1. Introduction

> *“A competitive EU security industry is the* conditio sine qua non *of any viable European security policy and for economic growth in general.” [1]*

The EU has a long-standing ambition to create an “area of freedom, security and justice”, as set out in Article 67 of the Lisbon Treaty. A more recent counterpart to this ideal is the plan to create a “true internal market for security”, in which companies will be able to sell security technologies, products and services to customers in any EU Member State without being hampered by differing regulatory or technical standards. The first formal announcement of this new policy came in 2012, when the European Commission published the Security Industrial Policy (SIP), with the “overarching aim” to “enhance growth and increase employment in the EU's security industry.”

The SIP has led to a whole host of initiatives: projects aimed at technical standardisation; attempts to bring industrial interests and state agencies together through various forms of public-private partnership; enhancing “synergies” between civil security and defence research; and initiatives aimed at introducing standards for “privacy by design”.

On the one hand, the launch of the SIP would appear to be simply the Commission doing the basic work of the EU – attempting to create a single market, in this case for “security” products. At the same time, the SIP goes some way to meeting the demands of the security industry, who lobbied heavily for the adoption of such a policy.

As one Commission official put it in 2011: “Whatever we propose, be it in the research budget or regulatory options, corresponds to the exact requirements of the sector.” [2] However, after initially welcoming the launch of the SIP, lobby groups began to voice displeasure with what were seen as limited ambitions and the Commission’s failure to meet some of their demands.

While the overall aim of the SIP is to enhance the profitability of the security industry, the policy itself states that there is “no clear definition” of that industry. The Commission argued in a “non-exhaustive list” that it encompassed everything from aviation security to “counter-terror intelligence” and protective clothing. One group of authors suggested that the definition appears designed “to fit the diverse constituency of ESRIF (the European Security Research and Innovation Forum, see below), rather than an evidence-based economic analysis.” [3]

A more recent study launched in the framework of the European Security Research Programme [4] sought to undertake the difficult task of working out more accurately the make-up, size and value of Europe’s security industry. While the Commission stated in the SIP that the “EU security market has an estimated market value in the range of €26 billion to €36.5

[1] European Commission, ‘Commission Staff Working Paper – Security Industrial Policy’, SWD(2012) 233 final, p.4, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN

[2] European Commission press release, ‘Stakeholders outline their views to Commission on future EU industrial strategy for the European security sector’, October 2011

[3] ‘Review of security measures in the 7th Research Framework Programme FP7 2007-2013’, *European Parliament Directorate-General for Internal Policies*, April 2014, http://statewatch.org/news/2015/jan/ep-2014-04-fp7-security-research.pdf

[4] The formal name of the ESRP is ‘Secure societies: protecting freedom and security of Europe and its citizens’. See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

billion with around 180,000 employees," [5] the authors of the study argued that it "generates a total turnover of as much as €191 billion and [employs] as many as 2.3 million people" – although they provide numerous caveats regarding those estimates. [6]

Whatever the real value of the "security industry", the Commission is set upon increasing it, in the hope of more "jobs and growth" and enhancing the implementation of EU and national security policies. The EU's initiatives in security are wide-ranging, but in significant aspects they dovetail with the interests of major security and defence companies: tools for mass data-gathering and predictive analytics, [7] continent-wide surveillance systems and databases, [8] the increasing use of biometrics in all walks of life, [9] and the closer integration of public authorities and private industry.

One study undertaken for the European Commission noted that:

> *"The development of a European public security market is perceived by [large security and defence] companies as a necessary condition for the achievement of profitable business." [10]*

An examination of the paper trail surrounding the SIP and the initiatives it has spawned serves to highlight some of the ways in which the EU is seeking to help these companies achieve "profitable businesses", and how the foundations for the EU's security project are being laid.

[5] European Commission, 'Security Industrial Policy: Action Plan for an innovative and competitive Security Industry', COM(2012) 417 final, 26 July 2012, p.3, http://www.statewatch.org/news/2012/jul/eu-com-security-industry-com-417-12.pdf

[6] Ecorys et al., 'Study on the development of statistical data on the European security technological and industrial base', June 2015, p.16, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/reference-documents/docs/security_statistics_-_final_report_en.pdf

[7] See for example, ESRP projects:
'ASGARD', http://cordis.europa.eu/project/rcn/203297_en.html;
'TENSOR', http://cordis.europa.eu/project/rcn/203292_en.html;
'DANTE', http://cordis.europa.eu/project/rcn/202691_en.html;
'RAMSES', http://cordis.europa.eu/project/rcn/202689_en.html.

[8] For example the proposed Entry/Exit System for tracking travellers entering and leaving the EU; and the EUROSUR border surveillance system.

[9] See 'The dawning of the biometric age' in *NeoConOpticon*¸ pp.46-48, http://www.statewatch.org/analyses/neoconopticon-report.pdf; and a more recent project, which hopes to "democratise" (i.e. maximise) the use of fingerprint scanners in society: 'INGRESS', http://cordis.europa.eu/result/rcn/165651_en.html

[10] *Istituto Affari Internazionali*, Manchester Institute of Innovation Research, *Institut des Relations Internationales et Stratégiques*, 'Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence', June 2010, p.143, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf

2. Background: persuasive action

In December 2009 the European Security Research and Innovation Forum (ESRIF), an informal public-private group convened to set the agenda for future EU security policy, recommended the establishment of “a persuasive European industrial policy,” in order to “open the door to global leadership in the security market, and spawn an efficient European industry, making our society best security solutions available to the world.” [11]

In a 2010 Communication on EU industrial policy the Commission signalled its intention to do more for the security industry, [12] and in March 2011 launched a public consultation. This received 59 responses from 13 countries. [13] There were also an unspecified number of position papers, from unspecified respondents, which the Commission said “do not appear in the statistics” but were “nevertheless taken into account in the overall analysis.” The responses broadly agreed with the Commission’s proposals, leading to the July 2012 publication of the Commission’s ‘Security Industrial Policy - Action Plan for an innovative and competitive Security Industry’. [14]

“A competitive EU security industry offering solutions for enhanced security can make a substantial contribution to the resilience of European society,” declared the Commission, announcing that the “overarching aim is to enhance growth and increase employment in the EU’s security industry,” in particular through gaining “market shares in emerging markets.”

The industry was pleased. Lobby group the European Organisation for Security (EOS) announced that it was “delighted to welcome the adoption of the long awaited Security Industrial Policy.” [15] Euralarm, the industry group for “the electronic fire and security industry”, said it would “be pleased to contribute to further works with the Commission.” One of the chief priorities of the ‘Security Business Unit’ of the lobby group ASD (AeroSpace and Defence Industries Association of Europe) is “influencing the outcome and implementation of an EU Security Industrial Policy.” [16]

The former head of ASD’s Security Business Unit, Alberto de Benedictis, is now chairman of the Commission’s ‘Protection and Security Advisory Group’ (PASAG), which provides advice on the content of work programmes for the European Security Research Programme. From 2007 to 2013 this had a budget of €1.4 billion; from 2014 to 2020 has a budget of €1.7 billion. [17] As detailed below, numerous security research projects have been geared towards the development of an EU-wide security market.

[11] See the ESRIF final report, available at: ‘European Commission responds to European Security Research and Innovation Forum (ESRIF) report’, *Statewatch News Online*, January 2010, http://database.statewatch.org/article.asp?aid=29548

[12] European Commission, ‘An Integrated Industrial Policy for the Globalisation Era: Putting Competitiveness and Sustainability at Centre Stage’, COM(2010) 614 final, 28 October 2010, p.27, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0614:FIN:EN:PDF

[13] *Statewatch* made a submission to the consultation: ‘Rethinking the EU Security Research Programme’, http://www.statewatch.org/analyses/no-133-esrp-consultation-response.pdf

[14] European Commission, ‘Security Industrial Policy: Action Plan for an innovative and competitive Security Industry’, COM(2012) 417 final, 26 July 2012, p.3, http://www.statewatch.org/news/2012/jul/eu-com-security-industry-com-417-12.pdf

[15] EOS, ‘New impetus to the competitiveness of the security industry’, 30 July 2012, http://www.eos-eu.com/?page=newsdetails&ListID=6&RowID=101&type=pressreleases

[16] ASD, ‘Security Business Unit’, http://www.asd-europe.org/security/

[17] For an overview of the early development and political trajectory of the ESRP, see: Ben Hayes, ‘NeoConOpticon’, 2009, http://www.statewatch.org/analyses/neoconopticon-report.pdf

The following sections follow the structure of the 2012 SIP paper and explain what the proposals entail, where they stand now and what is to come. An examination of the ins-and-outs of technical standardisation, public-private partnerships, or intellectual property regimes may not be particularly exciting. Nevertheless, understanding them is essential for understanding how the EU is attempting to develop its “true internal market for security”, a pre-requisite for building the so-called ‘Security Union’. [18]

[18] European Commission, ‘European Agenda on Security: Paving the way towards a Security Union’, 20 April 2016, http://europa.eu/rapid/press-release_IP-16-1445_en.htm

3. Joined-up markets

3.1. Standardisation for security

The first issue addressed in the SIP is “market fragmentation” – i.e. the EU does not have one unified market for security products and services, but numerous national markets. Key to addressing this are technical and regulatory standards. The SIP argues that standards “play a major role in defragmenting markets and helping industry in achieving economies of scale,” in ensuring “interoperability of technologies used by first responders, law enforcement authorities, etc.” and “for ensuring uniform quality in the provision of security services.” As CEN and CENELEC, two of Europe’s standardisation organisations, put it:

> *“All of the products and services we buy and use in our everyday lives have to meet certain standards of safety and quality. In Europe, these standards are developed and agreed by the three officially recognized European Standardization Organisations [ESOs]: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).” [19]*

Promoting and developing new standards in the security industry was recommended by the European Security Research and Innovation Forum (ESRIF) its predecessor, the European Security Research Advisory Board (ESRAB), the Commission itself, as well as an extensive Commission-contracted study on the industrial implications of the “blurring of the dividing lines between security and defence”. [20]

As well as funding projects in the EU’s Seventh Framework Programme for Research and Technological Development (FP7) dealing with standardisation issues, in 2011 the Commission sought to “accelerate” the ESOs’ work on security and in July 2013 and announced a focus on three areas: automated border control systems and biometric identifiers for border control; communications and command and control interoperability in the areas of crisis management and civil protection; and CBRNE (chemical, biological, radiological, nuclear and explosives) detection and sampling. [21]

According to the ESOs: “Human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness can be expected to be relevant to all the topic areas listed.” Unfortunately, while the choice of topics suggest that “privacy concerns” may certainly be relevant, they have not so far featured significantly in the work programmes and “roadmaps” that have been the result of the ESOs’ work.

[19] CEN-CENELEC, ‘European Standardization’, http://www.cencenelec.eu/standards/Pages/default.aspx

[20] *Istituto Affari Internazionali*, Manchester Institute of Innovation Research, *Institut des Relations Internationales et Stratégiques*, ‘Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence’, June 2010, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf

[21] The Commission set out a mandate in 2011, which was accepted by the ESOs, who produced a final report in July 2013. The work was supposed to have “an exclusively civil application focus”. A programme for security standardisation was also foreseen in the Commission’s Communication on ‘A strategic vision of European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020’, COM(2011) 311 final, 1 June 2011, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0311&from=EN

Zach Blas, an artist from the United States, has raised some interesting points regarding standardisation and networked surveillance systems:

> *"[D]igital, networked surveillance relies upon the production of global technical standards, or protocols, to account for human life… Technologies of identification like biometrics, GPS [Global Positioning System], and data-mining algorithms require normalizing techniques for indexing human activity and identity, which then operate as common templates for regulation, management, and governance. It is through the utilisation of such standards that surveillance is able to rapidly increase at a global scale… [with the] automated collection of information that is analysed against pre-established models… these models… are designed by humans, and therefore, contain socio-political tendencies and preferences within their very technical architectures." [22]*

The extent to which such a critique can or should be applied to other "missions" such as CBRNE protection, is open to discussion. Nevertheless, it is clear is that standardisation is not simply a technical issue. This point is also made clear in the CEN/CENELEC report: when it comes to the standardisation of crisis management operations and procedures, "Member States are very cautious," because attempts at ensuring "interoperability" in this area may be "perceived as contrary to the rights and the sovereignty of the States."

Standardisation is important not just for those selling products, but for those using them – for example, law enforcement authorities undertaking transnational operations. As the Commission noted in a 2007 Communication on 'Public-Private Dialogue in Security Research and Innovation':

> *"Standardisation… has proved to be an effective tool for the coherent and effective implementation of European legislation across a variety of EU policies.*
>
> *"…As a procurement tool, standards are a key element in market creation in the security domain at European and international level." [23]*

At the time of writing, the next steps in the Commission's standardisation agenda are not entirely clear. A representative of CEN/CENELEC said in response to an email that "there are some ongoing discussions regarding the real priorities identified by the Mandate M/487," and at the minute "the topics under consideration are crisis management and CBRNE." The Commission has apparently "identified a series of 10 items" for further standardisation work.

3.2. Certification and conformity assessment

After standardisation, the next step is "certification", described by the International Standards Organisation as:

[22] Zach Blas, 'Informatic Opacity', *The Journal of Aesthetics & Protest*, Issue 9, Summer 2014, http://www.joaap.org/issue9/zachblas.htm

[23] European Commission, 'Public-Private Dialogue in Security Research and Innovation', COM(2007) 511 final, 11 September 2007, p.7, http://www.statewatch.org/Targeted-issues/ESRP/documents/COM-2007-511-pub-private.pdf

> *“[T]he provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. Certification is also known as third party conformity assessment.” [24]*

According to the SIP, there are “no EU-wide certification procedures for security technologies. National systems differ widely, thus significantly contributing to the fragmentation of the security market.” [25] These differing national processes mean there are “uncertainties for equipment providers in relation to the expectations of customers regarding required performance and, in turn, for determining investments in technology/product development.” [26]

Investments are at stake, and publicly-funded research is here to assist the industry. The FP7-funded CRISP project aims to “facilitate a harmonised playing field for the European security industry by developing a robust methodology for security product certification.” One part of the project “will present a roadmap for adopting of the proposed certification scheme,” while another “will focus on activities to enhance acceptance of the new certification measures.” [27]

Another helping hand comes from the HECTOS project:

> *“As well as mechanisms to independently evaluate security product performance, on a scientifically valid and statistically reliable basis, [HECTOS] will consider ethical and privacy requirements and regulatory compliance. The approach will be validated through experiments using two different product groups as case studies: weapons and explosives detection systems (outside of aviation security) and biometric recognition.” [28]*

For the time being, the Commission has limited its own initiatives in the field to two areas: airport security screening equipment and alarm systems. For the former:

> *“[T]here exists a whole body of EU legislation which sets out performance requirements for such equipment. However, this legislation does not contain the required conformity assessment mechanism so that certification of screening equipment in one Member State would be mutually recognised in any other Member State.”*

As for the latter:

> *“[S]ome European performance standards already exist. Moreover, there exists the industry-led certification mechanism CertAlarm. However, this system is faced with the problem that it is privately run and that Member State authorities have no obligation to accept certificates established under the scheme.”*

The SIP Communication also claims that harmonising conformity assessment procedures for airport screening systems and alarm systems will create “a clearer European identity for these technologies, a possible ‘EU brand’,” which “should contribute to enhancing the global competitiveness of the EU companies with regards to their US and Chinese competitors.” In

[24] ISO, ‘What is conformity assessment?’, http://www.iso.org/iso/home/about/conformity-assessment.htm
[25] Security Industrial Policy, p.7
[26] Commission Staff Working Paper – Security Industrial Policy, p.20-21
[27] CRISP, http://cordis.europa.eu/project/rcn/185503_en.html
[28] HECTOS, http://cordis.europa.eu/project/rcn/192051_en.html

the explanatory document accompanying the SIP Communication this is described as “dynamic” competitiveness (as opposed to price competitiveness). [29]

This “possible ‘EU brand’ could take the form of an “EU Security Label”. The Commission noted that: “As suggested by ESRIF, such a label could act as a seal of ‘quality’ for security products (made and validated in the EU).” The Commission again raised the issue of US leadership in the global security market:

> *“The market leading US companies are still the technological front runners, they additionally also benefit from a harmonised legal framework and a robust internal market. This gives them not only a reassuring basis but also the benefit of a clearly recognised and distinguishable US brand, which has proven to be a highly valuable advantage compared to EU companies in terms of international competition.*
>
> *“This lack of a similar "EU brand" is especially critical if one considers that the central future markets for security technologies will not be in Europe but in emerging countries in Asia, South America and the Middle East.” [30]*

In 2013 the Commission launched public consultations on its proposals to develop harmonised conformity assessment procedures for airport screening equipment and alarm systems. In both cases, there was strong support for the establishment of an EU-wide system through new legislation. There were indications that legislative proposals on the two topics would be published in late 2015 and early 2016. In July 2016 the Commission announced that it “will soon come forward with a proposal on airport screening equipment to remove barriers to the Single Market and to enhance the competitiveness of the EU security industry in export markets.” [31]

3.3. Civil-military synergies

After standardisation and certification, the third plank of the Commission’s proposals to reduce market fragmentation revolves around “exploiting synergies between security and defence technologies”, which entails overcoming “fragmentation” between the two markets. The SIP said:

> *“To some extent, this fragmentation is normal, given that the industrial base supplying these two markets is not fully identical and that the end-users differ, application areas differ, and so do the requirements. However, this fragmentation is felt upwards at the level of R&D and capability development, and is felt downwards at the level of standardisation. It leads sometimes to the*

[29] “It is not expected, however, that the reduction in costs resulting from an EU-wide approach would have a significant impact on the price competitiveness of EU alarm products in international markets. Nonetheless, a less fragmented EU market should encourage investment in research, technology development and innovation, which would have an impact on ‘dynamic’ competitiveness.” See: Commission Staff Working Paper - Security Industrial Policy, p.38

[30] Security Industrial Policy, p.2

[31] European Commission, ‘Implementation of the European Agenda on Security – Questions & Answers’, 20 July 2016, p.4, http://statewatch.org/news/2016/jul/eu-com-agenda-on-security-update-20-7-16.pdf

> *duplication of R&D efforts and the impossibility of making use of economies of scale due to differing standards in these two markets.” [32]*

The Commission set out one objective: to issue a standardisation mandate to the ESOs for “hybrid standards”, which apply to both civil and defence technologies, for Software Defined Radio (SDR).

SDR is one of two types of Reconfigurable Radio Systems (RRS), the other being Cognitive Radio (CR). The Commission’s mandate noted that with regard to civil security, wireless communication development should address the “lack of interoperability due to different technology standards and systems”; “lack of broadband connectivity to support a wide range of new applications”; and “economic sustainability”. Some experience has been gained from Commission- and FP7-funded projects such as WINTSEC, [33] HELP [34] and EULER, [35] but there is a need “to ensure the standardization of suitable SDR architecture(s)… The ideal situation would be a single architecture fulfilling the requirements of both [civil and military authorities].” [36] The work is being undertaken “in close cooperation with the European Defence Agency.” [37]

Also under consideration are standardisation mandates relating to drones (with regard to sense and avoid technologies [38] and airworthiness requirements). Work in this field is being propelled by the European Defence Agency. In February 2016 the Agency, representing a group of Member States made up of France, Germany, Italy, Poland and Sweden, signed an agreement with “an industrial consortium led by Airbus Defence and Space… to contribute to the integration of Remotely Piloted Aircraft Systems (RPAS) into common airspace in Europe.” [39] The Agency is also reviewing submissions for projects related to RPAS standardisation as part of an EU “pilot project” on “defence research”. [40]

[32] Security Industrial Policy, p.8

[33] European Parliament Policy Department External Policies, ‘Software Defined Radio’, October 2007, p.5, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2007/381403/EXPO-SEDE_ET(2007)381403_EN.pdf

[34] ‘HELP’, http://cordis.europa.eu/project/rcn/97890_en.html

[35] ‘EULER’, http://cordis.europa.eu/project/rcn/106857_en.html

[36] European Commission, ‘Standardisation mandate to CEN, CENELEC and ETSI for reconfigurable radio systems’, 19 November 2012, http://www.etsi.org/images/files/ECMandates/m512.pdf

[37] Security Industrial Policy, p.8. See also: European Defence Agency, ‘Software Defined Radio’, 6 August 2012, https://www.eda.europa.eu/our-work/projects-search/software-defined-radio

[38] These are the systems that allow drones to automatically detect (“sense”) other aircraft or objects in their path, and subsequently to avoid them. The lack of reliable sense and avoid technologies has proved to be a major stumbling block to the introduction of long-distance and autonomous drones into civil airspace.

[39] European Defence Agency, ‘New project to facilitate the integration of RPAS into European airspace’, 11 February 2016, https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2016/02/11/new-project-to-facilitate-integration-of-rpas-into-european-airspace

[40] European Defence Agency, ’21 proposals received for Pilot Project on defence research’, 30 June 2016, https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2016/06/30/21-proposals-received-for-pilot-project-on-defence-research

4. From research to market

The Security Industrial Policy also identified a problem with the “gap between research and market,” highlighting four issues in particular:

- aligning funding programmes and exploiting Intellectual Property Rights (IPR) routes;
- pre-commercial procurement;
- access to international procurement markets; and
- third party liability limitation.

4.1. Funding programmes and intellectual property

As well as a €1.7 billion security research budget, the EU has a €3.1 billion Internal Security Fund (ISF) running from 2014 until 2020. This is based on two separate legal instruments, one dealing with policing and the other with borders. The majority of the money is distributed to Member States, but €606 million is available for ‘Union actions’ (€264 million from ISF-Borders and €342 million from ISF-Police). [41] This includes projects aimed at “testing and validating” the results of security research projects, intended to allow the Member States (and the EU) to increase their deployment and use of new technologies.

The ISF-Police Regulation says that funding reserved for “Union actions” may be used for:

> *“[P]articularly innovative projects developing new methods and/or deploying new technologies with a potential for transferability to other Member States, especially projects aimed at testing and validating the outcome of Union funded security research projects.” [42]*

The ISF-Borders Regulation contains similar wording. [43] However, “transferability to Member States” is not the Commission’s only interest – the Security Industrial Policy says:

> *“Where Union capacities are needed, the Commission will consider reinforcing these testing and validating measures through the actual purchase of prototypes for the EU, if adequate.” [44]*

Specific rules have been put in place on the use of information generated by security research projects, “in order to be able to exploit security research results in subsequent testing and validation.” These allow the Commission (and other public authorities) to make use of

[41] European Commission, ‘Investing in an open and secure Europe: €1.8 million to fund Asylum, Migration, Integration and Security’, 25 March 2015, http://statewatch.org/news/2015/mar/eu-com-2015-03-25-pr-amif-isf-programme-agreement.pdf

[42] Article 8(2)(h), Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1433323570404&uri=CELEX:52011PC0753

[43] Article 13(2)(i), Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1433323559156&uri=CELEX:32014R0515

[44] Security Industrial Policy, p.9

intellectual property from ESRP projects "on fair and reasonable grounds", [45] without certain caveats that apply to other research themes in Horizon 2020. [46]

Access will be granted to the information "for the purpose of developing, implementing and monitoring… policies and programmes in this area [civil security]," and will be limited to "non-commercial and non-competitive use". Access to the information must also be on:

> *"[A] royalty-free basis and upon bilateral agreement defining specific conditions aimed at ensuring those rights will be used only for the intended purpose and that appropriate confidentiality obligations will be in place. Such access rights shall not extend to the participant's background [intellectual property held before participation in an ESRP project]." [47]*

The Commission argues that these more permissive rules can help expand the "public-private dialogue" between industry and public authorities. They: "should lead to a more direct and faster exploitation of the results of EU security research by the national authorities and a closer cooperation with the mostly public end-users, thus enhancing greatly the efforts to overcome the gap from research to market in the security area." [48]

4.2. Bringing the state to the market: pre-commercial procurement

A second initiative is pre-commercial procurement (PCP). ESRIF's final report recommended that: "Pre-commercial procurement of innovative solutions should be exploited as a mechanism to bring research results closer to market." The Commission duly made a commitment to PCP in the Security Industrial Policy, stating that:

> *"PCP is a very useful tool in bridging the gap from research to market… Eventually, PCP should enable public users to play a more central role in the innovation cycle through the purchase of novel technologies. Procurers should act as 'agents of change'."*

PCP is used when a "challenge" – for example, intelligence-gathering or border surveillance – needs "R&D [research and development] to get new solutions developed." The problem may be clear, but competing "solutions" need to be compared or validated. Thus, public sector institutions or agencies "buy R&D to steer development of solutions to [their] needs," to "gather info about pros/cons of alternative solutions," and "to be better informed," in order for possible future PPI (Public Procurement of Innovative Solutions) schemes later on. [49] Public bodies

[45] Security Industrial Policy, p.9

[46] In relation to every other research scheme the Commission must, following a request for information, ensure that it the information in question "is relevant to public policy" and that "the participants have not provided sound and sufficient reasons for withholding the information concerned." See: Article 4(1), 'Information to be made available', Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 – the Framework Programme for Research and Innovation (2014-20)" and repealing Regulation (EC) No 1906/2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0081:0103:EN:PDF

[47] Article 49(2), 'Access rights for the Union and the Member States', Regulation (EU) No 1290/2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0081:0103:EN:PDF

[48] Security Industrial Policy, p.9

[49] In PPI schemes, the state acts as a "first buyer" for "innovative products and services that are newly arriving on the market," aiming to "trigger industry to scale up its production chain to bring products on the market with desired quality/price ratio within a specific time frame." See: Khoen Liem,

buy research and development “from several suppliers in parallel… in the form of competition,” subsequently “evaluating progress after critical milestones.” [50]

The SIP argues that “R&D support through a PCP scheme would lead in the security industry to extra sales of 2 billion Euros between today [July 2012] and 2020.” Thus:

> *“The Commission intends to make full use of the PCP instrument set out in Horizon 2020 and devote a significant part of the security research budget on this instrument. This novel funding approach should bring research closer to the market by bringing together industry, public authorities and end users from the very beginning of a research project. The Commission considers that border security and aviation security are the most promising areas for undertaking PCP.” [51]*

The 2014-15 security research work programme sought projects that would “prepare the ground for a future PCP for civil protection solutions” (including creating “a roadmap for a future PCP topic to be included for an upcoming Horizon 2020 Secure Societies research call”), although it appears that in the end no successful bids were submitted.

The work programme also included the first full-blown PCP scheme, on ‘Light optionally piloted vehicles (and sensors) for maritime surveillance’. It sought projects that would “plan the research and design of solutions covering a broad variety of issues, including technologies,” useful for “surveillance… detection and early identification and tracking of moving targets,” including “identification of anomalous behaviour.” By 2020, the winning project would produce at least three prototype systems and establish:

> *“[A]t least one operational scenario in which all the prototypes and elements of systems issued from the previous phase of the action… will be tested. This scenario should take place within an actual multinational operation, such as a FRONTEX-coordinated joint operation.” [52]*

However, as with the proposed civil protection project, the EU’s database of research projects, CORDIS, lists no projects funded under this work programme theme.

The 2016-17 work programme, for which the results have not yet been announced, contains proposals for PCP schemes in relation to “broadband communication systems” for law enforcement agencies and emergency services, “toolkits integrating tools and techniques for forensic laboratories” and “next generation of information systems” to support EU missions launched as part of the Common Security and Defence Policy. [53]

A scheme similar to PCP – Pre Operational Validation (POV) – has already been used in FP7. The Commission has described these schemes in the following way:

‘Security Industrial Policy + Horizon 2020 Secure Societies’, presentation given in Helsinki, 25 March 2014, p.39, http://www.defmin.fi/files/2769/Khoen_Liem_Helsinki_24_Mar_14.ppt

[50] Khoen Liem, ‘Security Industrial Policy + Horizon 2020 Secure Societies’, presentation given in Helsinki, 25 March 2014, p.37-38, http://www.defmin.fi/files/2769/Khoen_Liem_Helsinki_24_Mar_14.ppt

[51] Security Industrial Policy, p.10

[52] Ibid.

[53] European Commission, ‘Horizon 2020 Work Programme 2016-17 – 14. Secure societies – Protecting freedom and security of Europe and its citizens’, 25 July 2016, http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

> *“Pre Operational Validation involves directly – and [supports] financially – end-user agencies (typically national or European authorities). This would shorten time to market and encourage market acceptance of new technologies… The basic idea of a POV scheme is to support the* demand *side of research [public authorities], rather than the* supply *side [companies] in their direct quest for new security solutions.” [54]*

POV schemes were introduced in FP7 “to provide a support framework for National Authorities to elaborate joint specifications and validation of integrated border surveillance systems.” [55] The overarching policy purpose was to support the development of the European Border Surveillance System (EUROSUR). [56] Three projects were funded as POV schemes: CLOSEYE, PERSEUS and EWISA. [57]

For all the talk of the need to create a “true internal market for security”, the establishment of POV, PCP and PPI schemes simply seems to back up an admission made by the European Organisation for Security: that the “security industry” is in a position of “market failure,” where “the allocation of goods and services by a free market is not efficient.” [58]

The structural relationship envisaged by these schemes was the subject of an incisive point made in a 2014 study on the ESRP carried out for the European Parliament. They involve “the securing of acquisition commitments from ‘end-users’ before a product is put on the market,” and thus:

> *“In sharp contrast with the idea of shaping a security market, then, the underlying idea here seems to be the promotion of a non-market commercial relation between the 'security industry' and public sector customers.” [59]*

4.3. Securing the world: access to international markets

The Commission notes in the introduction to the SIP that “the central future markets for security technologies will not be in Europe but in emerging countries in Asia, South America and the Middle East.” The chief competitors in global markets for security technologies are currently companies from Israel and the US, but new competition is emerging:

> *“Asian countries are closing the technological gap that separates them from EU companies at an increasing rate. Without a technological advantage, the EU companies will be confronted with fierce competition, also in view of the*

[54] Commission Staff Working Paper – Security Industrial Policy, p.25, footnote 60

[55] Ecorys, ‘Study on pre-commercial procurement in the field of security’, November 2011, p.64, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/pcp_sec_finalreport_en.pdf

[56] ‘Eurosur extended: all participating states now connected to border surveillance system’, *Statewatch News Online*¸ December 2014, http://database.statewatch.org/article.asp?aid=34324

[57] CLOSEYE, http://cordis.europa.eu/project/rcn/108227_en.html; PERSEUS, http://cordis.europa.eu/project/rcn/97515_en.html; EWISA, http://cordis.europa.eu/project/rcn/192052_en.html

[58] EOS, ‘Proposed End-to-End Approach for Security Research and Innovation’, 16 February 2015, p.20, no longer available online.

[59] ‘Review of security measures in the 7th Research Framework Programme FP7 2007-2013’, *European Parliament Directorate-General for Internal Policies*, April 2014, p.29, http://statewatch.org/news/2015/jan/ep-2014-04-fp7-security-research.pdf

> *production cost disadvantage often faced by EU firms [e.g. due to higher wages and better working conditions, health and safety standards, etc.].” [60]*

Europe’s security industry is keen to get a slice of the global pie, [61] but it needs the EU’s support. The Commission says it “will make full use of the instruments at its disposal to ensure a fair access of its security industry to international procurement markets” (the purchase by state and government authorities of security products or services). However: “Given the sensitive nature of security technologies, utmost attention will be given to relevant export regulations.”

The only “instrument” mentioned in the SIP with regard to this proposal is legislation put forward by the Commission in 2012 on “negotiating access to the public procurement markets of third countries” and clarifying “the rules governing access by third-country markets to the EU’s public procurement market.” [62] The Parliament adopted a position on the proposed legislation in January 2014, [63] but according to a November 2014 Council document, Member States were “deeply divided” [64] – so much so that the 2012 proposal was scrapped, with the Commission publishing a revised draft in January 2016. [65]

There is a clear tension between a policy that aims to increase exports for security technologies and products and the need to protect fundamental rights. A number of EU Member States – the UK, France, Germany and Italy, amongst others – have become notorious for permitting the export of weapons and security technologies to authoritarian regimes. [66]

[60] Security Industrial Policy, p.2

[61] See, for example, Jan Pie, ‘Heading towards wider horizons’, *ASD Newsletter*, February 2014, p.1, http://www.asd-europe.org/fileadmin/user_upload/Client_documents/ASD_Contents/2_COMMUNICATION/2.5_Publications/2.5.1_Newsletters/ASD_Newsletter_2014_February.pdf

[62] European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the access of third-country goods and services to the Union’s internal market in public procurement and procedures supporting negotiations on access of Union goods and services to the public procurement markets of third countries’, COM(2012) 124 final, 21 March 2012, p.2-3, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0124:FIN

[63] European Parliament Legislative Observatory, ‘Public procurement: access of third-country goods and services to the Union’s internal market and procedures supporting negotiations on access of Union goods and services to the markets of third countries’, 2012/0060(COD), http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0060%28COD%29&l=en

[64] Presidency, Proposal for a Regulation of the European Parliament and of the Council on the access of third-country goods and services to the Union’s internal market in public procurement and procedures supporting negotiations on access of Union goods and services to the public procurement markets of third countries [First reading] – State of play’, 15874/14, 20 November 2014, p.2, http://data.consilium.europa.eu/doc/document/ST-15874-2014-INIT/en/pdf

[65] European Commission, ‘Amended proposal for a Regulation of the European Parliament and of the Council on the access of third-country goods and services to the Union’s internal market in public procurement’, COM(2016) 34 final, 29 January 2016, http://data.consilium.europa.eu/doc/document/ST-5752-2016-INIT/en/pdf

[66] In 2014 the UK’s Conservative-Liberal Democrat government, apparently well-aware of the promise of emerging “security” markets, announced a plan to boost relevant exports: “From homeland security and border control to surveillance and detection equipment, UK companies are at the forefront of designing, manufacturing and selling security-related goods and services all over the world.” See: Increasing our security exports: a new government approach, 27 February 2014, https://www.gov.uk/government/publications/increasing-our-security-exports-a-new-government-approach

In December 2014 the Commission added spyware and other telecoms and internet surveillance equipment to its list of "dual-use" items – "goods, software and technology normally used for civilian purposes but which might have military applications or contribute to the proliferation of weapons of mass destruction." [67] Parliamentarians and campaigners had called for change after European firms were found to have supplied spyware and other surveillance technology to a whole host of repressive regimes. It now appears that the Commission is to propose even more stringent rules "that may force firms to go through lengthy approval processes when they export technologies including location tracking devices, biometrics and surveillance equipment," if those items "can be used to abuse human rights, for 'internal repression in the country of final destination' or a terrorist act." [68]

Whether these measures can make it through the EU legislature – and subsequently be maintained in the face of demands for increased security exports – will demonstrate the commitment of the EU and its Member States to ensuring that the security industry acts in accordance with human rights requirements.

4.4. Escaping blame: third party liability limitation

Europe's security industry has for some time demanded legislation that would protect it from legal responsibility for failures in its products. Industry's demands have centred on attempting to secure legislation establishing "third party liability limitation", in imitation of US legislation that seeks to protect US businesses from legal claims in cases where terrorist attacks take place despite the existence of high-tech security systems. This seems to be one of the few areas where the Commission has refused to meet the demands of industry.

In a joint position paper published in 2009, Europe's two largest lobby groups for the security industry, ASD and EOS, noted with concern:

> *"[T]errorist incidents can generate unlimited liability exposure which bears no relation to the value of the product or service provided, which is potentially enterprise-threatening for the companies involved, and for which insurance is generally unavailable." [69]*

In 2010, the Confederation of European Security Services (CoESS, a lobby group for companies providing security guards and services) and the Aviation Security Services Association International (ASSA International) issued a joint paper expressing similar views. [70]

The basic argument of the industry is that acts of terrorism could result in manufacturers of security technologies, products and services being exposed to legal claims for vast amounts of compensation, should their products or services be found to have failed. Following the 11

[67] Alex Hern, 'Spyware exports will need a licence under new EU rules', *The Guardian*, 6 November 2014, http://www.theguardian.com/technology/2014/nov/06/spyware-exports-licence-new-eu-rules-military-applications

[68] Catherine Stupp, 'Commission plans export controls for surveillance technology', EurActiv, 22 July 2016, http://www.euractiv.com/section/trade-society/news/technology-companies-face-export-hurdles-under-draft-eu-rules/

[69] ASD and EOS, 'Joint proposal on third party liability limitation', 2009, p.1, http://www.eos-eu.com/files/Documents/Positions/third_party.pdf

[70] ASSA-I and CoESS, 'European Solution for Third Party Liability of the Aviation Security Providers', June 2010, http://www.coess.eu/_Uploads/dbsAttachedFiles/CoESS_ASSA-I_White_Paper_on_Third_Party_Liability.pdf

September terrorist attacks in the US, a huge number of compensation claims were filed. By late 2004, some $38 billion had reportedly been paid in compensation by insurers, the government and charities. [71]

After the attacks, the US government asserted that "technological innovation is the Nation's front-line defence against the terrorist threat," and declared its intention "to stimulate innovation, development and deployment of anti-terrorism products and services." However, Congress was concerned that:

> *"[R]isk and litigation management issues, derived from the nation's product liability system and the associated potential liability exposure of manufacturers and users of anti-terrorism products and services… could lead to potentially crippling litigation, as well as public relations and shareholder issues in the aftermath of a terrorist attack." [72]*

These factors were "seriously threatening to keep new products and services from the market," and the SAFETY Act ('Support Anti-terrorism by Fostering Effective Technologies Act of 2002') was subsequently passed into law with a narrow majority. This legislation "encourages the development and deployment of anti-terrorism products and services," by:

> *"[L]imiting the liability of sellers of these products and services for third-party claims arising out of an act of terrorism where the product or service has been deployed to prevent, respond to, or recover from such an act and capping their insurance requirements." [73]*

Exemption from liability is not automatic. Rather, the Act gives the Secretary of the Department of Homeland Security the power to grant "an individual company, upon application, the protection available under the Act." Individual products or services can be awarded a "Qualified Anti-Terrorism Technology" (QATT) label. [74]

ASD and EOS proposed their own model for limiting the liability of European companies, taking into account some aspects of the SAFETY Act. According to the two groups, limitations on industry's liability are "essential" to "provide an equivalent level of protection to companies operating in the European security market," and to "promote the development, availability, and deployment of the best anti-terrorism technologies and services in the EU for the protection of Europe's citizens."

The organisations also argued that due to the ongoing outsourcing and privatisation of security services, there was a need for "the proper rebalancing of liabilities between public and private sectors". [75] That is: the industry that has demanded ever more power in the realm of security policy design and implementation – and that has received increasingly significant funds from

[71] Maggie Farley, 'More Than $38 Billion Paid to 9/11 Vicims', *LA Times*, 8 November 2004, http://www.latimes.com/la-110804compensation_lat-story.html

[72] Lucas Bergkamp, Michael Faure, Monika Hinteregger and Niels Philipsen (eds.), 'Study evaluating the status quo and the legal implications of third party liability for the European security industry', pp.239-242, *Metro, the European Centre of Tort and Insurance Law and Hunton & Williams*, 11 October 2013, p.261, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/final-report-tpl-11-10-2013_en.pdf

[73] Ibid.

[74] 'Study evaluating the status quo and the legal implications of third party liability for the European security industry', p.262

[75] ASD and EOS, 'Joint proposal on third party liability limitation', 2009, http://www.eos-eu.com/files/Documents/Positions/third_party.pdf

public budgets through privatisation programmes – also wants the state to provide financial cover should it fail in its “mission”.

The SIP outlined the Commission’s response: contracting “a major study analysing the legal and economic implications of third party liability limitation.” [76] This was published in October 2013 and concluded:

> *“This study has not found any evidence of an impending liability crisis in the security industry. The assertions of ‘enterprise-threatening’ liability exposure are not consistent with the liability standards imposed by the laws of the Member States covered in this study [England, France, Germany, Netherlands, Poland, Spain and Sweden]. No urgent EU measures are therefore necessary. To prevent problems in future cases, a Commission recommendation or communication could be considered.” [77]*

The industry was not happy. A group of “producers, providers, operators, end-users and customers of security equipment and services” wrote a joint letter to the Commissioner for Enterprise and Industry, Antonio Tajani, to express their displeasure. A post on the CoESS website said the findings of the study were:

> *“[C]ontrary to the real world experiences of those in the security industry and despite their explicit and repeated statements to the contrary during both the study consultation rounds and at the occasion of the presentation of the summary of the study. As an illustration of the seriousness of this issue, members of industry have declined to participate in security procurements because of liability concerns. The decision to forego a chance to grow its business is not one that any Company makes lightly.” [78]*

But “repeated statements” were not enough for the authors of the study:

> *“[W]e should note also that the security industry representatives that participated in the study, despite our repeated explicit requests… have not provided any relevant documentary evidence to support their assertions. For example, the study team received no documents backing up the claims relating to ‘enterprise-threatening’ liability exposure, the unavailability of insurance and the contractual obligations imposed on security providers by public authorities… the only substantive analysis that the study team received from these representatives, was incomplete, provided only some very basic information about the liability regimes of some Member States, and did not support these representatives’ arguments about the industry’s third party*

[76] Security Industrial Policy, p.11

[77] ‘Study evaluating the status quo and the legal implications of third party liability for the European security industry’, p.xx-xxi, http://ec.europa.eu/enterprise/policies/security/files/final-report-tpl-11-10-2013_en.pdf

[78] CoESS, ‘Third Party Liability: Private Security Equipment and Services Sector’s Joint Letter to EU Commissioner Tajani (Vice-President of the EU Commission, European Commissioner for Industry and Entrepreneurship)’, undated, http://www.coess.eu/?CategoryID=204

> *liability exposure, the unavailability of insurance, or the onerous contractual obligations imposed on security providers." [79]*

This seems to have put an end to the issue – for now. EOS is committed to pushing for "for an EU-wider [sic] regulation on this issue." [80]

[79] 'Study evaluating the status quo and the legal implications of third party liability for the European security industry', p.296, http://ec.europa.eu/enterprise/policies/security/files/final-report-tpl-11-10-2013_en.pdf

[80] EOS, 'Third Party Liability Limitation', undated, http://www.eos-eu.com/Middle.aspx?page=thirdparty

5. Solving ethical problems, or soothing public concern?

The final section of the Communication on the SIP deals with “better integration of the societal dimension,” which the Commission argues “would help in reducing the uncertainty of societal acceptance.” The “societal dimension” is the phrase used by the Commission for referring to fundamental rights issues – in both a legal and ethical sense – raised by security technologies, products and services. It appears that it was only inserted into the public consultation that led to the SIP at rather a late stage. [81]

Firstly, the Commission “considers that the societal and fundamental rights impact should already be taken into account through societal engagement before and during the R&D phase,” meaning that “societal issues” could be addressed “early on in the process”. It proposed making “societal impact testing an obligatory part, where appropriate, of all future security research projects,” including in any PCP schemes that are launched.

Secondly, the Commission proposed introducing the concepts of “privacy by design” and “privacy by default” during the design phase, with companies having to comply with “an appropriate European standard”. The Commission has proposed a voluntary standard (in accordance with responses to its consultation on the SIP [82]), but is convinced market forces will triumph, through “a strong peer pressure” for companies to adopt it. The SIP therefore proposed issuing a mandate to the European Standardisation Organisations “to develop a standard modelled on existing quality management schemes, but applied to the management of privacy issues during the design phase.”

The mandate was published in January 2015 [83] and subsequently accepted by CEN and CENELEC. The two standardisation organisations have established a new working group to deal with it, which will aim to “define and share best practices balancing security, transparency and privacy concerns for security technologies, manufacturers and service providers in Europe.” [84]

What those standards will look like remains to be seen, but the fact that they will be purely voluntary may undermine them from the very beginning. Furthermore, while the EU has one of the most highly-developed legal frameworks around data protection and privacy in the world, such standards may not be so highly-regarded in the “new and emerging markets” that

[81] Ben Hayes, ‘Please help this beleaguered industry! Commission launches consultation on security industry’, *NeoConOpticon*, 15 March 2011, https://neoconopticon.wordpress.com/2011/03/15/please-help-this-beleaguered-industry-commission-launches-consultation-on-security-industry/

[82] The numbers presented in the Commission’s paper detailing the results of the consultation is rather confusing on this point. According to its author(s), retaining “privacy by design as a voluntary effort for industry”, without any guidelines, standards or other guidelines was approved by 17% of respondents, and disapproved by 73%. These figures do not match the accompanying table, which give them as 15% and 59% respectively. Nevertheless, the other two options in this category show that a greater number of respondents (30% as compared to 23%) preferred the establishment of guidelines/standards by the EU, but keeping compliance with them voluntary. See: European Commission, ‘Results of the Public Consultation on an Industrial Policy for the Security Industry’, annex to Commission Staff Working Paper – Security Industrial Policy, p.52

[83] European Commission, ‘Commission Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data’, C(2015) 102 final, 20 January 2015, p.8, http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#

[84] CEN/CENELEC, ‘Privacy’, http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Privacy/Pages/default.aspx

are supposed to provide the industry's future profits. EOS is clearly aware of this – in its "factsheet" on the Security Industry Policy, the lobby group makes a telling reference to "privacy constraints":

> *"[C]itizens' fundamental rights, including privacy and data protection, should be properly considered (but non EU countries do not have the same kind of privacy constraints) so that technologies should be developed in a "privacy by design" approach." [85]*

As the group has put it elsewhere: concern for fundamental rights is "not necessarily a competitive advantage at [Member State] and international level." [86]

More fundamentally, as a 2014 study for the European Parliament put it: "one may ask whether concerns with human rights and fundamental freedoms should primarily be endorsed in relation to the securing of societal acceptance [for security technologies]," as the SIP appears to do. The study continued: "The respect for fundamental rights and freedoms constitutes a non-negotiable tenet for a democratic EU and Member States, rather than a means to an end." [87] However, this is industrial policy – a mercenary approach, unfortunately, seems somewhat inevitable.

[85] EOS, 'Factsheet on Security Industrial Policy', undated, http://eos-eu.com/files/Documents/Factsheets/SIP.pdf
[86] EOS, 'Proposed End-to-End Approach for Security Research and Innovation', 16 February 2015, p.6, no longer available online
[87] 'Review of security measures in the 7th Research Framework Programme FP7 2007-2013', *European Parliament Directorate-General for Internal Policies*, April 2014, p.29, http://statewatch.org/news/2015/jan/ep-2014-04-fp7-security-research.pdf

6. By the industry, for the industry?

The July 2012 publication of the Security Industrial Policy was the result of long, hard lobbying by the security industry. In reports such as ESRIF's, at numerous "high-level" conferences, and no doubt in the private and 'informal' meetings that have taken place between EU officials and industry representatives, the same monotonous demand was repeated: design an industrial policy for the security industry, or the security industry will wither and die in the face of foreign competition. This coincides neatly with the interests of the EU, which is keen both to promote itself as a credible security "actor", and to find new sources of growth for the ailing European economy.

Research for the European Parliament has questioned "whether the 'security market' is an economic reality in the first place or a policy objective embraced by the Commission in conjunction with specific industrial players." [88] It is hard to deny that the latter proposition holds true: from inventing its own definition of the "security industry", to attempting to break down obstacles standing in the way of a "true internal market for security", this is an economic and political project intended to benefit both the EU and national institutions and major industrial interests.

That the creation of such a market will primarily benefit large corporations has been argued in two in-depth EU-funded studies. A survey carried out by the EUSECON (A New Agenda for European Security Economics) project [89] concluded that:

> *"A wider market will create incentives for industrial concentration to achieve a European dimension, a desirable feature since it is also recognised that the number of companies operating in the sector is often too high…*
>
> *"The increasing competition across EU Member States will lead to the concentration of sales in the hands of the largest and more efficient firms… While long-term benefits will be positive, the restructuring process may create short-term imbalances in terms of plant closures and job losses of the less efficient firms." [90]*

Meanwhile, a 'Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence', contracted by the European Commission in 2008 and published in 2010, came to the following conclusion (emphasis added):

> *"System integrators (large companies) have developed strategies for security business, based on the assumption of significant, post 9/11 growth in the market. In their perception, the development of the security market would generate attractive returns, largely by translating defence capabilities into security products and services. The growth of the security market would, under these conditions, foster a positive blurring between security and defence. In reality, though, the development of this 'High-end' security market has been slow, as security tends to be fragmented with different cost structures… For these system integrators, the development of a large scale security market is*

[88 Ibid.

[89] 'EUSECON', http://cordis.europa.eu/project/rcn/86256_en.html

[90] Carlos Martí, 'A survey of the European security market', *Economics of Security Working Paper 43*,

> *the principal requirement for gaining synergies from the blurring. The development of a European public security market is perceived by these companies as a necessary condition for the achievement of profitable business." [91]*

Despite the Commission's efforts, it has not been enough for the industry. EOS has argued:

> *"In occasion of its creation, the European Security Industry has recognised the value of launching a Security Industrial Policy, but has also pointed out the limited ambitions of such policy, as the envisaged actions were considered as not sufficiently supporting the competiveness of the EU offer.*
>
> *"Despite these envisaged actions of the Commission to create the basis of a cohesive Internal Market and an all-inclusive security market, the developments these past two years have been slow and even those "limited ambitions" have not been met." [92]*

Dissatisfaction was also in the air at ASD's 2014 'High Level Round Table', the programme for which asked: "Will our analysis serve as a wake-up call for the new teams at the EU helm after the European elections?" [93]

Such objections are of course to be expected from an industry that is highly reliant on public money, although all is not yet lost: the Commission recently issued a communication on 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive Innovative Cybersecurity Industry'. Part of this involves a new public-private partnership that will see lobby group the European Cybersecurity Organisation given the opportunity to help design a €450 million "research and innovation" agenda. [94]

[91] *Istituto Affari Internazionali*, Manchester Institute of Innovation Research, *Institut des Relations Internationales et Stratégiques*, ''Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence', 15 June 2010, p.170, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf

[92] EOS, 'Proposed End-to-End Approach for Security Research and Innovation', 16 February 2015, p.50, no longer available online.

[93] ASD, 'Detailed Programme', 30 April 2014, http://www.tpeb.cz/wp-content/uploads/2014/05/DETAILED-PROGRAMME-_-ASD-ANNUAL-CONVENTION-TECHNOLOGY-FORUM-2014.pdf

[94] European Commission, 'Communication: Strenghtening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', 5 July 2016, https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and; European Commission, 'Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats', 5 July 2016, http://europa.eu/rapid/press-release_IP-16-2321_en.htm

7. Security for all?

Whether the further development of the “security industry” is likely to foster economic growth and create jobs remains to be seen. However, given that the development of a European security industry will often be dependent on the sale of potentially highly-repressive tools and systems to states both inside and outside the EU, it would perhaps be better not to pursue “jobs and growth” as ends in themselves and rather to ask exactly what kind of “jobs and growth” are preferable. That, in turn, would require asking more fundamental questions about the general economic, social and political priorities being pursued by the EU and its Member States.

For those interested more specifically in security issues, the examination provided in this report hopefully provides useful overview of how the EU’s “true internal market for security” is being constructed. It has sought to highlight the institutions, agencies, organisations and ideas involved, rather than to provide definitive answers as to if and how the initiatives being put in place should be challenged: alternative proposals are best left to those with minds more suited to the task.

One thing is clear: the EU may be duty-bound to level the playing field across the single market, but it is also required to ensure that fundamental rights are promoted and protected. If it is only the security industry lobby that expresses an interest in the design and implementation of “security industrial policy,” there is a significant risk of prioritising the former at the expense of the latter.

Statewatch does not have a corporate view, nor does it seek to create one, the views expressed are those of the author. Statewatch is not responsible for the content of external websites and inclusion of a link does not constitute an endorsement.