European
Commission

FINAL REPORT

Data and information collection for EU dual-use export control policy review

Written by SIPRI and Ecorys
6 November 2015

The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Contents

Abstract

As part of the ongoing review of the EU dual-use export control system, the European Commission is conducting an impact assessment. This study supports the impact assessment through the collection and analysis of data and information. The April 2014 Communication 'Ensuring security and competitiveness in a changing world', which outlines the review options, issues and actions provides the overall rationale and framework for this study. The Stockholm International Peace Research Institute (SIPRI) implemented the project jointly with Ecorys during January to September 2015. The project included three main Actions: (1) development of the methodology for data collection; (2) analysis of the baseline scenario through the collection of data and information, both on the structure and performance of directly affected sectors, and with regard to the impact of current controls and related problems; and (3) the analysis of the review options and corresponding review actions. The project combines EU- and sector-wide data with case studies on the machine tools, chemical and aerospace sectors. A strong focus of the study has been the implementation and future expansion of controls on exports of cyber-surveillance technologies and related review options.

Executive summary

Background

As part of the on-going review of the EU dual-use export control system, the European Commission is conducting an impact assessment. *This study supports the impact assessment through the collection and analysis of data and information.* More specifically, the project collects and analyses data which can be used to support an assessment of (a) the economic, social (including security and human rights) and environmental impact of the current export control regime; (b) the review options outlined in the Commission communication; and (c) the problems associated with the export of cyber-surveillance technologies and the current and potential impact of the introduction of new controls in this area, including through the adoption of a 'human security approach'. The April 2014 Communication 'Ensuring security and competitiveness in a changing world', which outlines the review options, issues and actions, provides the overall rationale and framework for this study.

Project implementation and timeline

The Stockholm International Peace Research Institute (SIPRI) implemented the project jointly with Ecorys during January to September 2015 (the draft final report was submitted in September 2015). The relevant EU working groups and sub-groups (Dual-use Working Party, Dual-use Coordination Group, and the DUCG Surveillance Technology Expert Group) have been regularly briefed on the progress of the project.

Deliverables

The project includes three main Actions: (1) development of the methodology for data collection; (2) analysis of the baseline scenario through the collection of data and information, both on the structure and performance of directly affected sectors, and with regard to the impact of current controls and related problems; and (3) the analysis of the review options and corresponding review actions. The project combines EU- and sector-wide data with case studies on the machine tool, chemical and aerospace industries. As required by the terms of reference, a strong focus of the study has been placed on controls of cyber-surveillance technologies and the potential impact of associated review options.

Outlining the dual-use sector

The study includes: (a) a typology of actors; (b) an overview of key features of the dual-use industry divided by the main areas of dual-use (chemical, biological, nuclear and conventional dual-use and related delivery systems) including a discussion of cross-links; as well as the cyber-surveillance sector. It also discusses the diverse transport sector and explores the way it is affected by the control requirements for transit movements introduced with the 2009 EU Dual-use Regulation and how it may be impacted by certain review actions.

Types of impacts considered in the data collection

Data and information were collected with regard to the economic, social (including security and human rights) and environmental impact of the current system and review options. Economic impacts include the administrative burden for companies and public authorities (adjustment, compliance and transaction costs), as well as trade and reputational effects for companies. To the extent possible and where relevant, information was also collected on indirect economic impacts relating to investment and production; innovation and research; and effects on the level playing field. In all areas, particular attention was given to effects on small and medium-size enterprises (SMEs). When assessing social impact, the study considered security and human rights issues as well as employment. The initial scoping, which indicated that the environment does not appear to be significantly affected, was confirmed during in-depth interviews for the case studies. This, therefore, is not a main focus of the study.

In collecting data on the impact of the current system and of the review options, SIPRI and Ecorys looked at the question of who is affected when assessing the magnitude of impact (neutral, small or significant) on different sectors and types of companies (e.g. multinationals and SMEs).

The data and analysis presented are intended to assist the European Commission in assessing the social, economic and environmental impact of the existing regulatory system and the different review options. A summary of findings on each of these issues is presented. Human rights and security impacts are naturally difficult to measure. Environmental impact was not identified as a major issue in the surveys or the interviews.

Scope of the analysis and data sources

EU and sector-wide data have been gathered based on: (a) public statistics on trade, production, employment and number of enterprises, using the EU correlation table;[1] (b) licensing and export data provided by EU Member States in the context of an annual data exchange process and made available for this study,[2] complemented by additional detailed data provided by two Member States; and (c) data provided by companies and industry associations through interviews and online surveys.

During the inception phase, given the range and diversity of products affected by the EU's dual-use export controls, we assumed that we would need to narrow down the quantitative analysis to specific sectors. However, initial analysis and interviews showed that: (a) trade was concentrated in a more limited number of products than expected; (b) business associations showed a general willingness to cooperate

[1] The correlation table prepared by DG TAXUD seeks to correlate customs codes with EU control list entries that may covered by these codes (see Chapter 4).

[2] The EU-wide data on export licences was collected by the European Commission's Joint Research Centre in the context of the annual 'Data exchange questionnaire on the implementation of regulation 428/2009'. The data is shared by EU Member States in the context of the Dual-Use Coordination Group (DUCG). The data is used by the European Commission in aggregated format in public documents, such as the reports to Council and Parliament on the implementation of the Regulation or the Annual Reports on the activities of the DUCG.

through the provision of data and information; and (c) Member States were willing to share data that allowed the cross-checking of trade analysis data through licensing data for all EU Member States as well as through two cases studies. This allowed us to cover almost the entire dual-use sector in our analysis.[3]

The sector case studies on the machine tool, chemical and aerospace industries are designed to illustrate how different sectors are affected by EU dual-use export controls, and to complement the results of the data analysis and the surveys. The selection of case studies was based on the following criteria: (a) the size of the sector in terms of turnover and employment; (b) the proportion of products covered by the EU's dual-use export controls; (c) the overall volume and value of dual-use related exports; (d) the number and value of export licences; (e) the expected impact of the export control review; and (f) the availability and quality of the data. Due to the limitations of some of the criteria (in particular the general data limitations explained in Chapter 2), some more practical considerations, such as availability of interviewees, have been taken into account as well.

The impact of review options and associated actions is assessed in qualitative terms and where possible, we also applied quantitative approaches (based mainly on the responses to the survey questions to companies and associations).

Quantifying the size and scope of the EU's dual-use industry

This report includes the results of the data analysis conducted on the basis of public statistics and licensing data as indicated above. However, all data sources suffer from severe limitations. For public statistics, these limitations mainly stem from the difficulty to isolate dual-use items in the data, due to the use of different product classifications. As a result only a broad estimate of the size and scope of the dual-use sector in the EU is provided in this report.

Licences issued by EU Member States for the export of dual-use items to extra-EU destinations were worth approximately €50 billion in 2013. However, customs trade statistics indicate that the upper threshold value of *dual-use related* exports of goods in 2014 (which has been referred to as the 'dual-use domain') was approximately €476 billion to extra-EU destinations and €623 billion to intra-EU destinations.[4] The selection of Harmonised System (HS) codes used to generate this data was based on the DG TAXUD correlation table, which links dual-use items to customs product codes.

This total amount of €476 billion is substantially larger than the total figure for export licence data, mainly because the corresponding HS codes also contain many—and in numerous cases even mostly—non-dual-use products. According to research by the European Commission's Joint Research Centre (JRC), the dual-use industry measured according to customs codes correlations could be overestimated by a factor of approximately 6.2. Using this factor in our analysis, dual-use exports would be around 3.9% of total EU exports, or close to €180 billion. A case study using Dutch customs

[3] The data analysis focuses on those ten product categories that account for 90% of total dual-use related exports, while the survey was open to all relevant sectors.
[4] The Eurostat COMEXT database.

data shows that for the Netherlands actual dual-use exports are almost 13 times smaller than dual-use related export data suggests, resulting in dual-use exports accounting for 2.3% of total extra-EU exports.

The ten sectors that export the highest value of dual-use related goods represented 90% of the total export value and 74% of the total number of Annex I dual-use codes for which a corresponding Combined Nomenclature (CN) classification exists (in the correlation table). Amongst these top-10 sectors, the *machinery and mechanical appliances (HS-84), electrical machinery and equipment (HS-85)* and *aircraft & spacecraft (HS-88)* represent the most important industries from the perspective of exports of dual-use related goods (comprising 32%, 18% and 12% by value of the total in 2014).

The analysis of domestic EU dual-use related production, employment and enterprises suffered from an even greater lack of detail in the sectoral disaggregation of the data, so that the data for these indicators is likely to be even more overestimated than the dual-use related export data based on the correlation table. According to our analysis, production in dual-use related products in the top-10 sectors (based on extra-EU export value) in the EU equalled more than €600 billion in 2013. If we correct for the overestimation of dual-use related exports based on customs data (which is estimated to be a multiplier of 6.2 by Versino (see Chapter 4), the production in 2013 is approximately €102 billion. A 2015 study by King's College London finds that for most PRC product codes (the PRODCOM classification) only 2-5% of production is dual-use related, and estimates the total dual-use production value in the EU at €27 to €36 billion in 2013 (see Chapter 4).

The cyber-surveillance sector

Recently steps have been taken to place stronger controls over the export of cyber-surveillance technologies at the EU and Wassenaar Arrangement level. There is no agreed definition for the cyber-surveillance sector. This report defines it as lying at the intersection of the information and communications technology (ICT) sector and the surveillance sector. Hence, cyber-surveillance goods, services and technologies are ICTs that are specifically designed, in whole or in part, for surveillance purposes.

The report gives an overview of the size and composition of both the ICT sector and the surveillance sector, as well as a brief assessment of how each is affected by EU dual-use export controls. It then focuses more closely on particular cyber-surveillance technologies. These include, but are not limited to, the following technologies: Mobile telecommunications interception equipment; Intrusion software; Monitoring centres; Lawful Interception (LI) systems and data retention systems; Biometrics; Digital forensics; Location tracking devices; Probes; and Deep Packet Inspection (DPI) systems.

The contours of the cyber-surveillance sector are not clear. A number of companies—including a large number of SMEs—are exclusively engaged in the production of one or more cyber-surveillance technologies (so-called 'pure players'). Meanwhile, a number of larger defence companies do so alongside a broader spectrum of cyber and non-cyber surveillance and security solutions. Finally, a number of companies—including a large number of SMEs—produce technologies with both surveillance and non-surveillance applications.

The size of the cyber-surveillance sector is also not clear. In 2011 it was estimated that the global 'mass surveillance' industry was worth $5 billion a year. However, the basis for the figure is unclear and it has not been updated since. A number of other studies have also been produced that focus on particular cyber-surveillance technologies. However, these studies are difficult to compare and combine due to uncertainties and differences in the methodologies used.

The different cyber-surveillance technologies identified by the study vary significantly in a number of areas, including: (a) the extent to which they have non-surveillance applications; (b) whether or not they are currently affected by EU dual-use export controls, (c) the range of security and human rights concerns attached to their export and use; (d) how extensively they are used by EU Member State law enforcement agencies (LEAs) and intelligence agencies; (e) whether or not there are agreed standards relating to their use; and (f) the number and type of EU and non-EU based companies that are engaged in their production.

All of these differences have implications for the current impact of dual-use controls and the potential impact of the different review options.

As a result, we adopt a case study approach, whereby a selection of cyber-surveillance technologies is the focus of more detailed analysis. In doing so, we concentrate on cyber-surveillance technologies that have been of most cause for concern in relation to human rights and security concerns, and which are currently affected by EU dual-use export controls or the focus of discussion in relation to future expansion of controls. The case studies therefore are on: (a) mobile telecommunications interception equipment; (b) intrusion software; (c) monitoring centres; (d) lawful intercept data retention and mediation systems; and (e) biometrics.

Each case study gives: (a) a definition of the technology; (b) a description of how it is captured by EU dual-use export controls; (c) examples of human rights and security concerns linked to its export and use; (d) an analysis of the producer companies inside and outside the EU; (e) the number and type of EU and non-EU based producer companies; and (f) an analysis of the current and potential regulatory burden for governments and industry created by the application and potential expansion of export controls in this area.

Stakeholder consultation

The stakeholders consulted include: industry (EU-wide associations, national associations and companies—both SMEs and multinational companies); academia/research institutes; EU officials; Member State officials (licensing and enforcement); and non-governmental organisations. Research methods used were online surveys/questionnaires and in-depth interviews with key stakeholders, using a sampling approach. In addition, information was collected in conferences and seminars, as well as in meetings that took place alongside these events.

Three online surveys were designed and implemented: for business associations (EU-wide and national); companies; and licensing authorities. Jointly with the European Commission, a complementary questionnaire on cyber-surveillance issues was sent to EU Member States.

Stakeholder consultation results regarding economic impact

Compliance costs for business

Most companies have an internal compliance programme (ICP) in place, whether it is formal or informal. Costs related to complying with dual-use export controls do not only relate to the costs of applying for licences, but there are also other types of costs to be considered (e.g. for related software and databases). The amount and types of costs seem to be determined more by the size of the company rather than the sector it operates in. Finally, the survey found that costs can differ for each company and that companies do not have information on compliance costs readily available.

Administrative costs for authorities

The total budget of the export licensing authority (as per Art.9 of the EU Dual-use Regulation) differs considerably from one Member State to another, both in terms of total budget and the share of this budget spent on dual-use export controls. The budget spent on dual-use export controls varies from less than €100,000 to almost €6 million per year. This is likely due to variations attached to the importance of the dual-use industry in each country, the extent to which these products are exported outside the EU and the number of dual-use licence applications. Similarly to what we found for business, staff at licensing authorities also spend a lot of their time on activities other than issuing licences. The staff resources of other government authorities involved in dual-use export control were substantial. Resource constraints emerged as the top challenge in the implementation of dual-use export controls.

Competition and sales

Although compliance costs are directly affected by the Dual-use Regulation, they can also lead to more indirect costs, such as those associated with waiting times. When a company is unable to obtain a licence, this has a direct effect on trade, and more indirectly also on production. Given that this also does not occur often, this effect is likely to be small. However, compliance costs can also be generated by the 'friction' created by the application of export controls. In particular the process of requiring customers to sign and comply with end-use certificates can have an inhibitive effect on the search for new business.

The costs related to compliance can in turn impact on trade, production and investment, because of distortions of the level playing field. The degree to which this is the case differs however, depending on the specific product and the competition from third countries. At the same time, competition is not only determined by these factors, as issues like quality and reliability also play a key role. The more technologically advanced a product is, usually the price is less of a key determining factor for the purchasing decision. Even within sectors there can be big differences depending on the specific product, and hence it is difficult to make general assumptions on the effect of dual-use export controls on competition and sales.

With respect to the *level playing field* within the EU, several stakeholders have indicated that there are implementation differences between Member States. This can lead to differences in: (a) the time needed to obtain a licence; (b) the ease of obtaining a licence; and (c) the circumstances under which a certain type of licence (individual, national general or global) is offered. In some cases a company was unable to obtain an export licence, while a company from another Member State was able to do so. However, these cases appear to be exceptions rather than the rule. There are also third countries which can supply dual-use items, but which do not face (similar) export controls. This can put EU suppliers at a competitive disadvantage.

According to those interviewed, dual-use export controls play a very small role in the decision to invest. No examples were found of activities being relocated outside the EU to avoid dual-use export controls. While several reports have noted that companies have left the EU as a result of stronger export controls on cyber-surveillance technologies, the number of documented cases where this has happened remains small. In addition, concerns have been raised about the unintended economic and social impacts of stronger controls on cyber-surveillance technologies, particularly intrusion software. However, these effects are hard to quantify.

Reputation did not emerge as a major factor from the consultations affecting sales and in particular exports. However, certain companies involved in the production and export of cyber-surveillance technologies did note the benefits that can be associated with having your products subject to export controls. In particular, compliance with export controls can form part of a wider process of building the reputation of a company as a responsible actor. Moreover, having your products subject to export controls can help to provide political and economic support should a contract need to be cancelled because of misuse of the product by the end-user. However, such views are far from universally held and other companies in the sector appear equally keen to focus only on the negative impacts of being subject to export controls.

Research and innovation

Half of the companies work with academia and research institutes and, according to one third of them, export controls affect this cooperation and the innovative capacity of the company. Large enterprises indicated that they are affected more often than SMEs.

Potential impact of review options

Given that no details are known about the review options, we cannot quantify the effects of the different review options and the consequences will also vary considerably according to the type of company. Nevertheless, a number of insights into impact emerged from the consultations. For example, legal requirements are likely to affect larger companies less than SMEs. EU General Export Authorisations (EUGEAs) for intangible transfers of technology (ITT) are also likely to reduce compliance costs more in multinational companies than in SMEs. The majority of respondents expected the introduction of an EUGEA for low value shipments, encryption and ITT to have a positive effect on exports, production and investment, and the level playing field. The introduction of an EUGEA on ITT or other ways to facilitate intra-company knowledge transfers is considered to have a positive or very positive effect on research and innovation. A significant level of unease was expressed about the application of human security principles when assessing exports of cyber-surveillance technologies and an expansion of controls in this area. Companies noted the lack of a clear definition of 'human security' and the risk that these steps would place EU companies at a competitive disadvantage.

Licensing authorities highlighted that most of the review options would have implications for staff resources: in some cases positive (e.g. more EUGEAs), and in some cases negative (strengthened ITT controls and enhanced information exchange among EU Member States). At the same time, some of the cost savings were expected to have a negative impact on security (see below), thus potentially presenting a trade-off between two different types of impact.

Stakeholder consultation results for social impact

Security – company perspectives

28% of the associations indicated that the use or consumption of dual-use items generate positive effects on security. About half of the companies that produce cyber-surveillance technologies are aware that exports of these technologies from the EU and from third countries may pose a security threat or a risk of human rights violations. Self-regulation, an electronic list of blacklisted customers or institutes, clear rules on modern IT infrastructure and increased clarity in legislation were considered to have a strong positive security impact.

Security and human rights – perspectives of licensing authorities

Security and human rights would benefit from all the review actions under the option 'implementation and enforcement support'. The actions proposed to achieve catch-all convergence would have a positive impact on security and human rights. The actions proposed to optimise the licensing architecture, such as additional EUGEAs would negatively impact security and human rights, while legal clarifications and amendments would have a general positive impact on each aspect. A critical re-evaluation of intra-Community transfers is expected not to have an impact on security, and for human rights a neutral to slightly negative impact.

Stakeholder consultation results for environmental impact

Environmental impacts were found to be largely indirect, either stemming indirectly from production or from the use of the dual-use item. Overall, they were not found to be significant, although few stakeholders could provide details on this aspect.

1. Introduction

The EU dual-use export control system is currently undergoing a review, as foreseen in the EU Dual-use Regulation 428/2009. As part of the review process the European Commission in April 2014 adopted a Communication 'setting out concrete policy options for the modernisation of EU export controls and their adaptation to rapidly changing technological, economic and political circumstances'.[5] Before proposing amendments to current legislation, the European Commission will further consult stakeholders and also conduct an impact assessment. This study supports the impact assessment through the collection of data and information as well as analysis.

SIPRI implemented the project jointly with Ecorys. At the kick-off meeting on 6 January 2015, SIPRI/Ecorys presented the key elements of their approach. At the Impact Assessment Steering Group (IASG) meeting on 2 March 2015, SIPRI/Ecorys presented the inception report, which gave a detailed description of the proposed approach to project implementation (including a plan of activities and outputs); the methodology and data sources to be used, as well as the work plan; clarification of the scope of work; a draft list of stakeholders to be consulted and a consultation plan; and a draft questionnaire and interview plans. The revised and approved inception report thus concluded Action 1 ('Development of a methodological approach').

The interim report submitted in June 2015 included a first draft of Action 2 ('Analysis of the baseline scenario') by presenting data and information on the structure and performance of directly affected sectors. It also presented a first draft of Action 3 ('Analysis of the review options and corresponding review actions'). These first drafts of Actions 2 and 3 were based on the data collected in the scoping phase, through desk work, analysis of public statistics and statistics provided by Member States, as well as the results of the first round of interviews with industry associations. They were further developed through the data gathered in the consultation process (i.e. surveys and further interviews).

This report concludes the project and summarizes the results obtained. It includes an explanation of the methodology (Chapter 2); a conceptual overview of the dual-use industry and identification of affected sectors (Chapter 3); a quantitative assessment of the EU dual-use industry (Chapter 4); an analysis of the review options (Chapter 5); stakeholder perceptions of the EU's dual-use export control policy and the review options [resulting from a business survey and additional insights from interviews] (Chapter 6); a chapter dedicated to the cyber-surveillance sector (Chapter 7); additional case studies (Chapter 8); and the conclusions, including an overview of the impact (Chapter 9).

The project was managed by Sibylle Bauer (SIPRI), who was also the lead author on chapters 3 and 5, with contributions from Peter Clevestig and John Hart on biological and chemical issues. Mark Bromley (SIPRI) had overall responsibility for the cyber-surveillance aspects of the study and was the lead author for Chapter 7, which he co-

[5] European Commission, 'Communication from the Commission to the Council and the European Parliament, The Review of export control policy: ensuring security and competitiveness in a changing world', COM(2014) 244 final, Brussels, 24 April 2014.

authored with Vincent Boulanin, with research support from Reint-Jan Grootnuelend, Hyuk Kim and Maaike Verbruggen. The Ecorys team was led by Nora Plaisier. Francesca Berton contributed to the case studies and the analysis of the surveys, while Jurgen Vermeulen implemented the data analysis contained in Chapter 4. Other specific contributors are credited in the relevant sections.

2. Methodology

2.1 Overview of methodological approach and implementation

The overall aim of this study is to support the European Commission's impact assessment by providing as much factual data and information as possible on the EU dual-use industry, the impact of the current regulatory system and the expected impact of the review options. A challenge for this study is the lack of publicly available data on the topic. This is partly due to commercial confidentiality, the variety of the sectors involved, and because systematic data collection that accurately maps the size and composition of the dual-use sector at the EU-wide level has not been prioritised by the EU, national authorities or industry associations. This affects the type of quantitative analysis usually done in the framework of impact assessments. The project has therefore chosen a combination of different methodological approaches to quantify and qualify the dual-use industry and the potential impact of the review options. The elements include:

1. Desk work: (a) literature review; (b) analysis of trade statistics, in particular COMEXT data based on the correlation list, and verification of results with the European Commission's Joint Research Centre (JRC) and the World Customs Organization (WCO), and cross-checking against additional national data obtained from two Member States; (c) analysis of production statistics, in particular PRODCOM data based on the correlation list; (d) analysis of statistics on employment and number of enterprises, in particular Eurostat's Structural Business Statistics (SBS) based on the correlation table; (e) analysis of licensing data provided by EU Member States for the purpose of this study, to be used in aggregated form,[6] complemented by customs data for one Member State (the Netherlands).

2. Stakeholder consultation process: (a) Initial stakeholder consultations through identification of relevant associations and in-depth interviews with associations, as well as discussions with company and Member State representatives; (b) regular briefings of the Dual-use Working Party (DUWP), Dual-use Coordination Group (DUCG) and Surveillance Technology Expert Group (STEG) sub-group; (c) semi-structured interviews with a range of key stakeholders, including industry associations, companies, EU officials, Member State officials (licensing and enforcement), non-governmental organisations and academia; and (d) data collection through on-line surveys/questionnaires: two for industry and two for officials.

3. Case studies: Case studies complement the insights gained from the data analysis and stakeholder consultations, based on additional data collection on the size and scope of the industry and in-depth interviews. Two case studies had already been identified in the inception phase: one on the cyber-surveillance 'sector', as new controls may be placed on this sector and it was given the weight of a review option of

[6] The data on export licences was collected by the European Commission's Joint Research Centre (JRC) in the context of the annual 'Data exchange questionnaire on the implementation of regulation 428/2009'. The data is shared by EU Member States in the context of the Dual-Use Coordination Group (DUCG). The data is used by the European Commission in aggregated format in public documents, such as the reports to Council and Parliament on the implementation of the Regulation or the Annual Reports on the activities of the DUCG.

its own in the Commission Communication; and the other on the transport sector, as this sector is also affected by dual-use trade controls, especially since Regulation 428/2009, and is likely to be affected differently than producers. Based on the initial findings we conducted further case studies: on the biological sector, as this sector illustrates the issues of cooperation with academics and intangible transfers of technology (ITT); and on three important economic sectors: chemical, machine tools and aerospace. (For the selection of these sectors, see 2.5 below.) In addition, we conducted a national case study based on customs data in the Netherlands, where we looked at data available at Member State level and how it compares to what is available in public statistics.

Given the variety of sectors affected by controls, the project was asked to consider all relevant economic operators and their various activities in controlling exports, including ITT, transit and brokering. The multi-pronged methodological approach presented above seeks to capture this diversity of actors and activities.

2.2 The range of impacts considered

In collecting data aimed at assessing the impact of the current regulatory framework and the various review options the study focused on a range of potential economic, social and environmental impacts. Table 2.1 summarizes the range of potential impacts that were taken into consideration. The study distinguished between *direct* impacts and *indirect* impacts, which may materialize as a secondary by-product of the direct impacts. In all cases, the study paid particular attention to the impacts on SMEs, as they may be disproportionally affected by dual-use export controls. Thus, in identifying impacts the study always sought to distinguish between SMEs and larger companies.

2.2.1 Economic impacts

Direct impacts

- *Trade/ trade barriers:* The application of dual-use export controls may make it more difficult or easier to export dual-use items thereby affecting trade flows.
- *Adjustment, compliance or transaction costs for companies*: This includes the administrative burden generated by classifying controlled items, applying for export licences and setting up or implementing internal compliance programmes.
- *Adjustment, compliance and transaction costs for public authorities*: This includes the administrative burden generated by licensing assessments and outreach and enforcement activities.
- *Reputation of industry*: This includes the reputational effects for industry of being subject to export controls, particularly for companies in the cyber-surveillance section.

Table 2.1. Overview of potential impacts

	Impact	Economic	Social	Environmental
	Direct	• Trade/trade barriers • Adjustment, compliance or transaction costs for companies • Adjustment, compliance or transaction costs for public authorities • Reputation of industry	• WMD proliferation • Other threats to EU and Member State security • Human rights abuses in third countries	
	Indirect	• Investment & production • International competitiveness • Innovation & research/ITT • Level playing field	• Employment • Health and safety • Fundamental freedoms of EU citizens • Alignment of policy with EU values • IT security research • EU Member State capacities in law enforcement • Availability of key technologies for human rights activists in third countries	• Climate change, transport, resource use, waste generation, environmental risks

Indirect impacts

- *Investment and production:* If dual-use export controls make trade more difficult or increase costs this may lead to a relocation of investment and changes in EU production volumes. On the other hand, if they generate positive reputational benefits, this may increase demand and, indirectly, investment and production*.*
- *Innovation and research/ITT:* Any direct economic impacts of dual-use export controls may, in turn, reduce the funds available for investment in research and innovation. Secondly, dual-use export controls may affect the willingness and ability of universities to participate in research and innovation, to engage in international collaboration with non-EU universities, and to host non-EU students from countries considered sensitive from a WMD perspective.
- *Level playing field:* If EU Member States apply dual-use export controls differently at the national level this may distort competition. In addition, if costs for export controls become very high, it may create entry barriers.

2.2.2 Social impacts (including security and human rights)

Direct impacts

- *WMD proliferation*: The application of dual-use export controls is aimed at preventing or reducing the flow of items and technology to WMD programmes.
- *Other threats to EU and Member State security*: Controls on items that have applications in the field of conventional arms or certain types of ICTs may also reduce threats to EU or Member State security.
- *Human rights violations in third countries*: The application of dual-use export controls to cyber-surveillance systems that have been connected to violations of human rights in third countries may lead to their reduced availability and a reduction in human rights violations. However, companies manufacturing these technologies may leave the EU or companies based outside the EU may increase their exports, leading to the wider proliferation of these technologies and reduced oversight of their use.

Indirect impacts

- *Employment:* The application of dual-use export controls can affect both the amount and type of employment at the licensing authorities and in the companies within the different affected sectors. It could also affect employment opportunities of third country nationals.
- *Health and safety:* Dual-use export controls may have a positive impact on health and safety since they enhance oversight and awareness of risks in the field of bio-safety. Similar arguments could be made in the nuclear and chemical sectors, although awareness in those sectors tends to be much higher already. Restricting or delaying access to technology or materials under dual-use controls may also negatively impact the right to health.
- *Fundamental freedoms of EU citizens:* Dual-use export controls may have indirect impacts upon EU citizens' rights, as laid down in the 'Charter of Fundamental Rights of the European Union'. In the biological and pharmaceutical sectors, the application of dual-use export controls may have an impact on EU citizens' right to health care (Article 35) and academic freedom (Article 13). More broadly, dual-use export controls may also impact upon the freedom to conduct a business (Article 16).
- *Alignment of policy with EU values:* The EU has identified the promotion of human rights as a major foreign policy objective. Ensuring that the application of the EU's export controls reflects these commitments would contribute to the alignment of EU trade policy with these core principles.
- *IT security research*: Controls on cryptography and cyber-surveillance technologies—particularly controls on intrusion software—may inhibit the ability of the IT sector to conduct security research and therefore ultimately undermine cyber security.
- *EU Member State capacities in law enforcement*: Controls on cyber-surveillance technologies may lead to a reduction in the capacity of EU based companies in this area and potentially a reduced ability of EU Member States and other governments

to gain access to relevant technologies needed for the purpose of law enforcement and security.

- *Availability of key technologies for human rights activists in third countries*: Controls on cryptography and cyber-surveillance technologies may serve to block transfers of technologies needed to evade detection by national authorities that are used by human rights activists operating in repressive regimes.

2.2.3 Environment

Direct impacts

The study was unable to find any potential direct environmental impacts associated with the application of dual-use export controls.

Indirect impacts

- *Climate change, transport, resource use, waste generation, and other environmental risks*: For example, if an industry that is engaged in polluting activities experiences direct or indirect economic impacts due to dual-use export controls, this may have a positive environmental impact.

2.3 Methodological challenges

Collecting data that can be used to assess the impact of dual-use export controls posed significant problems, particularly with regards to indicators for social impacts. Human rights and security impacts cannot be measured in quantitative terms. Even economic impacts indicators, such as employment figures and compliance costs, are difficult to measure precisely with respect to 'the dual-use industry'. Dual-use employment figures are very rough estimates, because associations do not have these figures available, and even for companies this does not constitute a distinct product group for which figures are easily available. Even employment figures in the production of purely military items are difficult to measure.[7]

Generating data that could be used to assess the potential impact of the various review options also posed a number of challenges. Several factors limited the detail and disaggregation of data that we collected. They include (a) the complex, cross-cutting nature of dual-use issues in terms of industrial structure and internal company compliance efforts, and diversity of actors involved and (b) the number of review actions combined with their lack of concreteness at this point of the review process. Importantly, for many of the review options the question determining the economic and security impact is not whether they will be adopted and implemented, but how, as there are a number of ways to approach them.

As noted above, data on the dual-use industry is not readily available, mainly because the items covered by the dual-use list do not appear as such in EU statistics, which use different product and sector classifications. A correlation table developed by DG TAXUD is used to find the corresponding sectors in other databases, but in general,

[7] See SIPRI, 'Measuring arms production', <http://www.sipri.org/research/armaments/production/researchissues/measuring_aprod>.

this leads to a considerable overestimation of the relevant indicators (e.g. trade and production).[8] The limitations of the data are presented in more detail in the relevant sections (see Chapter 4).

In addition to data problems, some of the methods for quantitative analysis originally envisaged could not be applied. This is notably the case for the Standard Cost Model (SCM).[9] We proposed to apply the SCM for a selected number of companies in the baseline scenario, but even in this case the SCM could not be applied entirely. Following the SCM formula, the administrative burden is calculated on the basis of the average cost of the required administrative activities multiplied by the total number of activities performed per year.

However, in the analysis and collection of data, we noted that using the SCM model for only some individual companies would not be representative and therefore the usefulness of this exercise would be limited and possibly even misleading. The information collected through the survey as well as the additional interviews revealed the following issues that limit the applicability of the SCM: 1) in addition to variable costs related to each application, companies also face fixed costs related to compliance; 2) there is wide variation across companies on the costs related to compliance issues, which can be related for example to the size of the company, specific products exported or the type of licence required; 3) costs can vary per year, especially for smaller companies, as they depend on the specific transactions that year (e.g. more intra- or extra-EU exports), in particular for SMEs that export high-value products such as machine tools; and 4) many companies do not collect this data, and where they do, the data is not directly comparable as different methods are used and because it partly reflects salary differences between EU Member States rather than compliance priorities. Nevertheless, data on compliance costs has been collected and provides some indication of administrative costs for companies resulting from dual-use export controls.

2.4 Development and implementation of online surveys

2.4.1 Surveys for companies and business associations

Business associations were interviewed in the first phase of the research, followed up by additional consultations for those sectors that were selected for further research in the context of the cases studies and review options. The insights that emerged during the consultation phase guided us in designing the online survey on the export control policy review. Two separate questionnaires for business associations and companies were developed, and included questions on the characteristics of the sector/company, the baseline situation and the expected impact of selected review options, with specific attention to the cyber-surveillance sector.

[8] The correlation table is available at <http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153050.xlsx> or via the homepage of DG Trade <http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/>

[9] SCM is a method for calculating the administrative burden of regulations (among other things). For more information, see <http://ec.europa.eu/smart-regulation/refit/admin_burden/scm_en.htm>.

The majority of the questions included in the surveys were 'closed questions' for two reasons. First, these types of questions are easier and quicker for respondents to answer. Second, answers could be statistically analysed, whereas coding and comparing open responses would have been very difficult.

Full survey results are included in Annex 2 (a-c). The survey for business associations was completed by 70 respondents, of whom 25 reached the end of the survey (36%), while the survey for companies was completed by 539 respondents, of whom 282 reached the end (52%).

2.4.2 Surveys for EU Member States

In order to obtain information about the impact of the review options on Member States' authorities, a questionnaire was designed with input from EU Member States. At the request of some Member States, impact data was requested for all review options. The survey was designed to obtain information on the administrative burden of the current system and of potential changes, as well as on the social impact of the review options, notably security and human rights. It was presented at the Dual-use Working Party and subsequently sent to Member States in the form of an invitation to an online survey. 12 Member States participated.

The project also worked with the European Commission in drafting a questionnaire for export licensing officials focused on exports of cyber-surveillance goods, services and technologies. This questionnaire was focused on collecting data on licences issued for (and exports of) cyber-surveillance goods, services and technologies and the processes of assessing export licence applications in this area. The questionnaire was sent to licensing officials on 1 June 2015, together with the invitation to participate in the online-survey on broader review issues. 10 responded. The results have been integrated into Chapter 6.

2.5 Selection and implementation of case studies

To develop a better understanding of the impact of the Dual-use Regulation and given the diversity of sectors involved, we selected a sample group of sectors to develop the case study analysis. The following criteria were proposed in order to select specific sectors/products:

- Number and value of exports licences;
- Size of dual-use trade flows;
- Size of industry in terms of turnover and employment, and relative importance of dual-use;
- Expected impact of the export control review based on the initial data collection and the analysis of policy options; and
- Availability and quality of data.

Not all of these selection criteria could be applied and therefore the selection of case studies was also based on more practical criteria, such as the availability of interviewees. Based on these criteria, a few sectors stood out:

- Machinery/ machine tools;
- Electronic equipment;
- Aircraft/spacecraft; and
- Chemicals.

We looked into the following sectors/products in more detail, also based on sub-sectoral data and information provided by the business associations:

- Chemicals: This sector is one of the main EU manufacturing sectors, and one where multinationals are particular active. It is one of the main sectors covered by the Dual-use Regulation based on usage in weapon type and has also actively participated in the stakeholder events on export controls organized by the European Commission.
- Machine tools: This sector is important in terms of trade flows, comprises many SMEs and has indicated that almost all of its extra-EU exports are affected by export controls.
- Aerospace: This sector's products feature highly on the extra-EU trade data.

Within electronic equipment, ICT products are among the top extra-EU dual-use exports, like telephone sets (covering among others specific mobile radio telephones) and electronic integrated circuits. Since many ICT-related companies are already addressed as part of the cyber-surveillance analysis, we only selected the other three sectors for the case studies.

The in-depth interviews were conducted with 15 companies (operating in the machine tool, chemical and aerospace sectors) of which 20% were SMEs. Companies consulted are located in the following Member States: Austria, France, Germany, Netherlands, Spain and the UK. Moreover, in order to gain a broader and comprehensive view on the importance of dual-use and the impact of export controls at industry level, we conducted some interviews with EU-wide business associations representing these three sectors. More specifically, we consulted:

- CECIMO (the European Association of Machine Tool Industries);
- Cefic (the European Chemical Industry Council);
- Eurospace (the trade association of the European Space Industry); and
- ASD (AeroSpace and Defence Industries Association of Europe).

2.6 The cyber-surveillance sector

For the cyber-surveillance sector, the study conducted a comprehensive review of over 200 reports and news articles relating to the export and use of cyber-surveillance goods, services and technologies. Based on the results, the study collected information on over 80 cases where cyber-surveillance technologies exported from the EU have been connected with violations of human rights or threats to international or EU security. The study also collected information on over 250 companies based inside and outside the EU that produce cyber-surveillance technologies or that may be affected by export controls in this area.

In addition, interviews were conducted with the following stakeholders: (a) representatives of licensing authorities in those countries that are the more significant exporters of information communication technologies (ICTs) and cyber-surveillance technologies; (b) companies that are either engaged in exporting cyber-surveillance technologies or that might be inadvertently captured by controls in this area; (c) companies, academics and researchers working in IT security; (d) NGOs that have been engaged in highlighting the risks posed by exports of cyber-surveillance goods and services; and (e) Members of the European Parliament (MEPs) and representatives of EU bodies that are engaged with ICT and cyber-surveillance related issues.

3. Analysing the baseline: Defining the dual-use industry and identifying directly affected sectors

3.1 Conceptualising the dual-use industry and identifying affected sectors

As the European Commission's Export Control Review Roadmap highlights, the dual-use industry comprises a very wide range of industry sectors and actors including: 'energy, aerospace, defence and security, lasers and navigation, telecommunications, life sciences, chemical and pharmaceutical industries, manufacturing and material-processing equipment, electronics, semiconductor and computing industries'.

These entities may be structured according to: (*a*) items produced or exported; or (*b*) their uses (actual or stated). Defining the scope of the dual-use industry and its different components brings with it methodological challenges. One can argue that there is no dual-use industry as such, but there are different ways to delineate and conceptualise it—as reflected in the use of the term 'elusive dual-use sector' in Commission documents.

One possible categorisation of the different sectors is based on the dual-use items produced, as a function of their potential use or purpose according to certain weapon types: nuclear, biological, chemical or conventional weapons related dual-use items, since there are characteristics that can be identified. Missiles/delivery systems, which include certain types of Unmanned Aerial Vehicles (UAVs), are a cross-cutting category.[10] These areas broadly correlate with the international export control regimes, in which the control lists are agreed that have been consolidated into Annex I of the EU Dual-use Regulation.

There are a variety of cross-sectoral linkages and overlaps. For example, some chemicals have uses in nuclear weapons, missile systems or cyber-surveillance technology. We also consider the new category of cyber-surveillance technology, the inclusion of which in the dual-use list would entail a new or expanded definition of the current dual-use concept in Regulation 428/2009. Given its importance to the overall study, the cyber-surveillance issue is discussed in a separate chapter (Chapter 7).

The transport sector is part of the categorization exercise, also because it was newly impacted by the introduction of a transit control regime under the 2009 Dual-use Regulation. Moreover, the review options include the possibility of increased or harmonized transit controls (e.g. through EU-wide extension of add-on controls imposed by some Member States). As one stakeholder put it: 'we are normally the "forgotten" piece in the Export Controls regulations'. This sector is therefore given special attention in both the analysis of the baseline (Chapter 3) and the relevant review options (Chapter 5).

[10] The Australia Group provides a forum for the control of both biological and chemical dual-use items, while the Nuclear Suppliers Group is concerned with items that have applications in relation to nuclear weapons. Controls on WMD-capable delivery systems are discussed in the Missile Technology Control Regime. The Wassenaar Arrangement is a forum for the development of guidelines and control lists for conventional arms and dual-use items.

There are distinct differences between the biological, chemical and nuclear areas in terms of regulatory frameworks and the private, governmental and international stakeholders involved. However, all include producers and exporters of dual-use materials, equipment and technology.

The *chemical industry* is a very large industry comprising sectors such as printing, textile, plastics, pharmaceutical, food and cosmetics, all of which use toxic chemicals. The chemical sector has the peculiarity of extensive regulations based on health and safety considerations as well as oversight of imports and exports of some chemicals within the framework of the 1993 Chemical Weapons Convention (CWC). Some materials, equipment and technology are also subject to control through measures agreed in the Australia Group and implemented in Annex I of the Dual-use Regulation.

The internationally accepted and legally binding definition of a chemical weapon is that provided by the CWC. The definition covers toxins and multicomponent chemical weapon systems (including unfilled munitions and devices). The phrasing embodies a general purpose criterion (GPC), whereby all toxic chemicals and their precursors are prohibited except for permitted purposes. This is done to ensure that the CWC's legal prohibitions cover the possible development of new or 'novel' chemicals that might be used as a 'method of warfare'. In order to fully implement the GPC, states must consider the purpose for which the chemical is being sought, including whether it is for defensive evaluation purposes, or to support a standby chemical weapon capacity. This definition, which covers some potential biological warfare agents, therefore requires a broad monitoring and control system to track international flows of toxic chemicals and associated equipment and technology.

The *biological sector* includes pharmaceutical and biotech industries, waste management, diagnostic laboratories (hospitals), and agricultural and veterinary facilities. Importantly, it thus includes public and private sector actors and a range of entities that are not ordinarily the target of traditional industry outreach activities. Users of listed controlled technology also branch out to other industries such as the food processing and mineral/oil processing industries.

International transfers of biological agents notably include the exchange of materials within and between public sectors.[11] One aspect of the global disease surveillance system is the need for diagnostic and reference samples to be transferred between countries, regions and continents on a regular basis, which is fundamental in scientific exchanges. These in turn contribute to safeguarding both human and animal health.

The biotech service industries may present an additional layer of complexity as the steady decline of costs for basic and advanced biotechnological services provides both the private and public sectors with an attractive alternative of outsourcing expensive and time-consuming work. These international transfers are an essential element of risk mitigation. They simultaneously pose safety and security risks (e.g. when

[11] The downloading and sharing of DNA information for reproduction by so-called digital biological converters are the biological equivalent of 3-D printers. Venter has also characterized life as 'DNA software driven'. Venter, J. C., *Life at the Speed of Light: From the Double Helix to the Dawn of Digital Life* (Viking: New York, NY, 2013).

biological agents are transferred to regions where they are not common, or where a specific disease-causing agent is not endemic). In such cases, stricter containment infrastructure and controls (biosafety and biosecurity) are required.[12]

Furthermore, the EU dual-use control list of includes biological technology that has applications outside the traditional biological sectors, such as mineral oil and lubricant industry, food processing industries and others, which may complicate the identification of relevant importers or stakeholders (see also Figure 3.3).

The *nuclear industry* in the narrow sense is tightly controlled and subject to detailed security and safety regulations.[13] However, nuclear-related dual-use items with applications in a nuclear weapons programme (such as certain aluminium alloys) are produced in a wide range of industry sectors, many of which have mostly non-nuclear and civilian end-uses. While nuclear materials are subject to tight controls due to both security and safety risks, a broad range of nuclear weapon-relevant dual-use items in and of themselves pose no health nor environmental risks, and are thus only subject to export controls, but not production, import or transport regulations.

Companies producing dual-use goods, software and technology with applications in missile programmes and UAVs that could be used as *delivery systems*, come from different sectors, such as defence manufacturers, space technology and machine tools. Controlled items include specialised machines such as filament winding machines and isostatic presses, materials such as graphite and carbon fibre, as well as maritime navigation equipment and systems such as gyroscopes and accelerometers.

Conventional dual-use items fall outside the scope of WMD-related policies. They also fall outside of the scope of the Arms Trade Treaty (ATT), which entered into force on 24 December 2014.[14] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies maintains two control lists: one for conventional arms, and one for related dual-use items.

The Wassenaar dual-use list is divided up into 9 categories that illustrate the broad range of industries concerned or potentially concerned: Special Materials and Related Equipment; Materials Processing; Electronics; Computers; Telecommunications; Information Security; Sensors and Lasers; Navigation and Avionics; and Marine and Aerospace and Propulsion. These in turn are each divided into 5 sections: Systems, Equipment and Components; Test, Inspection and Production Equipment; Materials; Software; and Technology.[15]

Additionally, there are technical linkages as some categories of goods and technologies appear on both conventional and WMD control lists, and some

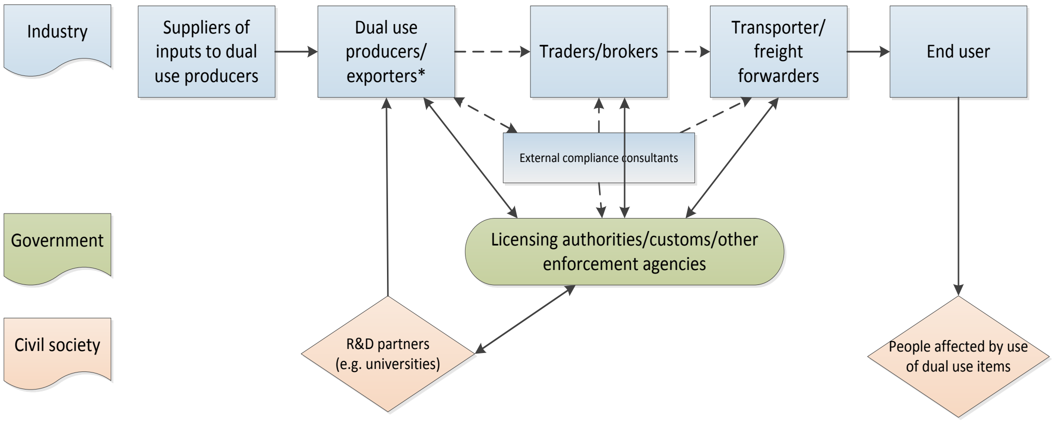
[12] See WHO, 'Biosafety', <http://www.who.int/topics/biosafety/en/> and Clevestig, P., *Handbook of Applied Biosecurity for Life Science Laboratories*, SIPRI: Stockholm, 2009.
[13] E.g., Swedish National Council for Nuclear Waste, *Nuclear Waste State-of-the-Art Report 2015: Safeguards, Record-keeping and Financing for Increased Safety* (Swedish National Council for Nuclear Waste [Kärnavfallsrådet]: Stockholm 2015).
[14] For details, see <http://www.un.org/disarmament/ATT/>.
[15] The Wassenaar dual-use list is available at <www.wassenaar.org>.

conventional arms can also be used to deliver WMD. Some items, such as machine tools and lasers, have both conventional arms and WMD applications.

3.2 Typology of actors and sector specific characteristics

To respond to the question of who will be affected by the review of the export control system the project seeks to identify the main players in the supply chain for dual-use items. Figure 3.1 below is a generic typology of actors.

Figure 3.1. Typology of actors


Industry
Suppliers of inputs to dual use producers
Dual use producers/ exporters*
Traders/brokers
Transporter/ freight forwarders
End user
External compliance consultants
Government
Licensing authorities/customs/other enforcement agencies
Civil society
R&D partners (e.g. universities)
People affected by use of dual use items

Note: *The exporter and producer are not necessarily the same, but may involve other players, like traders and transporters, as depicted by the dashed lines.

In all dual-use areas, stakeholders include private companies that produce, trade or use the relevant materials, equipment and technology. In some cases—notably in the biological field—there are significant actors in the public sector, including academia, and diagnostic and scientific laboratories. Many of the private stakeholders participate in associations, which are themselves key actors (e.g. due to their multiplier function).

In the biological area, stakeholders include the pharmaceutical and biotechnology industries and waste-management facilities. Diagnostic laboratories in hospitals and other health institutions (which can be public or private) and academia are also involved in the handling and international transfer of biological materials. Human, animal and plant pathogens are also present in veterinary or some agricultural facilities. Stakeholders in the life sciences have traditionally not been security conscious, which contrasts sharply against the culture in the nuclear sector. Military research facilities working on bio-defence projects are also highly relevant, although more security aware.

Key stakeholders in the chemical area are traditional companies that produce and trade in chemicals. The chemical industry includes a substantial number of companies, since chemicals are integral to industrial production and consumer products. There is a relatively high degree of safety awareness in the chemical industry, due to laws and regulations in both areas and well-known chemical accidents. Concerns are primarily accidents and environmental consequences. Security-related issues have become more prominent with the use of chemical weapons in Syria.

There is generally a high degree of security-awareness in the nuclear sector, partly due to accidents and previous use of nuclear weapons. The nuclear industry includes a limited, well-known number of stakeholders subject to strict safety and security regulation both within a country and for international flows (e.g. the International Atomic Energy Agency IAEA maintains a registry of all known civil and military nuclear facilities and associated reactor types). The nuclear industry includes the various designers and operators of nuclear power plants as well as various supplier organizations. Radioactive materials are also used in the medical field and in the food industry, among others.

A typology of actors in the transport sector is included in section 3.3 below. It should be noted that while an exporter would always deal with the licensing authority, the transport provider would usually not be in contact with the licensing authority, but deal exclusively with customs. According to stakeholder consultations undertaken in the framework of this project, brokering as defined by the EU in terms of third-country to third-country transactions appears not to play a very important role in the dual-use industry.

3.3 Transport sector

While the core of the transportation sector is basically the same as it has been for the last half century (air, sea, rail and road), developments in the last decade or so have seen these transport modes evolve and supplemented with additional modes of delivery.[16] These include pipelines, electronic data transfer, video conferencing and 3D printing/additive manufacturing. The majority of software programmes, manuals and blue prints are delivered digitally. 3D printing applications and capabilities are expanding.[17] Additive manufacturing will have important implications for dual-use export control, particularly on controlling intangible transfers of technology, since a number of items are expected to be transferred in this manner in the future: from the points of design to the point of production or end use, including engines and nucleotide sequences of biological agents. 3D printing of commodities will drastically reduce the costs of international transactions.

In spite of the increase in electronic transmission rather than physical transport, the classic transport sector is a growing industry, due to continued increases in world trade and globalisation. Predictions by the International Transport Forum are included below.

[16] This section is based on a background paper provided by Martin Palmer for this project.
[17] Computer Science Corporation (CSC), ‘Printing and the future of manufacturing 2012’, Fall 2012, <http://assets1.csc.com/innovation/downloads/LEF_20123DPrinting.pdf>.

Table 3.1. Global volumes by key transport mode (billion tonne – KM)

Year	AIR	SEA	RAIL	ROAD
2010	191	60053	4262	6388
2050	1111	256433	19126	30945

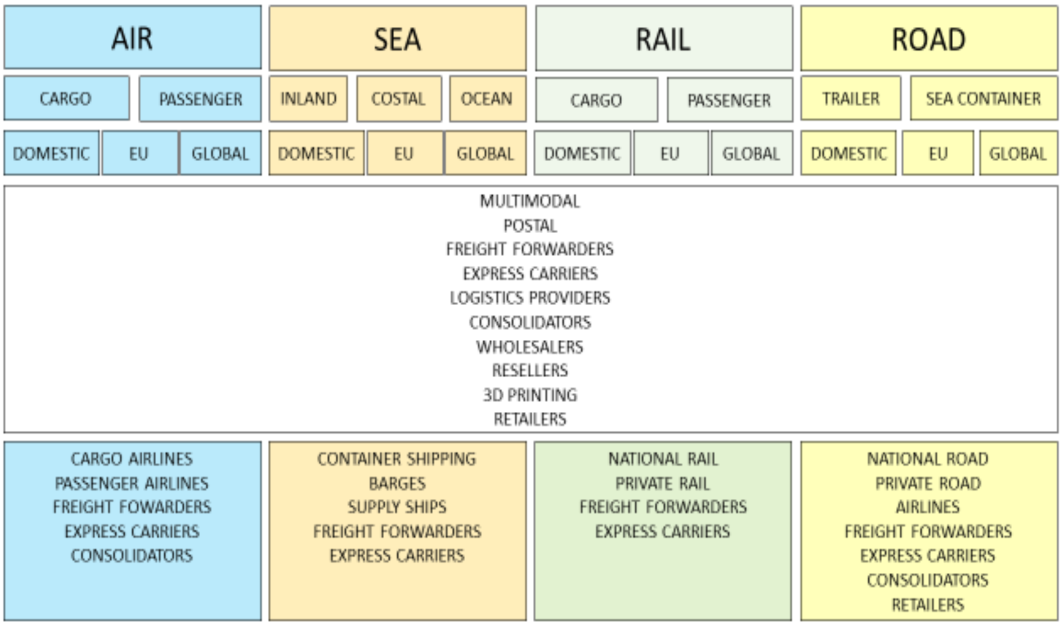
Source: International Transport Forum

The transport sector continues to evolve towards increased interdependence and overlapping of functions within the sector. For example, some freight forwarders operate container ships, while some container shipping companies own freight forwarders. Some postal organisations own express carriers, while express carriers own freight forwarders, etc. Postal authorities are an important part of the transport sector, complementing private sector transportation. These developments are driven by a constant push for faster delivery times and lower distribution costs.

The transportation or distribution sector provides various ancillary services in addition to the physical transportation of a commodity. These can include handling, packaging, customs processing, consolidations,[18] documentation, insurance and customs clearance. Especially for customs clearance, certain aspects of the actual and potential role of transport actors have to be kept in mind regarding compliance with transit, transhipment and export control provisions. First, export control provisions necessarily relate to other laws regulating the transit and export movement of goods, notably customs regulations. The role and responsibilities of transport providers are not specified in the EU Dual-use Regulation, but rather in customs law. Second, transporters (like traders) are not the manufacturer of the commodities and do not have expertise regarding the technical characteristics of the commodity. Third, the transporter relies on information supplied by the shipper from the country of export, supplier or manufacturer. Fourth, transporters often have thousands, even millions, of customers shipping between them tens of millions of commodities. Fifth, the transporter works with multiple jurisdictions and regulatory bodies globally, whereas the shipper works with regulatory bodies in the country of export. And finally, the transporter seldom acts as either exporter or importer of record or has legal ownership over the commodities transported.

[18] Consolidations are the process of bringing together shipments from a single or multiple shippers destined for multiple recipients, to create a single shipment to obtain reduced transport rates. The shipment is later broken down (de-consolidated) into its individual elements for delivery to the recipient.

Figure 3.2. Key components of the transportation sector



AIR
CARGO
PASSENGER
DOMESTIC
EU
GLOBAL

SEA
INLAND
COSTAL
OCEAN
DOMESTIC
EU
GLOBAL

RAIL
CARGO
PASSENGER
DOMESTIC
EU
GLOBAL

ROAD
TRAILER
SEA CONTAINER
DOMESTIC
EU
GLOBAL

MULTIMODAL
POSTAL
FREIGHT FORWARDERS
EXPRESS CARRIERS
LOGISTICS PROVIDERS
CONSOLIDATORS
WHOLESALERS
RESELLERS
3D PRINTING
RETAILERS

CARGO AIRLINES
PASSENGER AIRLINES
FREIGHT FOWARDERS
EXPRESS CARRIERS
CONSOLIDATORS

CONTAINER SHIPPING
BARGES
SUPPLY SHIPS
FREIGHT FORWARDERS
EXPRESS CARRIERS

NATIONAL RAIL
PRIVATE RAIL
FREIGHT FORWARDERS
EXPRESS CARRIERS

NATIONAL ROAD
PRIVATE ROAD
AIRLINES
FREIGHT FORWARDERS
EXPRESS CARRIERS
CONSOLIDATORS
RETAILERS

Source: Martin Palmer, Background paper on transport sector for this study

While the transportation sector is legally required to maintain defined compliance standards particularly in areas such as health and safety, the compliance programmes and standards for supply chain security are largely optional, and mainly driven by their customers' demands as part of the customer value added proposition and sales contracts rather than regulatory requirements. Within the EU, a number of supply chain compliance programmes and standards are in place, including: the United Nations Office of Drugs and Crime (UNODC) Container Control Programme, the EU Authorised Economic Operator (AEO), the Transported Asset Protection Association (TAPA) Air Cargo Security Standard and the International Air Transport Association (IATA) Secure Freight, as well as the International Organisation for Standardisation (ISO) standards and programmes. None of these programmes and standards covers the full spectrum of the supply chain, particularly in relation to dual-use commodities (i.e. they have been developed in 'silos'). Moreover, it is difficult for an authority or a business partner to identify a company that has obtained a particular standard, and once the transaction moves outside of the domestic (national) jurisdiction of the programme, it is difficult to recognise a compliance programme accreditation. In addition to participation in formal programmes or compliance with specified standards, most transportation companies have a formal or informal alert arrangement that will escalate to the responsible person anything that may appear unusual about a transaction. For transactions that do not raise any red flags, the transporter has to rely upon the documentation and information that has been supplied by the exporter.

Chapter 5 explores some of the implications of the current regulatory system and the review options for this sector.

3.4 Particularities of the biological sector

The biological sector clearly is directly affected by the EU Dual-use Regulation through the extensive list of biological materials, technology and equipment included in the EU control list. However, the biological sector 'exporting' controlled items is not only comprised of industrial actors, but also includes a wide range of public sector actors such as research institutes, hospitals and universities. While these may have some awareness of export licensing requirements for pathogens and biotechnology, awareness for potential licensing requirements for the export of intangible technology is likely very low. Where there is awareness, such requirements are controversial as it may be viewed as infringing on the freedom of research. Moreover, the EU Dual-use Regulation exempts basic or fundamental research (as opposed to applied research) from such requirements, but this term has been open to interpretation and has become the central issue in disputes regarding the publication of controversial Influenza A research (see Chapter 5).

A question that has been raised by stakeholders from the biological sector is how import and export restrictions may impact on Article 35 of the Charter of Fundamental Rights for the EU, which states:

"Everyone has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection shall be ensured in the definition and implementation of all Union policies and activities."

Restricting or delaying access to technology or materials under dual-use controls may impact the right to health under the Charter. Furthermore, the right to health is universal under a number of international treaties[19] and export controls may also have more wide reaching impacts to nations outside of Europe that have sub-standard health care systems (i.e. countries under embargos) and/or are in need of international emergency response and support during times of crisis.

Codes of conduct and awareness raising through education outreach have been a major international policy theme and strategy for strengthening oversight of the life sciences. Monitoring developments and establishing controls over synthetic biology has been a topic of much discussion in regards to biological security, including gene synthesis and oversight of trade regarding DNA segments, genes and whole genomes. Established in 2009, the International Gene Synthesis Consortium (IGSC), which currently comprises 7 partners responsible for approximately 80% of international commercial gene synthesis, implements screening procedures against such potential misuse. The companies involved rely on the 'know your customer' principle and a documentation system that permits questionable cases to be examined individually to confirm the end-use. The National Science Advisory Board for Biosecurity (NSABB), which is managed and supported by the US National Institutes of Health (NIH), has

[19] Treaties referencing the right to health include the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights and the Convention on the Rights of Persons with Disabilities.

identified 7 dual-use research characteristics of concern, such as reconstituting an eradicated or extinct biological agent, e.g. *variola major* (smallpox).

Since 2014 the NSABB has focused on gain-of-function (GOF) research involving pathogens with pandemic potential, such as Influenza A, SARS and MERS-CoV. GOF studies are defined as studies where modifications to a biological agent confers new or enhanced abilities to cause disease. This method is used to better understand the fundamental mechanisms of human-pathogen interactions. Understanding how such interactions work is important within research of biological agents that have pandemic potential, as it may assist in public health preparedness planning and in developing more efficient medical countermeasures (such as vaccines).[20] GOF is becoming more prominent in the context of export controls and also likely to be discussed and become an agenda item at the Eighth Review Conference to the BTWC in 2016.

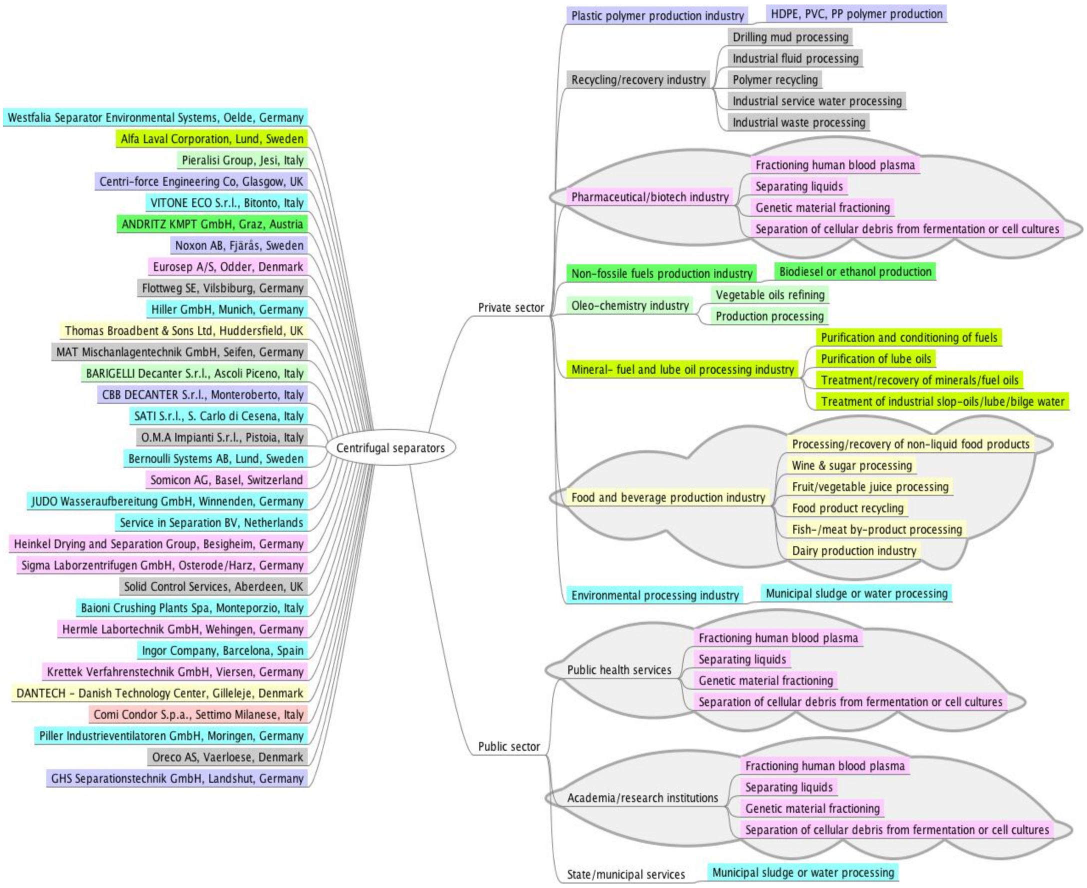
A baseline of EU life sciences facilities consists of high containment laboratories (BSL-3 and BSL-4), including isolation units suitable for the treatment of haemorrhagic fever patients under BSL-4 conditions. Some are located in the civilian sector and are members of the European Network of BSL-4 laboratories,[21] while others are in the defence sector (with possible working relations with civilian partners) and may include mobile capabilities for the transport of patients via air or land, or the deployment of laboratory infrastructure abroad via mobile laboratories in emergencies. Such facilities and capabilities may in principle be listed by EU Member States who choose to provide such information as part of their annual politically (not legally) binding confidence-building measures (CBMs) to the BTWC's Implementation Support Unit (ISU).[22] Italy's National Institute for Infectious Diseases (Instituto Nacional per le Male Infective, IMNI) heads the European Network for Infectious Diseases (EUNID) and carries the largest patient BSL-4 isolation capacity within the EU. EUNID is a project co-funded by the European Commission and has 16 EU Member States participating. It periodically carries out inventories of high-level isolation rooms (HIRs). In 2009 the EUNID found that HIRs were available at 211 hospitals in the 16 EU participating states with a total of 1789 beds.[23]

Another interesting sector for consideration is the DIY (Do-it-Yourself) bio or 'bio-hacking' community where both experts and amateurs are building makeshift laboratories in homes and public spaces to experiment with molecular biology. Such communities have rapidly expanded thanks to the increasing availability of biotechnology at low costs. Together with new biotechnology developments, such as within synthetic biology, the DIY bio community has become increasingly multi-sectorial with the inclusion of non-biologists, coming from engineering, art, sociology, IT and chemistry communities, where biology has been found to be a new and

[20] U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS, and SARS viruses. 17 Oct. 2014. Available at: <http://www.phe.gov/s3/dualuse/documents/gain-of-function.pdf>.
[21] See: <http://www.euronetp4.eu/>.
[22] UNOG, 'CBM returns', <http://www.unog.ch/80256EE600585943/%28httpPages%29/4FA4DA37A55C7966C12575780055D9E8?OpenDocument>.
[23] Fusco, F. M., 'Isolation rooms for highly infectious diseases: an inventory of capabilities in European countries', *Journal of Hospital Infection*, vol. 73, no. 1 (Sep. 2009), pp. 15-23.

interesting platform on which to build their work. The DIY bio community is both global and regional. Within the EU, the DIY Bio Europe science network, established in 2012, has developed its own codes of conduct in an effort to help guide its members in the safe and secure conduct of their work.[25] Also, the DIY bio movement has allowed the establishment of low-cost private start-ups in the biotech sector, which previously was beyond the economical and technical reach of most aspiring entrepreneurs.[26] The DIY Bio community and industry that emerges from this movement may present an interesting challenge for future export controls within and outside the EU.

Figure 3.3. Map of centrifugal separator manufacturers and applications in different sectors[24]


Westfalia Separator Environmental Systems, Oelde, Germany
Alfa Laval Corporation, Lund, Sweden
Pieralisi Group, Jesi, Italy
Centri-force Engineering Co, Glasgow, UK
VITONE ECO S.r.l., Bitonto, Italy
ANDRITZ KMPT GmbH, Graz, Austria
Noxon AB, Fjärås, Sweden
Eurosep A/S, Odder, Denmark
Flottweg SE, Vilsbiburg, Germany
Hiller GmbH, Munich, Germany
Thomas Broadbent & Sons Ltd, Huddersfield, UK
MAT Mischanlagentechnik GmbH, Seifen, Germany
BARIGELLI Decanter S.r.l., Ascoli Piceno, Italy
CBB DECANTER S.r.l., Monteroberto, Italy
SATI S.r.l., S. Carlo di Cesena, Italy
O.M.A Impianti S.r.l., Pistoia, Italy
Bernoulli Systems AB, Lund, Sweden
Somicon AG, Basel, Switzerland
JUDO Wasseraufbereitung GmbH, Winnenden, Germany
Service in Separation BV, Netherlands
Heinkel Drying and Separation Group, Besigheim, Germany
Sigma Laborzentrifugen GmbH, Osterode/Harz, Germany
Solid Control Services, Aberdeen, UK
Baioni Crushing Plants Spa, Monteporzio, Italy
Hermle Labortechnik GmbH, Wehingen, Germany
Ingor Company, Barcelona, Spain
Krettek Verfahrenstechnik GmbH, Viersen, Germany
DANTECH - Danish Technology Center, Gilleleje, Denmark
Comi Condor S.p.a., Settimo Milanese, Italy
Piller Industrieventilatoren GmbH, Moringen, Germany
Oreco AS, Vaerloese, Denmark
GHS Separationstechnik GmbH, Landshut, Germany
Centrifugal separators
Private sector
Plastic polymer production industry
HDPE, PVC, PP polymer production
Recycling/recovery industry
Drilling mud processing
Industrial fluid processing
Polymer recycling
Industrial service water processing
Industrial waste processing
Pharmaceutical/biotech industry
Fractioning human blood plasma
Separating liquids
Genetic material fractioning
Separation of cellular debris from fermentation or cell cultures
Non-fossile fuels production industry
Biodiesel or ethanol production
Oleo-chemistry industry
Vegetable oils refining
Production processing
Mineral- fuel and lube oil processing industry
Purification and conditioning of fuels
Purification of lube oils
Treatment/recovery of minerals/fuel oils
Treatment of industrial slop-oils/lube/bilge water
Food and beverage production industry
Processing/recovery of non-liquid food products
Wine & sugar processing
Fruit/vegetable juice processing
Food product recycling
Fish-/meat by-product processing
Dairy production industry
Environmental processing industry
Municipal sludge or water processing
Public sector
Public health services
Fractioning human blood plasma
Separating liquids
Genetic material fractioning
Separation of cellular debris from fermentation or cell cultures
Academia/research institutions
Fractioning human blood plasma
Separating liquids
Genetic material fractioning
Separation of cellular debris from fermentation or cell cultures
State/municipal services
Municipal sludge or water processing

[24] The map, contributed by Peter Clevestig, illustrates the complex chain of diffusion of listed dual-use technology. The map takes the example of centrifugal separators (listed under Annex I, 2B352c) identifying major manufacturers in Europe (left side) and identifying sectors and applications (right hand side) for the technology (colour coded). The figure highlights the key 'biological' sectors (circled) where such controls may be most relevant and illustrates that controls for this technology, and thus the impact of the control system, may have ramifications for other industrial sectors.

[25] See: <https://biohackspace.org/launch-of-diy-bio-europe/>.

[26] 'Garage biotech: life hackers', *Nature*, 6 Oct. 2010, <http://www.nature.com/news/2010/101006/full/467650a.html>.

Figure 3.3 above illustrates how widely dual-use technology in general is distributed in different public and private sectors, and that there may be exports that are easily overlooked as they do not relate to biological applications but may have the correct parameters in terms of volume and particle size separation. Many of these centrifuges may not be subject to licensing requirements. Identifying which product falls under export control would require detailed analysis and interviews with the companies' technical units, but all of them should be aware of the EU Dual-use Regulation.

4. Quantifying the size and scope of the EU's dual-use industry

A thorough understanding of the size and the scope of the industry involved in producing and/or exporting dual-use goods and technologies is crucial for assessing the impact of the review of the EU export control regime. For example, in order to understand the impact of changes in the review, the assessment should measure the potential impact on export volume, companies and employment. However, since dual-use items often concern very specific products or technologies and the data available on such socio-economic indicators is not available in the exact detail that is needed, sizing and scoping the EU's dual-use industry has proven very difficult. Nonetheless, since the European Commission's impact assessment would benefit even from partial estimates, this chapter explores the size and scope of the EU dual-use industry based on the best available data. It presents a quantitative assessment based on the following indicators and/or information:

- Section 4.1 Number and value of export licences;
- Section 4.2 EU dual-use industry in terms of dual-use related exports;
- Section 4.3 Case study on Dutch dual-use exports;
- Section 4.4 EU dual-use industry in terms of production;
- Section 4.5 EU dual-use industry in terms of employment and enterprises; and
- Section 4.6 EU dual-use industry from an international perspective

The indicators are sourced from different databases (more details in the sections below) using different product classifications, which inherently gives rise to difficulties in comparing the results. Moreover, the data analysis in general also suffers from a mismatch between the very detailed nature of dual-use goods or technologies and the aggregated nature of product or sector definitions in the databases used for this analysis. The case study on the Dutch dual-use exports sheds light on the extent of the mismatch between estimates of *actual* dual-use exports and *dual-use related* exports. In order to draw some general conclusions on the information gathered from a variety of databases, each with their own limitations, we conclude this chapter with a synthesis of the results and some aggregate conclusions on the size and the scope of the dual-use industry in the EU.

4.1 Number and value of export licences

An analysis of the export licence applications, authorizations and notifications is the most direct method of measuring the value and volume of the dual-use industry. While all EU-28 national licensing authorities collect this data, it does not provide the complete and full picture of the industry. For intra-EU trade, licences are only required for Annex IV items. For EUGEA E001 countries, only Annex II items need to go through a licensing process. Therefore, data used in this analysis will primarily focus on the rest of the world, where exports of all Annex I dual-use items need to be authorized. The data received confidentially from the EC for this study is sourced directly from these authorities, which receive the applications from exporters. The data is collected by the Joint Research Centre (JRC) in the context of the annual reporting process initiated in 2013, based on a 'Data exchange questionnaire on the implementation of regulation 428/2009'. Member States share this data in the Dual-use Coordination Group (DUCG).[27] Versino provides a comprehensive summary of the data, including a discussion on its limitations.[28]

In short, the data gives a rough picture of the real value of exports for which a licence was issued and thus, in turn, about the size of the dual-use industry. It is important to note that even issued licences do not reflect all exports, as a licence may be issued without some or all of the related business exchange taking place. Moreover, as mentioned before, not all dual-use items need to go through the export licensing process (e.g. only a subset of intra-EU or E001 countries trade). Similarly, there are also challenges concerning the licensing authorities' data that make the drawing of conclusions difficult. First, not all Member States systematically report applications as well as authorisations. For example in 2011 and 2012, the value of authorisations was higher than the value of applications, which shows that this data limitation could be significant for the EU as a whole. The most practical solution to this problem—as also applied by the European Commission in public reports—is to set the volume and value of applications at the same level as authorisations for those Member States that do not systematically report licence applications.

Secondly, the total value and volume of licences based on Annex I categories (Table 4.1b) differ significantly from the total value and volume according to total licences issued (Table 4.1a). The applications which include a data entry for the relevant Annex I category only covered about one third of total authorisations in that year. This suggests that not all licensing authorities keep track of the relevant Annex I categories or report this information. Sometimes licences also include multiple items from different Annex I categories, in which case the licensing authorities could be unable to attribute the share values to the separate Annex I categories. Lastly, the licensing data also includes General Export Authorisations as well as global licences for which the value authorised might not correspond directly to the value of actual exports under that licence. From this perspective, the licensing data represent an upper limit of the value of exports actually traded under the Dual-use Regulation. Despite these limitations, the data on the value and volume of export licence applications and authorisations handled by licensing authorities are a sound indicator of the scope of the administrative burden involved in implementing the Regulation.

Figure 4.1 and Table 4.1a summarise EU-28 aggregate licensing data, presenting both the total value and volume of the applications and authorisations as well as the

[27] The data is used by the European Commission in aggregated format in public documents, such as the reports to Council and Parliament on the implementation of the Regulation or the annual reports on the activities of the DUCG.

[28] Versino, C., 2015, '*Data views and comments on the Data Exchange Questionnaire for the year 2013*'. Presentation to the 52nd Dual-Use Coordination Group, Brussels, 10 March 2015.

detailed breakdown of the latter. Figure 4.1 shows that that—based on the reported data—the individual licence authorisations represent the largest share of the total value of authorisations in the years 2010-2013. In 2013, the individual licence authorisations represented 56% of the total. However, as explained in Versino (2015), only 19 Member States reported the value of global licence authorisations, whereas of the then-27 Member States reported individual licence authorisations. Therefore, in reality the share of global licence authorisations is likely to be higher than suggested by the figures presented here. Since individual licence applications are potentially the most burdensome to administer (comparing the value of licences granted and the effort involved from the licensing authorities), this information is important for assessing the impact of the review of the Dual-use Regulation. The fact that the total value and volume of authorisations has been increasing since 2010 is likely to be at least partly a result of improved data reporting by Member States over time, rather than an absolute increase in the value of dual-use exports.

Since we will also look into specific dual-use sectors and/or products in more detail, it is useful to try to distil as much information as possible on sectorial or product disaggregation from the licensing data. The information available from licensing authorities that comes closest to a sector disaggregation of licences issued, is the information on licences according to Annex I categories. Table 4.1b shows this detailed split for both value and volume of licences as at March 2015. However, as mentioned in the introduction, the information on Annex I categories does not seem to be systematically documented or reported. Thus the representativeness of this data is questionable. Based on the same data, the JRC calculated that approximately 33% of the available data on authorised licences had information on the Annex I category.[29] As a result, no firm conclusions can be drawn from this data. Due to these limitations, we also explore the sectoral and product level information based on customs trade data and production data in the next sections.

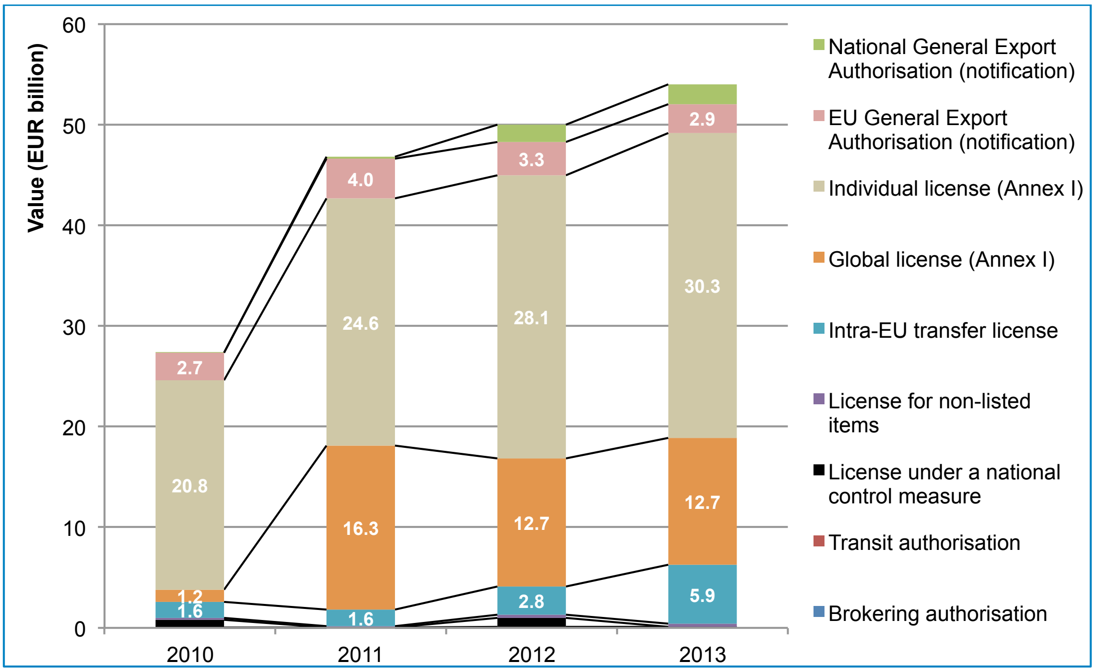
[29] Ibid.

Table 4.1a. Value and volume of export licences, 2010-2013

	2010	2011	2012	2013
Value of export licences handled				
General Export Authorisations (notification) (€ million)	2,725	4,123	5,046	4,828
Export licence applications (incl. Global) (€ million)	24,721	34,211	38,675	62,283
Export licence authorisations (incl. Global) (€ million)	24,616	42,681	44,959	49,207
Volume of export licences handled				
General Export Authorisations (notification) (number)	4,834	5,619	8,384	3,687
Export licence applications (incl. Global) (number)	31,538	32,231	32,880	34,926
Export licence authorisations (incl. Global) (number)	22,778	25,124	25,142	27,807

Source: Confidential data from EU licensing authorities

Figure 4.1. Development of value of export authorisations, by type, EU, 2010-13



Source: Confidential data from EU licensing authorities

]

Table 4.1b. Value and volume of licences according to Annex I categories as of March 2015

	Category	Value of licences *(€ million)*	Volume of licences *(number)*
0	Nuclear materials, facilities, and equipment	3,262	948
1	Special materials and related equipment	1,013	5,052
2	Materials processing	2,721	6,734
3	Electronics	2,370	1,844
4	Computers	6	45
5	Telecommunications and 'information security'	7,012	4,473
6	Sensors and lasers	843	2,518
7	Navigation and avionics	65	514
8	Marine	73	143
9	Aerospace and propulsion	219	327
	Total	**17,585**	**22,598**

Source: Confidential data from EU licensing authorities

4.2 Value and volume of dual-use related exports

Since a key aim of the EU's export control regime is to control the *export* of certain technologies and products, the indicator that comes closest to directly measuring the size and scope (in terms of types of products and technologies) of the dual-use industry is the *value of exports* for specific product categories. DG TAXUD has developed a correlation table[30] that relates the type of items that may require a licence for exporting them outside the EU (Annex I of the Regulation) to the corresponding customs trade code (in the HS or CN classification) for which detailed trade statistics are available. The trade analysis has the considerable advantage of being able to identify specific sectors and products that are most important in terms of export value. While this method is the most direct way of collecting trade data on the dual-use industry using publicly available data at the sector and product level. However, it also has important *limitations,* which need to be understood before interpreting the data:

[30] In this study, the latest available correlation table has been used, released on 1 Jan. 2015 and available at: <http://trade.ec.europa.eu/doclib/html/153050.htm>.

- The correlation is in most cases not unique: many dual-use items correspond to several HS codes, while at the same time specific HS codes often correspond to several dual-use items. There is thus not a one-to-one relationship, and this makes the analysis more complicated.

- Controls that apply to intangible transfers of technology do not correlate to the HS/CN customs codes, which cover only physical goods. There are also controls included in the list that do not identify specific goods, so that a correlation is often not even possible (e.g. for 1C101 — materials 'usable in' — a clear correlation to all related products is difficult).

- Some other (non-technological) controls also miss a direct and adequate match to a HS/CN product code as the product is not defined as such in the customs trade classification.

- Even the most detailed level of customs trade codes classification for which publicly available trade data is available (CN-8 in COMEXT) covers an aggregation of products that in most cases includes both dual-use items and items without a dual-use. As such, even though the TARIC correlation table identifies the very precise product codes that apply to the dual-use items, on the whole the classification will largely overestimate the actual value of dual-use trade. For most customs codes, only a small proportion of products covered by the customs code are likely to be subject to control under the Dual-use Regulation.

The overview of the EU's dual-use industry based on customs trade data presented below therefore needs to be interpreted with care. It is most likely that the dual-use industry sized according to customs trade data is overestimated since the effect of an eight-digit CN code also capturing non-dual-use related products is likely to dominate. As a result, this analysis identifies the maximum threshold of the size of the dual-use industry in terms of exports. It is also possible that the exporter has chosen a wrong customs code, perhaps intentionally, by mistake or through negligence. Still, aside from national customs data, if correlated with licensing data, customs trade data may be the best approximation of the dual-use industry from an export perspective.

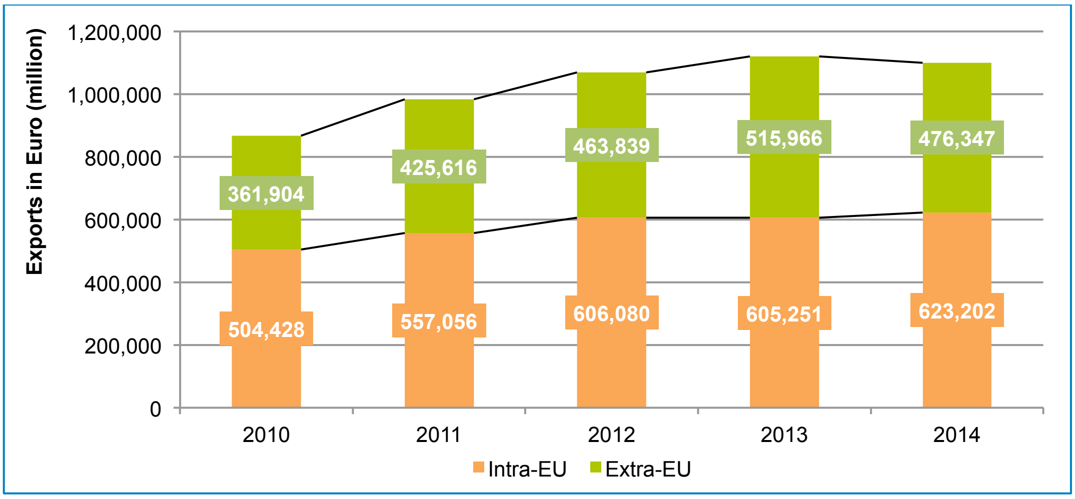
We have used the latest correlation table (released on 1 January 2015), which has matched the latest version of the Annex I categories of dual-use items to customs trade codes. Due to updates of the correlation table based on an evolving control list, regular amendments to the CN classification and potential methodological improvements that could change the correlation, the data in this section differs slightly from other estimates of the dual-use exports of the EU.[31] Section 4.2.1 presents the general size and trend in dual-use related exports, whereas section 4.2.2 presents the export flows for the top-10 sectors with the highest value of dual-use related exports.

[31] Compared to EC-JRC work, the correlation table used in this study includes more DU items. For example, the correlation table related to Regulation 388/2012 includes 1033 CN codes, the table related to Regulation 1382/2014 includes 1204 CN codes.

4.2.1 Size of EU dual-use industry according to customs trade statistics

Against the background of the limitations discussed in the previous section, Figure 4.2 presents the value of the dual-use related exports from the EU-28 to both intra-EU and extra-EU partners. As the graph shows, the dual-use industry is generally understood to represent approximately €1,100 billion in intra- and extra-EU exports from the EU-28 if we assume that the correlation table provides a 100% match. Approximately 40% of dual-use related exports are destined for extra-EU partners, which is the share of exports that is most relevant for the impact assessment of the review of the export control regime as these require a licence under the regulation.

Figure 4.2. Total value of dual-use related exports from the EU (Intra-EU; Extra-EU), 2010-2014



Source: EU COMEXT, Ecorys calculations based on 01-01-2015 correlation table

However, given the limitations presented in the introduction, to what extent do these estimates reflect the *actual* size of the dual-use industry? Compared with total exports of EU Member States, the dual-use industry represents approximately 24% (EU-28) in 2014.[32] Other available estimates (using older correlation tables but the same methodology)[33] indicate that the dual-use industry represents around 20% of total EU exports in 2013, including intra-EU exports.[34] This is thus more or less comparable. Based on that research the actual domain of total dual-use extra-EU exports that is potentially subject to applications for licences is estimated at 5.8% of total EU exports. This is the value of dual-use related exports to extra-EU countries that are not part of E001 General Export Licence destinations. Together with dual-use related exports intra-EU (11.6%) and to E001 countries (2.7%) this constitutes again total dual-use related exports. Since this study uses a similar methodology and arrives at a more or

[32] It should be noted that the EU has only had 28 Member States since July 2013, after the accession of Croatia. Data before this presented here also includes Croatia, but therefore EU trade flows in 2010-2013 are slightly higher than reality. However, given the small share of Croatia in total EU trade flows, this difference is only marginal.
[33] The study referred to uses the previous version of Annex I, namely Regulation 388/2012.
[34] Versino (note 28).

less comparable share of dual-use related exports, the estimated licence domain of 5.8% could also be assumed for the remainder of this study.

In order to estimate the share of *actual* dual-use exports, the JRC compared this share of 5.8% (which is the share of total exports in the EU subject to export licensing authorisation) to the total value of export licences granted by EU licensing authorities (€43 billion), which equalled 0.94% of total EU exports in 2013.[35] On this basis, Versino concluded that the dual-use industry measured according to customs codes could be overestimated by approximately 6.2 times and is more likely to be around 3.3% of total EU exports.[36] Using this multiplier on the data in this analysis, the *actual* dual-use industry based on total EU-28 exports could be approximately 3.9% (24/6.2) of total EU exports. Box 4.1 repeats a similar analysis using proprietary Danish licensing authority data.

The Danish Business Authority (DBA) in cooperation with Danish customs have collected data regarding the value of all the exports from 2012-2014, where Box 44 in the customs declaration is filled out, indicating that it is an export under a dual-use global license. In the cases where the Danish Business Authority did not find any customs data about the companies that have global licenses, the Danish Business Authority contacted the companies to collect the information on the value of the dual-use export, destination country etc. under their global license. The survey also includes ITT transfers, where the data is collected either from the DBA's own database on individual licenses or from information from companies on the export value of ITT exports covered by global licenses.

The case study in the next section of this chapter provides further analysis on the share of *actual* dual-use exports in the dual-use related product categories identified by the correlation table, using detailed customs data from the Dutch Customs Office.

Since this study also delves more deeply into the specific products and items that are most likely affected by the review of the regulation, it is worthwhile to examine the type of products traded in greater detail. Figure 4.3 shows the value of dual-use related exports by sector (at HS-2 digit level) to extra-EU partner countries in 2014. The top-10 sectors that export the highest value of dual-use items represent 90% of the total *value* extra-EU dual-use related exports from EU-28 Member States in 2014. This share has been relatively stable over the last five years. Also the sectors that comprise the top-10 have not changed over the last five years. In terms of *number of dual-use items*, these top-10 sectors jointly represent 74% of the total Annex-I dual-use codes with a correlation to CN codes as available in the 01-01-2015 correlation table. In the remainder of this chapter, we therefore consider the characteristics of these ten sectors in more detail in order to better understand the size and scope of the majority of the EU dual-use industry. For more information on the other sectors (based on HS classification), Table 4.2 (Annex 1) presents the value of dual-use trade in all HS sectors and their share in total dual-use trade.

[35] Ibid.

[36] Since the data from licensing authorities indicated that the total value of applications for export licences to non-E001 extra-EU partners equal to 0.94% of total EU exports, the customs trade data seems to over-represent the value by (5.8/0.94) = 6.2.

Box 4.1. Danish export licence data

In a recent survey, the Danish Licensing Authority collected internal licence authorisation data (on individual licence applications) as well as the value of exports cleared under a global licence. Building on this data and research conducted, we are able to assess the share of Danish dual-use exports as a share of total exports. The value of exports approved under the different types of licences available (except for EU general licences) as collected by the Danish Authority is presented in Table 4.3.

Table 4.2. Value of Danish exports with export control licence and value of dual-use related exports based on correlation table, 2014

Licence	Value (€ '000)
Catch-all licences	€ 1,987
Global licences	€ 29,818
Individual licences	€ 50,705
Total licenced exports	**€ 82,510**
Total extra-EU dual-use related exports 2014*	**€ 6,719,567**
Total exports 2014	**€ 83,558,696**
Licensed share of exports (as % of total exports)	0.1%

** based on the sum of the extra-EU 28 export value of the dual-use related CN codes sourced from the Jan-2015 correlation table*

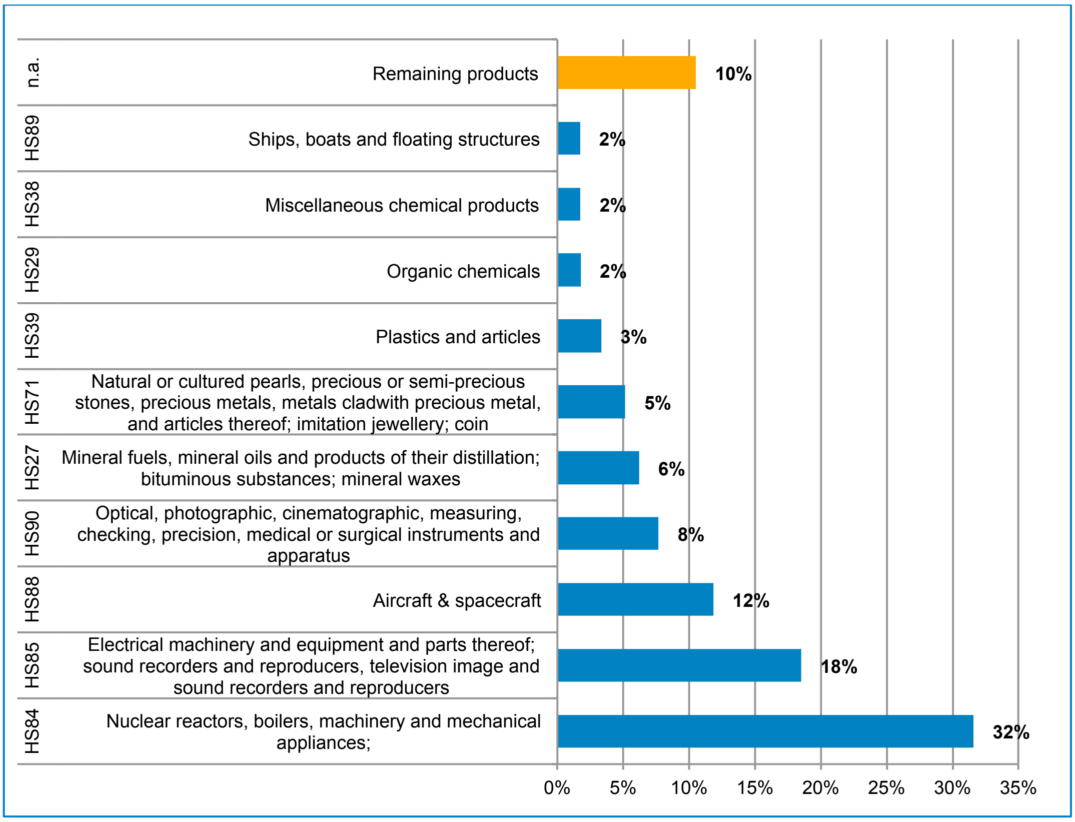
Source: Confidential data from Danish Licence Authority, Eurostat COMEXT

The value of export licences granted (excluding EU general licences) equalled €82.5 million in 2014. Using additional customs trade data, we are able to compare the value of total Danish exports in 2014 with the value of licences granted. In the case of Denmark, this share is 0.1%, which compared to Versino's computed share of 0.94% for the EU as a whole, is a lot lower. However, the share of Danish dual-use related exports to extra-EU countries (8%) is more or less similar to the EU average of 8.5% found in Versino (2015). We should consider that the export mix of EU Member States could strongly differ and that Denmark could export a lower than average share of dual-use goods. Therefore, it is likely that actual exports of Danish dual-use goods subject to licence applications is relatively low (and lower than EU average) at 0.1% of total Danish exports, and 1.2% of extra-EU dual-use related exports.

4.2.2 Detailed characterisation of top-10 product sectors containing highest volume dual-use related export

Table 4.7 shows a more detailed breakdown of the value of dual-use related exports for the top-10 largest sectors in Figure 4.3. The table provides the export value for the HS-4 product groups for both extra-EU and intra-EU destinations for the year 2014. The last column provides the relative share of the total value of extra-EU exports of the product group compared to total dual-use related extra-EU exports in 2014 (e.g. 32% for HS84) as well as the individual HS-4 product groups' share of extra-EU exports in the sector's total (e.g. 11% for HS-8411). The first column shows the number of products (at 8-digit level) that have a correlation with a dual-use code per (HS-2 or HS-4 level) sector to give an idea of the number of products that may be affected by export control regulation in that sector. Since the value of dual-use related exports increases with the number of products that may require a licence, sectors with many product correlations are likely to show a larger dual-use related export value. In order to provide a more complete picture, the 'average' dual-use related export value per (8-digit) product in the sector is also given.[37]

Figure 4.3. Value of extra-EU dual-use related exports, 2014, EU-28



Source: EU COMEXT, Ecorys calculations based on 01-01-2015 correlation table
Note: The largest sector (HS84: Nuclear reactors…) also includes machinery and mechanical equipment which are likely to be the most dominant dual-use related export products in this product group.

[37] The average dual-use related export value per product is calculated by dividing the total value of dual-use related exports in a sector by the number of products with correlation to a dual-use item in that sector. E.g. for HS-84 the average trade value is: €329,083 / 903 ~ €364 million.

Table 4.3. Value of dual-use **related** exports of top-10 largest sectors, at HS-4 detail, 2014

HS-4 description				Jan.-Dec. 2014			
Values in EUR (millions)		Nr. DU	€ AVG	Extra-EU	Intra-EU	Total	
84	**Nuclear reactors, boilers, machinery and mechanical appliances and parts**	903	364	**150,412**	**178,671**	**329,083**	**32%**
8411	Turbo-jets, turbo-propellers and other gas turbines.	26	927	16,964	7,131	24,095	11%
8481	Taps, cocks, valves and similar appliances for pipes, boiler shells, tanks, vats or the like, including pressure-reducing valves and thermostatically controlled valves.	82	362	15,643	14,022	29,665	10%
8471	Automatic data processing machines and units thereof; magnetic or optical readers, machines for transcribing data onto data media in coded form and machines for processing such data, not elsewhere specified or included.	72	816	14,078	44,709	58,787	9%
8479	Machines and mechanical appliances having individual functions, not specified or included elsewhere in this Chapter.	76	286	12,534	9,164	21,698	8%
8414	Air or vacuum pumps, air or other gas compressors and fans; ventilating or recycling hoods incorporating a fan, whether or not fitted with filters.	60	373	10,141	12,240	22,381	7%
8421	Centrifuges, including centrifugal dryers; filtering or purifying machinery and apparatus, for liquids or gases.	14	1,265	8,764	8,948	17,712	6%
8413	Pumps for liquids, whether or not fitted with a measuring device; liquid elevators.	39	362	7,907	6,214	14,121	5%
8486	Machines and apparatus of a kind used solely or principally for the manufacture of semiconductor boules or wafers, semiconductor devices, electronic integrated circuits or flat panel displays; machines and apparatus specified in Note 9 (C) to this Chapter	30	272	7,427	748	8,175	5%
	Other			56,955	75,496	132,450	38%
85	**Electrical machinery and equipment and parts thereof; sound recorders and reproducers, television image and sound recorders and reproducers**	2,661	91	**88,124**	**153,653**	**241,777**	**18%**
8517	Telephone sets, including telephones for cellular networks or for other wireless networks; other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network	60	1,233	19,878	54,113	73,991	23%
8542	Electronic integrated circuits.	124	212	11,226	15,029	26,255	13%
8536	Electrical apparatus for switching or protecting electrical circuits, or for making connections to or in electrical circuits (for example, switches, relays, fuses, surge suppressors, plugs, sockets, lamp-holders and other connectors, junction boxes)	29	859	9,901	15,005	24,905	11%
8537	Boards, panels, consoles, desks, cabinets and other bases, equipped with two or more apparatus of heading 85.35 or 85.36, for electric control or the distribution of electricity, including those incorporating instruments or apparatus of Chapter 90	66	281	9,365	9,159	18,524	11%
8504	Electrical transformers, static converters (for example, rectifiers) and inductors.	39	262	4,376	5,836	10,212	5%
	Other			33,378	54,512	87,889	38%
88	**Aircraft, spacecraft, and parts thereof**	101	1,037	**56,384**	**48,346**	**104,729**	**12%**
8802	Other aircraft (for example, helicopters, aeroplanes); spacecraft (including satellites) and suborbital and spacecraft launch vehicles.	9	7,835	41,902	28,616	70,518	74%
8803	Parts of goods of heading 88.01 or 88.02.	89	380	14,209	19,640	33,849	25%
	Other			273	90	363	0%
90	**Optical, photographic, cinematographic, measuring, checking, precision, medical or surgical instruments and apparatus**	334	194	**36,588**	**28,229**	**64,817**	**8%**
9027	Instruments and apparatus for physical or chemical analysis (for example, polarimeters, refractometers, spectrometers, gas or smoke analysis apparatus); instruments and apparatus for measuring or checking viscosity, porosity, expansion	34	358	7,358	4,797	12,155	20%
9031	Measuring or checking instruments, appliances and machines, not specified or included elsewhere in this Chapter; profile projectors.	106	101	6,293	4,387	10,680	17%
9018	Instruments and appliances used in medical, surgical, dental or veterinary sciences, including scintigraphic apparatus, other electro-medical apparatus and sight-testing instruments.	3	4,215	5,735	6,910	12,645	16%
9026	Instruments and apparatus for measuring or checking the flow, level, pressure or other variables of liquids or gases (for example, flow meters, level gauges, manometers, heat meters)	13	595	4,143	3,593	7,736	11%
9022	Apparatus based on the use of X-rays or of alpha, beta or gamma radiations, whether or not for medical, surgical, dental or veterinary uses, including radiography or radiotherapy apparatus, X-ray tubes and other X-ray generators	22	235	3,075	2,105	5,180	8%
9030	Oscilloscopes, spectrum analysers and other instruments and apparatus for measuring or checking electrical quantities, excluding meters of heading 90.28; instruments and apparatus for measuring or detecting alpha, beta, gamma, X-ray	23	127	1,930	987	2,918	5%
	Other			8,054	5,450	13,504	22%

	HS-4 description			Jan.-Dec. 2014			
	Values in EUR (millions)	Nr. DU	€ AVG	**Extra-EU**	**Intra-EU**	**Total**	
27	**Mineral fuels, mineral oils and products of their distillation; bituminous substances; mineral waxes**	34	2,344	**29,549**	**50,143**	**79,693**	**6%**
2710	Petroleum oils and oils obtained from bituminous minerals, other than crude; preparations not elsewhere specified or included, containing by weight 70 % or more of petroleum oils or of oils obtained from bituminous minerals, these oils being the basic con	16	4,111	26,554	39,227	65,780	90%
2707	Oils and other products of the distillation of high temperature coal tar; similar products in which the weight of the aromatic constituents exceeds that of the non-aromatic constituents.	6	1,069	1,200	5,213	6,413	4%
2711	Petroleum gases and other gaseous hydrocarbons.	8	764	1,174	4,936	6,110	4%
2712	Petroleum jelly; paraffin wax, micro-crystalline petroleum wax, slack wax, ozokerite, lignite wax, peat wax, other mineral waxes, and similar products obtained by synthesis or by other processes, whether or not coloured.	4	95	93	287	379	0%
71	**Natural or cultured pearls, precious or semi-precious stones, precious metals, metals cladwith precious metal, and articles thereof**	24	1,165	**24,518**	**3,448**	**27,966**	**5%**
7108	Gold (including gold plated with platinum) unwrought or in semi-manufactured forms, or in powder form.	4	6,215	23,094	1,767	24,861	94%
7110	Platinum, unwrought or in semi-manufactured forms, or in powder form.	10	143	688	737	1,425	3%
	Other	10	168	735	943	1,679	3%
39	**Plastics and articles thereof**	104	513	**15,820**	**37,569**	**53,390**	**3%**
3926	Other articles of plastics and articles of other materials of headings 39.01 to 39.14.	21	876	5,106	13,292	18,398	32%
3906	Acrylic polymers in primary forms.	7	810	1,810	3,862	5,673	11%
3907	Polyacetals, other polyethers and epoxide resins, in primary forms; polycarbonates, alkyd resins, polyallyl esters and other polyesters, in primary forms.	7	826	1,757	4,025	5,782	11%
3921	Other plates, sheets, film, foil and strip, of plastics.	17	309	1,447	3,812	5,260	9%
3917	Tubes, pipes and hoses, and fittings therefor (for example, joints, elbows, flanges), of plastics.	10	396	1,400	2,563	3,963	9%
3919	Self-adhesive plates, sheets, film, foil, tape, strip and other flat shapes, of plastics, whether or not in rolls.	1	3,796	1,220	2,576	3,796	8%
	Other	41	257	3,079	7,439	10,517	19%
29	**Organic chemicals**	98	166	**8,442**	**7,800**	**16,242**	**2%**
2933	Heterocyclic compounds with nitrogen hetero-atom(s) only.	6	1,714	5,130	5,154	10,284	61%
2922	Oxygen-function amino-compounds.	8	142	708	429	1,137	8%
2930	Organo-sulphur compounds.	5	241	662	544	1,206	8%
2909	Ethers, ether-alcohols, ether-phenols, ether-alcohol-phenols, alcohol peroxides, ether peroxides, ketone peroxides (whether or not chemically defined), and their halogenated, sulphonated, nitrated or nitrosated derivatives.	5	195	591	385	977	7%
	Other	74	36	1,351	1,287	2,638	16%
38	**Miscellaneous chemical products**	288	69	**8,352**	**11,433**	**19,785**	**2%**
3822	Diagnostic or laboratory reagents on a backing, prepared diagnostic or laboratory reagents whether or not on a backing, other than those of heading 30.02 or 30.06; certified reference materials.	64	163	4,553	5,862	10,415	55%
3815	Reaction initiators, reaction accelerators and catalytic preparations, not elsewhere specified or included.	5	1,311	2,409	4,146	6,555	29%
3818	Chemical elements doped for use in electronics, in the form of discs, wafers or similar forms; chemical compounds doped for use in electronics.	7	161	795	329	1,124	10%
	Other	212	8	596	1,096	1,691	7%
89	**Ships, boats and floating structures**	40	255	**8,157**	**2,047**	**10,204**	**2%**
8901	Cruise ships, excursion boats, ferry-boats, cargo ships, barges and similar vessels for the transport of persons or goods.	16	526	6,677	1,738	8,415	82%
8905	Light-vessels, fire-floats, dredgers, floating cranes and other vessels the navigability of which is subsidiary to their main function; floating docks; floating or submersible drilling or production platforms.	10	110	1,010	92	1,102	12%
8906	Other vessels, including warships and lifeboats other than rowing boats.	9	72	447	203	649	5%
8902	Fishing vessels; factory ships and other vessels for processing or preserving fishery products.	5	7	23	14	37	0%
	Total	*4,587*		*426,347*	*521,340*	*947,686*	
	DU Industry Total	*6,197*		*476,347*	*623,202*	*1,099,549*	
		74%		*90%*	*84%*	*86%*	

Source: EU COMEXT, Ecorys calculations, based on 01-01-2015 correlation table

4.3 Case study on Dutch dual-use exports

4.3.1 Introduction

Rationale and objective

This chapter on estimating the size and scope of the EU dual-use industry began by explaining the difficulties and data-related challenges to estimating the size of the dual-use industry and its characteristics. One of the main difficulties relates to the mismatch between the often very specific nature of the technologies, components or products that make a given item dual-use and the corresponding customs code that is assigned to the product when it is exported. At the EU level, the most detailed and harmonised trade statistics can be gathered at CN-8 digit level. Even though this is already a fairly detailed level of reporting, aggregate export values at eight-digit level also include a share of non-dual-use exports. As a result, and as explained in section 4.2, the export analysis performed using customs trade data provides an 'upper threshold' value of dual-use related exports only. The actual value of dual-use product exports will be lower, likely by a factor of 6, according to recent research from the JRC.[38]

This case study further complements and validates the estimates of the actual size and scope of the dual-use industry by analysing detailed customs export data at Member State level, including the information provided by exporters in Box 44 of the Single Administrative Document (SAD), which identifies whether an exporter has obtained an export licence for its product or whether the product is excluded from the EU list of dual-use items. However, this approach will only work for extra-EU exports, as intra-EU exports do not require a SAD document. By identifying the cases where the exporter indicated that their product is on the dual-use list and applied for an export licence, we are able to approximate the *actual* share of dual-use exports as a percentage of total trade in dual-use related products (proxied by the relevant CN-8 codes).

Although this analysis is conducted only for one Member State (the Netherlands, see below) and for one year (2014), this snapshot provides a very good estimate of the share of *actual* dual-use exports in the total value of extra-EU exports in the relevant CN-8 digit product groups, given that trade data are now filtered for licences. Of course, every country (and EU Member State) has a unique export structure based on its comparative strengths, which will generate different dual-use export shares depending on whether certain goods are exported from a country in significant numbers. By combining these estimates with the 'upper threshold dual-use related export values' at EU level (presented in Section 4.2), these case study results will help to further estimate the size and scope of the EU dual-use industry.

Data and approach

This analysis is based on data on exports from the Netherlands in 2014. The data used was obtained from the Dutch Customs Office and contains all export transactions in

[38] Versino (note 28).

the year 2014 for the products at CN-8 level that are included in the DG TAXUD correlation table.[39] The analysis focuses on transactions from the Netherlands registered by the *Douane Sagitta Uitvoer* system. This means that all exports from the Customs Offices located in the Netherlands are registered here. For the Netherlands, a total of 1,086 unique product codes on CN-8 level were present in the data (compared to the total of 1,204 unique CN-8 codes available in the correlation list). The data includes the information from Box 44 of the SAD, which contains additional information from a customs perspective, such as whether the export concerned a simplified export procedure, and information about documents, certificates and authorisations produced in support of the customs.[40] This means that Box 44 also contains information about whether a dual-use export licence was declared in the customs procedure.

If an export authorisation for dual-use goods under the EU Dual-use Regulation is declared, this is indicated by the code X002. In practice, three different types of dual-use export licences exist: Individual export licences, Global export licences and General Export Authorisations (EUGEAs). If the exported product has a EUGEA, the exporter declares both the code X002 and the code corresponding with the EUGEA, ranging from EU001 to EU006, in Box 44 of the SAD. When a product is not included in the dual-use list, but is part of the broader CN-8 product group code, the declarant writes the code Y901 in Box 44 of the SAD. For the analysis, this means that we are interested in knowing the share of extra-EU exports under 'X002', which will yield the share of *actual* dual-use extra-EU exports in a particular CN-8 product category.

The dataset that has been used for the analysis shows that the number of dual-use related export transactions from the Netherlands in 2014 was 3.2 million with a total export value of €91.1 billion.[41] In order to calculate more precisely what the actual share of dual-use exports was in 2014, the following data manipulation steps were taken:

- The total number of transactions and the corresponding export values were calculated for every unique product group on CN-8 level [Columns 3 and 4 in Table 4.5a, see Annex 1].
- Similarly, the number of transactions and export values were calculated for transactions with code reference X002 in Box 44 of the SAD, thereby calculating the total transactions and values within the dual-use export regime [Columns 5 and 6 in Table 4.5a, see Annex 1].
- The number of transactions and export values were calculated for exports with a EUGEA, indicated by the codes X002 and any of the EU001-EU006 codes in Box 44 [Columns 7 to 10 in Table 4.5a, see Annex 1].

[39] See: <http://trade.ec.europa.eu/doclib/html/153050.htm>.
[40] SAD Guidelines C44: <http://ec.europa.eu/taxation_customs/customs/procedural_aspects/general/sad/article_5317_en.htm>.
[41] The total value of Dutch extra-EU exports according to the database used was €304 billion. Therefore, the relative share of dual-use related exports in the total Dutch extra-EU exports is 30%. This is very similar to the share retrieved from Dutch extra-EU COMEXT data: €40 billion/ €122 billion = 33%.

- The number of transactions and export values were calculated for exports with an individual or global export licence by subtracting the export transactions under an EUGEA from the total of dual-use export transactions.
- The shares were calculated both as a percentage of the number of transactions and as a percentage of total export value.

The following section presents the results of this exercise.

4.3.2 Results

Table 4.5a containing all the results of this analysis, including the relevant product sectors of the correlation table aggregated at HS2 level, is provided in Annex 1. We highlight the ten sectors identified as containing the highest share of dual-use related exports in 2014 to illustrate the results of the analysis for a relevant sample of the data. Table 4.5b below shows the results for these sectors (according to value of dual-use related exports from high to low). For example, the sector with the highest value of actual dual-use exports, HS84 [nuclear reactors, boilers and machinery] had a total export value of €38.9 billion in 2014, of which 12.6%, or €4.9 billion, was exported with a dual-use export authorisation. The majority of these exports, 12.5% of the total export value, were exported by a licence other than an EUGEA (i.e. by individual or global licence).

Table 4.5b. Share of dual-use exports in dual-use related exports from the Netherlands, top-10 dual-use related export sectors, 2014

HS	Description	Export value	Number transactions	X002 (Total)		X002 (EUGEA)	X002 (Non-EUGEA)
		(€m)		€ million	%	%	%
84	Nuclear reactors, boilers, machinery and mechanical appliances;	38.942	1.262.481	4.908	12,6%	0,1%	12,5%
27	Mineral fuels, mineral oils and products of their distillation; bituminous substances; mineral w axes.	12.366	8.081	0	0,0%	0,0%	0,0%
85	Electrical machinery and equipment and parts thereof;	10.822	1.131.081	1.680	15,5%	0,8%	14,7%
90	Optical, photographic, cinematographic, measuring, checking, precision, medical or surgical instruments	4.268	277.911	72	1,7%	0,0%	1,7%
39	Plastics and articles thereof	3.311	155.225	0	0,0%	0,0%	0,0%
88	Aircraft, spacecraft, and parts thereof.	1.855	41.784	9	0,5%	0,0%	0,5%
38	Miscellaneous chemical products.	880	43.462	0	0,0%	0,0%	0,0%
89	Ships, boats and floating structures.	587	102	0	0,0%	0,0%	0,0%
29	Organic chemicals.	331	5.792	3	1,0%	0,0%	1,0%
71	Natural or cultured pearls, precious or semi-precious stones, precious metals.	7	408	0	0,0%	0,0%	0,0%
Total/Average for top-10 export sectors		**73.368**	**2.926.327**	**6.673**	**9,1%**	**0,2%**	**8,9%**
Total/Average for all exports		**91.086**	**3.244.714**	**7.103**	**7,8%**	**0,1%**	**7,7%**
	Share of top-10 export sectors	*81%*	*90%*				

Source: Confidential Dutch Customs Data, Ecorys calculations

The 10 sectors together have a total export value of €73.4 billion (81% of the total), of which €6.7 billion, or 9.1% was exported under a dual-use export authorisation. The values of exports in the sectors HS84, 27 and 85 are the highest, with values of €38.9 billion, €12.4 billion and €10.8 billion respectively. These sectors contain nuclear products & machinery, mineral fuels and oils, and electrical machinery. Therefore, the three largest dual-use related exporting sectors in the Netherlands are the same as in the EU as a whole. However, Table 4.5b also shows that the actual share of dual-use exports in these sectors is much lower, ranging from 0 to 16% (share of X002). The sector with the highest relative share of dual-use exports is HS85, with 16% of the total value of exports indicated as dual-use exports. On the other hand, in absolute terms HS84 has the largest dual-use export value, with a total of €4.9 billion, followed by HS85, representing a total export value of €1.7 billion. Together these two sectors account for 98.7% of the total *actual* dual-use exports in these top-10 sectors. For all 10 sectors combined, the average share of transactions with a declared dual-use export authorisation is 4.8%. Of the total export value in 2014, 9.1% was exported under a dual-use export authorisation.

Table 4.5b also summarizes the aggregate data for all exports from the Netherlands (as obtained from the Table in the Annex). On the aggregate for the Netherlands, we find that total exports in dual-use related goods equalled €91.1 billion, of which 7.8% were declared under a dual-use export authorisation. Only 0.1% of the total 7.8% exported dual-use goods, were declared under an EUGEA. The other 7.7% of dual-use exports had either a global or an individual export licence. Therefore the 7.8% share of extra-EU dual-use related exports represents the actual dual-use exports from the Netherlands. This corresponds to a share of 2.3% of total extra-EU exports from the Netherlands (total extra-EU exports based on SAD).

The data analysis conducted in this case study shows that the actual share of dual-use goods exports is likely to be a fraction of the total value of dual-use related exports estimated based on CN-8 codes identified through the correlation table. In order to base future policies in the field on more accurate data, future policy and research efforts should therefore aim to further improve data collection and reporting on dual-use goods exports.

4.4 EU dual-use industry in terms of production

Even though exports are probably the most direct and reliable measure for assessing the dual-use industry in the EU, we need to know more about the industrial base that is associated with dual-use exports in the EU to assess the impacts of control. To this end, we also quantified the dual-use industry based on *production values*. Production (or output) associated with dual-use exports is important to consider, especially where exports constitute a large share of a firm’s total dual-use sales. A change in the export control regime could trigger a change in the entire production process of that dual-use item, and affect domestic or intra-EU sales. Secondly, in order to understand the impact of the dual-use industry on the EU economy, including production figures provides a more complete picture. Since the top ten (HS-2) sectors introduced above represented approximately 90% of the industry, we selected these sectors for the production data collection exercise.

In the process of retrieving reliable production data, however, we face similar challenges as for obtaining dual-use trade data. Dual-use items are often very specific technologies or products, so it is important to have the most precise production data for the EU. The PRODCOM database provides production data on an 8-digit level, though these eight digits do not correspond directly to the CN classification that we have used for the customs trade data analysis. As a result, we applied a second conversion process from relevant CN codes (the selected CN codes based on the DG TAXUD correlation table) to PRC codes (the PRODCOM classification). However, the CN to PRC classification table also has limitations that are similar to those described in the previous section for matching dual-use items with CN codes. Most importantly, for certain dual-use CN codes, no corresponding PRC code is available. For the 2013 dataset, this was the case for 81 CN-8 digit codes (based on the dual-use related CN codes in the top-10 selected sectors). Compared with all the relevant codes, however, this mismatch is not too problematic.

Table 4.6 shows the match between dual-use related CN codes and PRC codes for the top-10 of sectors based on extra-EU exports, both in percentage (missing matches compared to the total relevant CN codes) as well as the absolute number of missing matches. Since the match for 2013 between the total number of dual-use CN codes and corresponding PRC codes is very good for most sectors (except for HS27 and HS89), this section continues with the presentation of the production data for that year.[42] We believe that a snapshot picture of the industry in 2013 provides a useful picture of the size (value) and scope (type of products) of the sector in terms of production values.

Another limitation of the data is that PRC codes could also include certain non-dual-use production, so that the figures presented could be an overestimate. A complicating factor is that the PRC as well as CN codes are updated every year, so that the correlation will also change every year. Lastly, the PRODCOM database uses production data sourced at a detailed level from Member States. However, since the sector disaggregation is very detailed, production data at Member State level could sometimes be traced back to companies when there are few companies active in that sector. For this and other reasons, Member States sometimes mark production data as confidential, in which case the values are not reported. Table 4.6 also indicates the share of confidential entries present in the dual-use related production codes in the top-10 selected sectors (approximately 23% overall). For the EU-28 in the aggregate, however, estimates for the confidential data are included so that on the whole the production data should be an accurate reflection. This study uses only the EU-28 aggregate values and thus should not be as much affected by the confidential figures.

[42] Ideally, the production data for multiple years would be presented in this section, but as Table 4.6 shows the quality of the match between PRC codes and CN codes reduces for the years further in the past. Therefore, when we do not compare production data for the same amount of PRC codes across different years, the comparison of total production values becomes worthless since one is not comparing production values across the same base.

Table 4.6. Top 10 sectors with highest extra-EU dual-use exports, PRODCOM coverage, 2006, 2009, 2013

				PRODCOM – CN Correspondence		
			’13	’13	‘09	‘06
HS 2	Sector name (short)	Share of ‘confidential’ PRODCOM entries	No. of missing matches	%	%	%
84	Nuclear reactors and machinery	22%	13	95%	92%	79%
85	Electrical machinery	23%	30	86%	79%	44%
88	Aircraft and spacecraft	19%	0	100%	100%	94%
90	Optical, measuring and medical equipment	23%	2	100%	93%	84%
27	Mineral fuels and oil	17%	28	18%	6%	6%
71	Pearls, precious stones and precious metals	23%	1	92%	77%	77%
39	Plastics	23%	0	100%	84%	80%
29	Organic chemicals	25%	3	94%	62%	45%
38	Miscellaneous chemical products	29%	4	77%	71%	71%
89	Ships, boats and floating structures	n.a.	n.a.	0%	0%	100%

Source: Ecorys calculations based on the RAMON CN -> PRC (2013) correlation table

This section first introduces the overall size of the ten largest dual-use related export sectors (see previous section) and then continues with a more detailed presentation of the most prolific types of products within each of the ten sectors.

4.4.1 Size of the EU dual-use industry based on production

The previous section demonstrated that based on a customs trade statistics analysis, the value of exports containing dual-use items is approximately €1,100 billion in recent years. However, when cross-checking the value with licensing authority data, the registered value of licenced exports is more likely to be close to 3.3% (or €150 billion in 2013) of total EU exports.[43] Based on the corresponding production data for the ten[44] largest sectors (based on extra-EU exports values) and following the

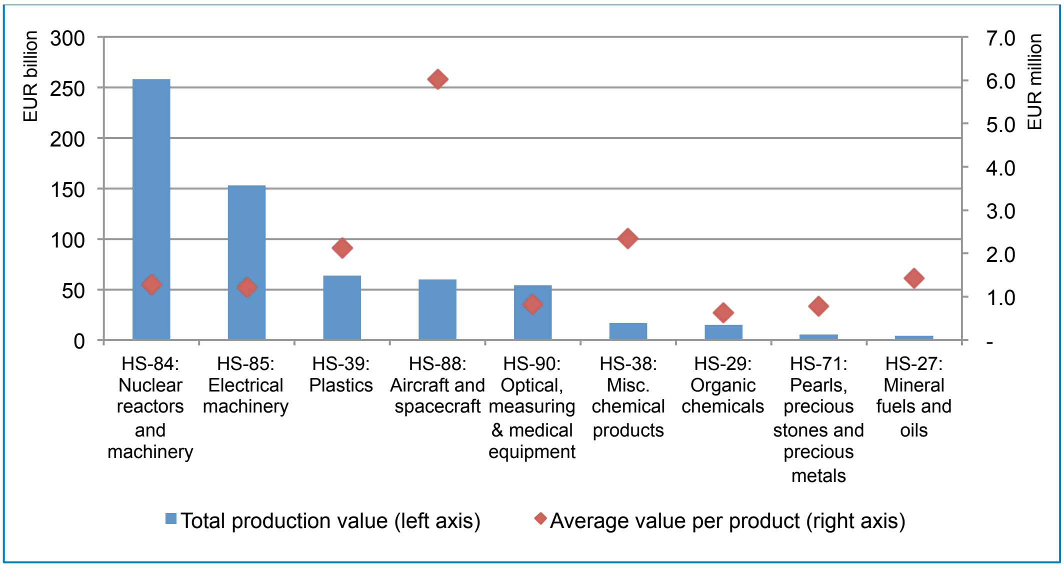
[43] Versino (note 28)

[44] Though effectively the production data represent the production of dual-use related products in *nine* of the top-10 sectors, since there is no correlation possible for the dual-use items in HS-89 (see Table 4.6).

methodology we described above, we find that the size of the 'dual-use related industry' is over €600 billion for all EU-28 Member States combined.

Figure 4.4 shows the contribution of the nine individual sectors (grouped at HS-2 digit level) to the total production value. Sector HS-84 (mostly machinery products) is by far the largest dual-use sector in terms of production, with over €250 billion of production in 2013. The graph also shows the average value per product (in € billion) in the EU-28 per PRC product code. This indicator is useful to consider since HS-84, for example, consists of many more dual-use relevant production (and trade) codes than HS-88, which only has four dual-use relevant 8-digit codes. As a result, the average value of production per dual-use relevant production code could significantly differ across sectors.

Figure 4.4. Total production value and average value for most important sectors, based on extra-EU export value, 2013, in € billions



Source: PRODCOM (2013), Ecorys calculations

These figures, however, need to be interpreted with great caution since the actual value is likely to be much lower. As shown in the trade analysis in Section 4.2, customs trade data needed to be adjusted downward by a factor of six, while the correlation between the customs trade codes and PRODCOM codes also has its additional limitations. It is therefore highly likely that the 8-digit PRODCOM codes include large shares of non-dual-use related production. This would explain the large divergence between both figures.

In an effort to address the limitation that PRC codes also include unknown (but likely large) shares of non-dual-use related products, a study simultaneously conducted to this study by King's College London uses additional expert judgement to estimate for a selected number of products the share of actual dual-use products included in dual-use relevant PRC codes (Stewart, 2015).[45] The methodology applied by Stewart also has limitations, including the inherent PRODCOM database limitations, and the fact that bandwidths of dual-use shares [0, 2-5%, 5-30%, 30-60%, 60-95%, 95-97% and 100%] that were used in the study limit the accuracy of the estimates. Moreover, Stewart (2015) identifies dual-use relevant PRC codes manually, whereas this analysis used the Annex I – CN and CN – PRC correlation tables in order to arrive at the relevant list of dual-use relevant PRC codes.

The list of selected dual-use relevant PRC codes therefore differs between both studies. Despite the differences in approaches and the different limitations to both analyses, it is useful to compare the available estimates on the size of the dual use industry in the EU. Stewart finds that the range of [2-5%] is most often applied as the most realistic share of dual-use items in the selected PRC codes, meaning that actual dual-use goods included in PRC codes are likely to be only a fraction of total production. As a result (as well as due to the selection of different PRC codes), he finds that dual-use production in the EU is likely to be between €26.5 and €36.2 billion in 2013.

We estimate the value of dual-use related production in the EU to be approximately €102 billion in 2013. This is calculated by taking the production value from the ten largest sectors (based on extra-EU exports values), €631 billion, and dividing this figure by Versino's overestimation factor of 6.2 (actual dual-use exports compared to dual use-related exports, see section 4.2.1).

4.4.2 Detailed overview of most important products in top-10 dual-use items producing sectors

Fully exploiting the fact that the PRODCOM database has production statistics for products up to 8-digit level, we detail which type of products represent the most important products in the selected ten sectors. However, since the share of dual-use goods in the selected PRC codes is unknown, we have not corrected the below results with the above mentioned average share of dual-use items. Therefore, the results overestimate the actual value of the dual-use production in these sectors. The most important products are presented based on their share in the sector's total value of dual-use *production*. For comparison, we have also computed the dual-use related production for the most significant HS-4 sub-sectors based on total extra-EU *export value* in the top-10 HS-2 sectors. This list of HS-4 sub-sectors was already presented in Table 4.7.

In the following sub-section, the production data for the largest product groups (based on production) in the ten sectors is presented. All tables show the combination of product groups that jointly represent at least 50% of the total production of dual-use related items in the overall HS-2 sector. Secondly, the aggregate production figures for the top HS-4 sub-sectors is reveal the relative share of the HS-4 sub-sector in aggregate production and aggregate extra-EU exports.

[45] At the time of publication of this study, the research conducted by Stewart (2015) was still unpublished.

1) HS84 - Nuclear reactors, machinery and mechanical appliances[46]

Tables 4.7 and 4.8 present the most important dual-use related products for this sector based on total production values in 2013 and based on HS-4 sub-sectors with the highest extra-EU trade values.

The total EU-28 production value of dual-use items in HS-84 was €258.5 billion in 2013. Jointly, other machinery and mechanical appliances and their parts (8%) as well as turbo-jets and parts of turbo-jets (7%) form the largest product groups based on value. The semi-conductor industry (represented in this sector by 'machines for the manufacture of semi-conductor devices, 3%) proves its importance for the dual-use industry combined with the manufacture of semi-conductor and related devices covered by HS85.

Table 4.8 shows that products that are important in terms of production volumes also export most to extra-EU destinations. Since this sector is relatively more important from the perspective of total extra-EU exports (representing a higher share in the total for exports compared to production), this sub-sector might thus be more affected by potential changes in the export control regime than the production data alone would suggest.

[46] Machinery and mechanical equipment are likely to be the most dominant dual-use related export products in this product group.

Table 4.7. Most important dual-use **related** products in HS84, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS84)	Production value (€ 1,000)
28993955	Other machines	5%	13,181,000
30301600	Parts of turbo-jets or turbo-propellors	4%	9,682,946
28992040	Machines for the manufacture of semiconductor devices or electronic integrated circuits	3%	8,000,000
28995280	Parts of machines	3%	7,000,000
30301200	Turbo-jets and turbo-propellors	3%	6,651,713
26202100	Storage units	2%	6,000,000
28251130	Heat exchange units	2%	5,360,000
28292150	Sealing machinery	2%	4,962,727
28221840	Lifting machinery	2%	4,934,999
28926150	Parts for earthmoving equipment	2%	4,543,798
28141380	Other appliances	1%	3,719,042
28251390	Other refrigerating equipment	1%	3,590,100
28152440	Other gear boxes	1%	3,477,093
28151030	Ball bearings	1%	3,343,856
28121450	Valves for oleohydraulic pow er transmission	1%	3,217,152
28141235	Taps, cocks and valves	1%	3,200,000
28133100	Parts of pumps for liquids and liquid elevators	1%	3,099,322
28113300	Parts of gas turbines	1%	3,070,718
28142000	Parts for taps, cocks and valves	1%	3,046,263
28112300	Gas turbines	1%	2,987,454
28924030	Sorting, screening, w ashing machines	1%	2,951,513
28152450	Gearboxes	1%	2,939,349
26204000	Parts and accessories of the machines of HS 8471	1%	2,896,311
28993935	Industrial robots	1%	2,788,967
28291230	Machinery for purifying w ater	1%	2,728,000
28298400	Non-automatic lubricating pots	1%	2,709,335
28298250	Parts for purifying machinery	1%	2,633,001
28291270	Machinery for solid-liquid seperation	1%	2,500,000
28141315	Process control valves	1%	2,500,000
28132530	Turbo-compressors	1%	2,330,004
Total		**50%**	**130,044,665**

Source: PRODCOM (2013), Ecorys calculations

Table 4.8. Most important dual-use **related** products in HS84, based on extra-EU trade, 2013

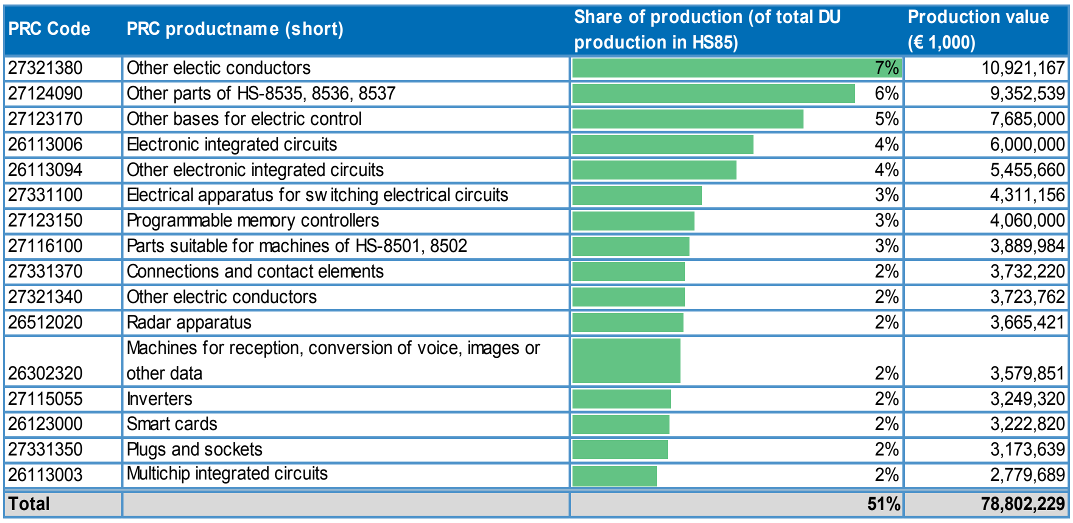
HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS84 DU products)	Share of production (of total DU production in HS84)	Production value (€ 1,000)
8411	Turbo-jets, turbo-propellers and other gas turbines	11%	9%	22,392,832
8481	Taps, cocks, valves and similar appliances	10%	11%	29,026,033
8471	Automatic data processing machines and units thereof	9%	6%	14,349,128
8479	Machines and mechanical appliances	8%	10%	24,995,630
8414	Air or vacuum pumps, air or other gas compressors and fans	7%	7%	17,541,828
8421	Centrifuges, filtering or purifying machinery	6%	5%	13,154,484
8413	Pumps for liquids; liquid elevators	5%	5%	11,826,140
8486	Machines and apparatus for the manufacture of semiconductor boules or w afers, semiconducter devices, electrnoic integrated circuits	5%	4%	9,101,826
Total		**61%**	**56%**	**142,387,901**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

2) HS85 - Electrical machinery

Tables 4.9 and 4.10 present the most important dual-use related products for this sector based on total production values in 2013 and based on HS-4 sub-sectors with the highest extra-EU trade values. This sector covers largely electrical machinery and equipment and parts that are relevant for the EU dual-use industry. The total EU-28 production value of dual-use items in this sector equalled €153.2 billion in 2013.

Table 4.9. Most important dual-use related products in HS85, based on production, 2013

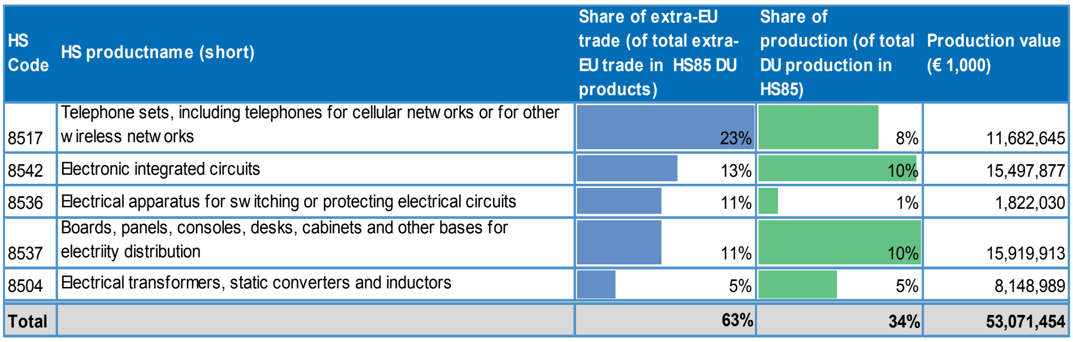


PRC Code	PRC productname (short)	Share of production (of total DU production in HS85)	Production value (€ 1,000)
27321380	Other electic conductors	7%	10,921,167
27124090	Other parts of HS-8535, 8536, 8537	6%	9,352,539
27123170	Other bases for electric control	5%	7,685,000
26113006	Electronic integrated circuits	4%	6,000,000
26113094	Other electronic integrated circuits	4%	5,455,660
27331100	Electrical apparatus for sw itching electrical circuits	3%	4,311,156
27123150	Programmable memory controllers	3%	4,060,000
27116100	Parts suitable for machines of HS-8501, 8502	3%	3,889,984
27331370	Connections and contact elements	2%	3,732,220
27321340	Other electric conductors	2%	3,723,762
26512020	Radar apparatus	2%	3,665,421
26302320	Machines for reception, conversion of voice, images or other data	2%	3,579,851
27115055	Inverters	2%	3,249,320
26123000	Smart cards	2%	3,222,820
27331350	Plugs and sockets	2%	3,173,639
26113003	Multichip integrated circuits	2%	2,779,689
Total		**51%**	**78,802,229**

Source: PRODCOM (2013), Ecorys calculations

The top-5 most important products based on production values largely cover electronic conductors, electronic integrated circuits and other bases for electric control. This top five accounts for 26% of the total production value of dual-use items within the electrical machinery product group.

Table 4.10. Most important dual-use related products in HS85, based on extra-EU trade, 2013



HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS85 DU products)	Share of production (of total DU production in HS85)	Production value (€ 1,000)
8517	Telephone sets, including telephones for cellular netw orks or for other w ireless netw orks	23%	8%	11,682,645
8542	Electronic integrated circuits	13%	10%	15,497,877
8536	Electrical apparatus for sw itching or protecting electrical circuits	11%	1%	1,822,030
8537	Boards, panels, consoles, desks, cabinets and other bases for electriity distribution	11%	10%	15,919,913
8504	Electrical transformers, static converters and inductors	5%	5%	8,148,989
Total		**63%**	**34%**	**53,071,454**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

Comparing the export performance and production figures (Table 4.10) shows that especially HS8517, where apparatus for communication in a wired or wireless network are included, is very important in terms of extra-EU exports compared to the relative importance of production. Also sub-sector HS8536 [electrical apparatus for switching or protecting electrical circuits] is relatively more important in the context of the export control review due to the strong relative focus on extra-EU exports.

3) HS88 - Aircraft and spacecraft

The third largest sector covers aircraft and spacecraft and related parts. Figure 4.4 already showed that the average value per product group is high compared to the other sectors, which is understandable given the nature of the product. Tables 4.11 and 4.12 present the most important dual-use related products for this sector based on total production values in 2013 and based on HS-4 sub-sectors with the highest extra-EU trade values. The total EU-28 production value of dual-use items in this sector equalled €60.2 billion in 2013.

Table 4.11. Most important dual-use related products in HS88, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS88)	Production value (€ 1,000)
30305090	Parts for aircraft	55%	33,210,961
30303400	Aeroplanes and other aircraft >15,000 kg	20%	12,000,000
30304000	Spacecraft, satellites	8%	5,000,000
30303100	Helicopters	7%	4,454,318
30303300	Aeroplanes and other aircraft >2,000 kg but ≤15,000 kg	6%	3,347,371
Total		**96%**	**58,012,649**

Source: PRODCOM (2013), Ecorys calculations

Aircraft and aircraft parts are by far the most important items in this group in terms of production value. Aircraft parts alone account for over half of the production value of dual-use items within the aircraft and spacecraft product group. Table 4.12 shows that in terms of extra-EU exports, other (e.g. helicopters) aircraft and spacecraft are most important. It should be noted, however, that the other sub-sectors in this group (HS-8801 and HS-8804) did not report extra-EU trade data for 2014. It is likely that exports in these groups are actually occurring. However, due to the data limitations, they are not reported in this table.

Table 4.12. Most important dual-use related products in HS88, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS88 DU products)	Share of production (of total DU production in HS88)	Production value (€ 1,000)
8802	Other aircraft and spacecraft	74%	42%	24,981,436
8803	Parts of goods of heading 88.01	25%	58%	34,694,904
Total		**99%**	**99%**	**59,676,340**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

4) HS90 – Medical, measuring and optical instruments

The fourth largest sector from the perspective of extra-EU exports covers a wide range of optical, photographic, cinematographic, measuring, checking, precision, medical and or surgical instruments. The total EU-28 production value of dual-use related items in this sector equals €54.1 billion. Since it is a sector with potentially a large variety of dual-use relevant items, it is useful to break the sector down more specifically into dual-use related products. Tables 4.13 and 4.14 show that in this sector the measuring devices, navigational and medical equipment are the most relevant products (in terms of production). While based on PRC codes, medical and surgical instruments have the largest share of production (11%, table 4.13), based on HS codes measuring and checking instruments account for the largest share of production (20%), and the second largest share of extra EU exports (17%).

Table 4.13. Most important dual-use related products in HS90, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS90)	Production value (€ 1,000)
32501370	Medical, surgical instruments	11%	6,050,000
26518200	Parts, accessories for 26.51.12, .32, .33, .4 and .5	7%	3,690,899
26516670	Other electronic measuring instruments	6%	3,399,353
26511150	Aeronautical or space navigation instruments	6%	3,300,000
26601115	Apparatus based on the use of X-rays	6%	3,200,871
26516650	Electronic instruments for measuring geometrical quantities	3%	1,815,043
26518520	Parts of instruments of HS-9031	3%	1,552,599
26515283	Electronic instruments for measuring variables of liquids/gases	2%	1,318,104
26515383	Other electronic instruments	2%	1,276,051
26516620	Test benches	2%	1,273,905
26516689	Non-electronic measuring machines and instruments	2%	1,200,000
Total		**52%**	**28,076,825**

Source: PRODCOM (2013), Ecorys calculations

Table 4.14. Most important dual-use related products in HS90, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS90 DU products)	Share of production (of total DU production in HS90)	Production value (€ 1,000)
9027	Instruments and apparatus for physical or chemical analysis	20%	16%	8,505,284
9031	Measuring or checking instruments, appliances and machines	17%	20%	10,618,293
9018	Instruments and appliances used in medical, surgical, dental or veterinary sciences	16%	12%	6,537,474
9026	Instruments and apparatus for measuring or checking the flow , level, pressure or other variables of liquids or gases	11%	17%	9,171,218
9022	Apparatus based on the use of X-rays or of alpha, beta or gamma radiations	8%	11%	5,686,182
9030	Oscilloscopes, spectrum analysers and other instruments and apparatus for measuring or checking electrical quantities	5%	12%	6,317,406
Total		**77%**	**87%**	**46,835,857**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

5) HS27 - Mineral fuels and oils

The fifth largest group includes mineral fuels, mineral oils and products of their distillation. This sector has only a few relevant dual-use related production codes. Moreover the correlation between dual-use relevant CN codes and PRC codes was particularly poor in this sector (as shown in Table 4.7 with a match of only 17.6%). Thus there were only three matching PRC codes with the CN classification. The total EU-28 production value of these three production codes was €4.3 billion in 2013.

Table 4.15. Most important dual-use related products in HS27, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS27)	Production value (€ 1,000)
20147340	Naphthalene	53%	2,275,930
20147320	Benzol, toluol and xylol	29%	1,255,386
20147390	Other oils and oil products	18%	754,700
Total		**100%**	**4,286,015**

Source: PRODCOM (2013), Ecorys calculations

Table 4.16. Most important dual-use related products in HS27, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS27 DU products)	Share of production (of total DU production in HS27)	Production value (€ 1,000)
2707	Oils and other products of the distillation of high temperature coal tar	4%	100%	4,286,015
Total		**4%**	**100%**	**4,286,015**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

6) HS71 - Pearls, precious stones and precious metals

The sixth largest sector covers pearls, precious stones and precious metals. The more detailed trade analysis had already shown that exports with corresponding codes in the correlation list mostly concern the export of gold (and small quantities of platinum). The matching to PRC codes also provided production codes for silver and other precious metals. Jointly, the total EU-28 production value of possibly dual-use related items in this sector equalled €5.5 billion.

Table 4.17. Most important dual-use related products in HS71, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS71)	Production value (€ 1,000)
24412050	Gold, in semi-manufactured forms	56%	3,079,172
24411050	Silver, in semi-manufactured forms	17%	949,990
24413050	Platinum, palladium, rhodium, iridium, osmium and ruthenium	11%	574,497
32121400	Other articles of precious metal	8%	410,335
32121100	Cultured pearls, precious or semi-precious stones	7%	393,029
Total		**99%**	**5,407,024**

Source: PRODCOM (2013), Ecorys calculations

Table 4.18. Most important dual-use related products in HS71, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS71 DU products)	Share of production (of total DU production in HS71)	Production value (€ 1,000)
7108	Gold, unwrought or in semi-manufactured forms, or in powder form	94%	56%	3,079,172
7110	Platinum, unwrought or in semi-manufactured forms, or in powder form	3%	11%	574,497
Total		**97%**	**67%**	**3,653,669**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

7) HS39 – Plastics

Even though 'plastics' is the seventh largest group from an extra-EU export perspective, the total EU turnover in the sector is substantial. In total, the production potentially related to dual-use items equalled €63.5 billion in 2013 (more than for example HS27 and HS71). Comparing Table 4.19 and Table 4.20, we find that in terms of both production and extra-EU exports, the 'other articles of plastics' products are the most important. Studying the 8-digit level product or trade codes included in the HS-4 sub-sector in more detail, however, does not reveal more information about the type of products that are included in this category.

Table 4.19. Most important dual-use related products in HS39, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS39)	Production value (€ 1,000)
22292990	Other articles of plastics	27%	17,000,000
22221950	Articles for the conveyance or packaging of goods	12%	7,590,665
20165390	Acrylic polymers, in primary forms	7%	4,500,000
20165150	Polymers of propylene or of other olefins, in primary forms	6%	3,700,208
20165700	Silicones, in primary forms	5%	3,326,650
Total		**57%**	**36,117,523**

Source: PRODCOM (2013), Ecorys calculations

Table 4.20. Most important dual-use related products in HS39, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS39 DU products)	Share of production (of total DU production in HS39)	Production value (€ 1,000)
3926	Other articles of plastics and articles of headings 39.01 to 39.14	32%	29%	18,694,497
3906	Acrylic polymers in primary forms.	11%	7%	4,500,000
3907	Polyacetals, other polyethers and epoxide resins, in primary forms	11%	7%	4,522,836
3921	Other plates, sheets, film, foil and strip, of plastics	9%	8%	4,808,828
3917	Tubes, pipes and hoses, and fittings therefor	9%	11%	7,090,975
3919	Self-adhesive plates, sheets, film, foil, tape, strip and other flat shapes	8%	3%	2,140,418
Total		**80%**	**66%**	**41,757,554**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

8) HS29 - Organic chemicals

The eighth largest sector in terms of extra-EU exports in 2014 comprises organic chemicals. The total EU-28 production value of dual-use related products in this sector equalled €15.0 billion in 2013. Tables 4.21 and 4.22 present the most important dual-use related products for this sector based on total production values in 2013 and based on HS-4 sub-sectors with the highest extra-EU trade values.

Table 4.21. Most important dual-use related products in HS29, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS29)	Production value (€ 1,000)
20145280	Compounds containing in the structure an unfused pyridine ring or a quinoline or isoquinoline ring-system	42%	6,339,431
20145139	Other organo-sulphur compounds	7%	1,051,113
20145150	Organo-inorganic compounds	6%	950,584
20143475	Carboxylic acid w ith alcohol, phenol, aldehyde or ketone functions	6%	939,173
20142265	Lauryl alcohol; cetyl alcohol; stearyl alcohol and other saturated monohydric alcohols	6%	845,767
Total		**68%**	**10,126,068**

Source: PRODCOM (2013), Ecorys calculations

Tables 4.21 and 4.22 show that in terms of both production and extra-EU trade, there is a specific group of products that are particularly important for this sector: compounds with nitrogen heteroatoms. From a production perspective, this product represents 42% (or €6.3 billion) of total production of dual-use related organic chemicals.

Table 4.22. Most important dual-use related products in HS29, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS29 DU products)	Share of production (of total DU production in HS29)	Production value (€ 1,000)
2933	Heterocyclic compounds w ith nitrogen hetero-atom(s) only	61%	42%	6,339,431
2922	Oxygen-function amino-compounds	8%	6%	876,020
2930	Organo-sulphur compounds	8%	7%	1,051,113
2909	Ethers, ether-alcohols, ether-phenols, ether-alcohol-phenols, alcohol peroxides, ether peroxides, ketone peroxides	7%	6%	835,206
Total		**84%**	**61%**	**9,101,770**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

9) HS38 - Miscellaneous chemical products

The penultimate largest group also concerns chemical products and relates to any other chemical products not covered by the categories earlier. The total EU-28 production value of dual-use items in this sector equals €16.9 billion in 2013. Tables 4.23 and 4.24 show that in terms of both production and extra-EU exports, the importance of certain products can differ. From a production perspective, the production of biofuels covers the most important dual-use related product (€7.1 billion of production, relating to 42% of the entire dual-use production in the sector).

Table 4.23. Most important dual-use related products in HS38, based on production, 2013

PRC Code	PRC productname (short)	Share of production (of total DU production in HS38)	Production value (€ 1,000)
20595997	Biofuels (diesel substitute)	42%	7,128,885
20595210	Composite diagnostic or laboratory reagents	26%	4,387,017
20595660	Reaction initiators, reaction accelerators and catalytic preparations	20%	3,359,890
20595300	Chemical elements doped for use in electronics	5%	808,752
20595953	Preparations for electroplating	3%	480,074
Total		**95%**	**16,164,619**

Source: PRODCOM (2013), Ecorys calculations

On the other hand, from an export perspective (Table 4.24), the product that stands out in terms of export performance (and thus potentially more significantly impacted by the export control review) relates to the second largest product in terms of total EU-28 production: diagnostic or laboratory reagents. This product covers more than 50% of the total value of extra-EU dual-use exports in this product group and 26% of the total value of dual-use related production.

Table 4.24. Most important dual-use related products in HS38, based on extra-EU trade, 2013

HS Code	HS productname (short)	Share of extra-EU trade (of total extra-EU trade in HS38 DU products)	Share of production (of total DU production in HS38)	Production value (€ 1,000)
3822	Diagnostic or laboratory reagents on a backing, prepared diagnostic or laboratory reagents	55%	26%	4,387,017
3815	Reaction initiators, reaction accelerators and catalytic preparations	29%	20%	3,359,890
3818	Chemical elements doped for use in electronics	10%	5%	808,752
Total		**94%**	**50%**	**8,555,659**

Source: PRODCOM (2013), Eurostat COMEXT, Ecorys calculations

10) HS89 - Ships, boats and floating structures

The last sector in the top-10 largest sectors from an export perspective covers the production (and export) of ships, boats and floating structures. However, as explained at the start of this section, there are no matching PRODCOM codes for the dual-use related CN codes in this sector for 2013. For this sector, therefore, we can only rely on the export data presented in Section 4.2.

4.5 EU Dual-use industry in terms of employees and enterprises

While production and trade statistics provide the most direct estimate about the total size of the EU dual-use industry, estimates on the total employment and number of enterprises related to the production of dual-use goods help to define the potential socio-economic impacts of the review. Unfortunately, there is no data available that directly measures the number of jobs and enterprises engaged in producing dual-use goods. As a result, we base our estimates on the number of jobs and enterprises involved in producing dual-use goods in the EU on the selection of PRODCOM product codes selected in the previous section. PRODCOM codes (at 8-digit level) are based on the NACE classification of economic activities in the EU, which in turn is the reference classification for Eurostat's Structural Business Statistics (SBS) database. The SBS data, including employment and number of enterprises,[47] is collected by National Statistical Institutes (NSIs) of all EU-28 Member States.

However, a large limiting factor to the analysis is that the highest level of SBS data available (including for employment and number of enterprises) is four-digit. In addition to the matching problems described for both the Annex I – CN correlation table as well as the CN – PRC correlation, the scope of this analysis is further restricted to only the first four (NACE) digits of the PRC code. As a result, the dual-use relevant NACE sectors selected for this analysis include (very) large shares of non-dual-use related production. We expect the share of non-dual-use production in the relevant NACE four digit codes to dominate and we should therefore be very careful in drawing any conclusions about the EU dual-use industry on the basis of this data. As presented in Section 4.3, based on trade data the best estimate of the share of actual dual-use items in the aggregate CN-8 product groups is around 3-8%, but since this analysis is conducted at NACE 4-digit level, this share is likely to be even smaller for this analysis. This limitation should be taken into account when interpreting the results in this section (which have not been corrected by any share estimates).

All dual-use related PRC codes selected in Section 4.4 were also used as the basis for this analysis and in turn aggregated at NACE 4-digit level. The duplicate NACE (4-digit) sectors were removed, so that a list of 51 unique NACE (4-digit) dual-use related codes remained. Table 4.25a below shows this list of dual-use relevant NACE sectors (for simplicity at 2-digit level) and the relation to the HS (2-digit) sectors that have been used in this chapter before. The corresponding HS sectors are sorted in order of importance, meaning that for the sector C20 [Manufacture of chemicals and chemical products], most of the dual-use relevant NACE (4-digits) corresponded to the products included in HS71, but that also some relevant NACE 4-digit codes corresponded to products included in HS27. The expanded table (Table 4.25b) is found in Annex 1.

In order to give a representative picture of employment and the number of enterprises involved in dual-use related production, data for 2008 through 2012 has been collected for the EU-27 as a whole. Figures 4.5 and 4.6 present the data collection results. Given the severe data limitations, the results are only presented at the aggregate NACE 2-digit level. While data are also available at NACE 4-digit level, it is not possible to draw conclusions on the *actual* number of enterprises and employees involved in dual-use goods production.

[47] The precise indicators that were used for employment and number of enterprises are defined as 'number of employees' [those persons who work for an employer and who have a contract of employment and receive compensation in the form of wages, salaries, fees, gratuities, piecework pay or remuneration in kind] and 'number of enterprises' [a count of the number of enterprises active during at least a part of the reference period].

Table 4.25a. Matching NACE Rev. 2 – HS

NACE Rev.2	Activity	HS 2-digit
C20	Manufacture of chemicals and chemical products	HS71: Pearls, precious stones and precious metals
		HS29: Organic chemicals
		HS39: Plastics
		HS27: Mineral fuels and oils
C22	Manufacture of rubber and plastic products	HS39: Plastics
C23	Manufacture of other non-metallic mineral products	HS38: Misc. chemical products
C24	Manufacture of basic metals	HS71: Pearls, precious stones and precious metals
C25	Manufacture of fabricated metal products, except machinery and equipment	HS84: Nuclear reactors and machinery
		HS85: Electrical machinery
C26	Manufacture of computer, electronic and optical products	HS85: Electrical machinery
		HS84: Nuclear reactors and machinery
		HS90: Optical, measuring and medical equipment
C27	Manufacture of electrical equipment	HS85: Electrical machinery
		HS90: Optical, measuring and medical equipment
		HS84: Nuclear reactors and machinery
C28	Manufacture of machinery and equipment n.e.c.	HS84: Nuclear reactors and machinery
		HS85: Electrical machinery
		HS90: Optical, measuring and medical equipment
C30	Manufacture of other transport equipment	HS88: Aircraft and spacecraft
		HS84: Nuclear reactors and machinery
C32	Other manufacturing	HS71: Pearls, precious stones and precious metals
		HS90: Optical, measuring and medical equipment
		HS84: Nuclear reactors and machinery

4.5.1 Results

Figure 4.5 below shows the number of enterprises within dual-use related sectors in the EU in the years 2008 through 2012. The three dual-use related sectors with the largest number of enterprises are C32 [*Other manufacturing*], C28 [*Machinery and equipment*], and C25 [*Fabricated metal products (no machinery and equipment)*]. In 2012, 117,000 enterprises were active in the *Other manufacturing* sector. Delving deeper into the dual-use relevant 4-digit level subsectors, only three subsectors are dual-use related, namely the *Manufacture of jewelry and related articles* (C3212), the *Manufacture of medical and dental instruments and supplies* (C3250), and *Other manufacturing* (C3299). In 2012, 60,000 of the enterprises in the C32 sector were active in the *Manufacture of medical and dental instruments and supplies*. Some 27,000 enterprises were active in the *Manufacture of jewellery and related articles*, and the remaining 29,000 enterprises were active in *Other manufacturing* (C3299).

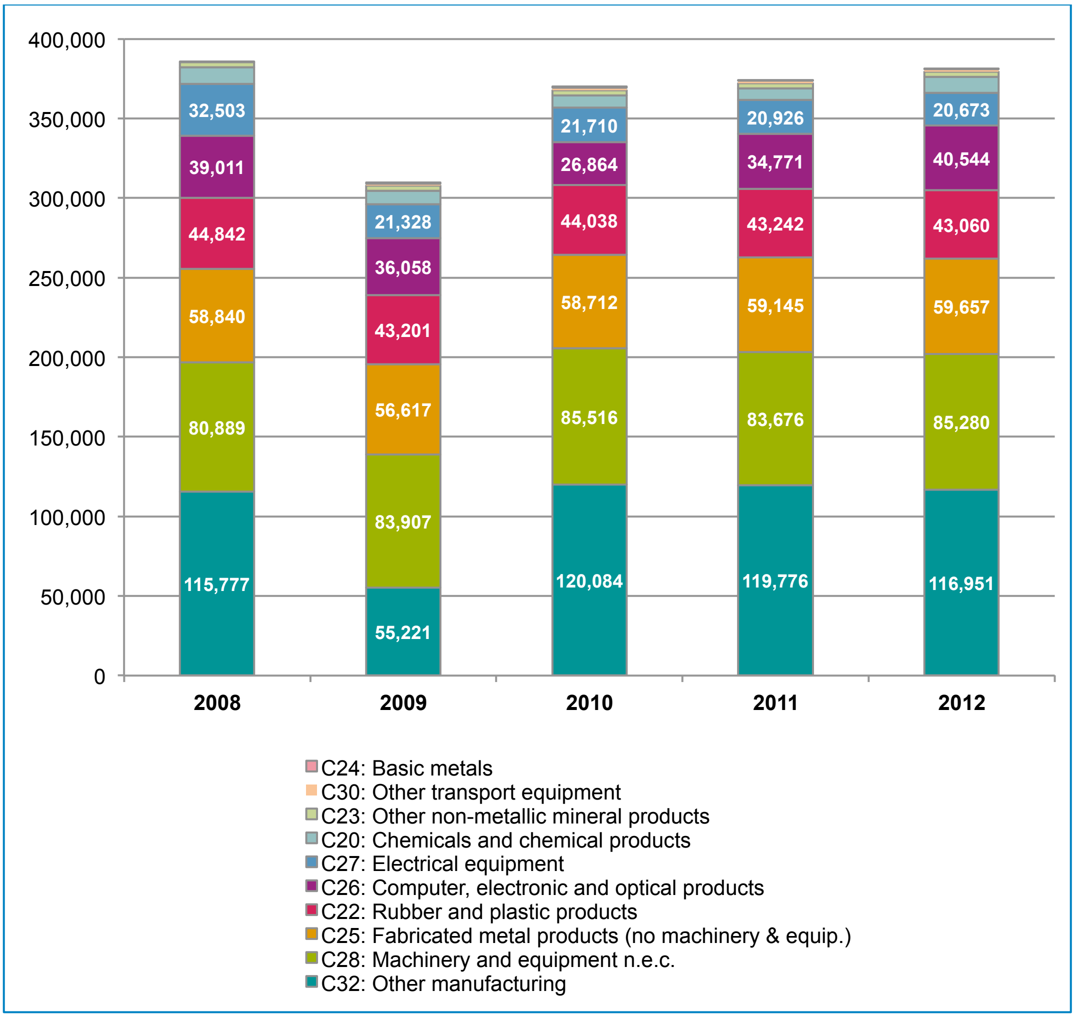
The drop in the number of enterprises for sector C32 in 2009 can be explained by missing data on the number of enterprises within the *Manufacture of medical and dental instruments and supplies*. With the exception of the drop in this particular sector, the total number of enterprises in all dual-use related sectors appears to be relatively stable over time.

Within the *Manufacture of machinery and equipment* (C28), 85,000 enterprises were active in 18 dual-use related NACE 4-digit sectors in 2012. The largest number of enterprises are found in three 4-digit sectors within C28, namely the *Manufacture of other general-purpose machinery* (C2829), the *Manufacture of other special-purpose machinery* (C2899), and the *Manufacture of lifting and handling equipment* (C2822), together accounting for 35,000 enterprises in the EU-28 in 2012.

Of the 60,000 enterprises in Dual-use related sectors within C25 [*Fabricated metal products (no machinery & equipment)*] in 2012, 19,000 are active in the *Manufacture of tools* (C2573), and another 1,000 are active in the *Manufacture of steam generators* (C2530). The remaining 40,000 enterprises are active in the *Manufacture of other fabricated metal products* (C2599).

The number of enterprises in dual-use related NACE sectors in the EU between 2008 and 2012 seems to be stable at approximately 375,000.

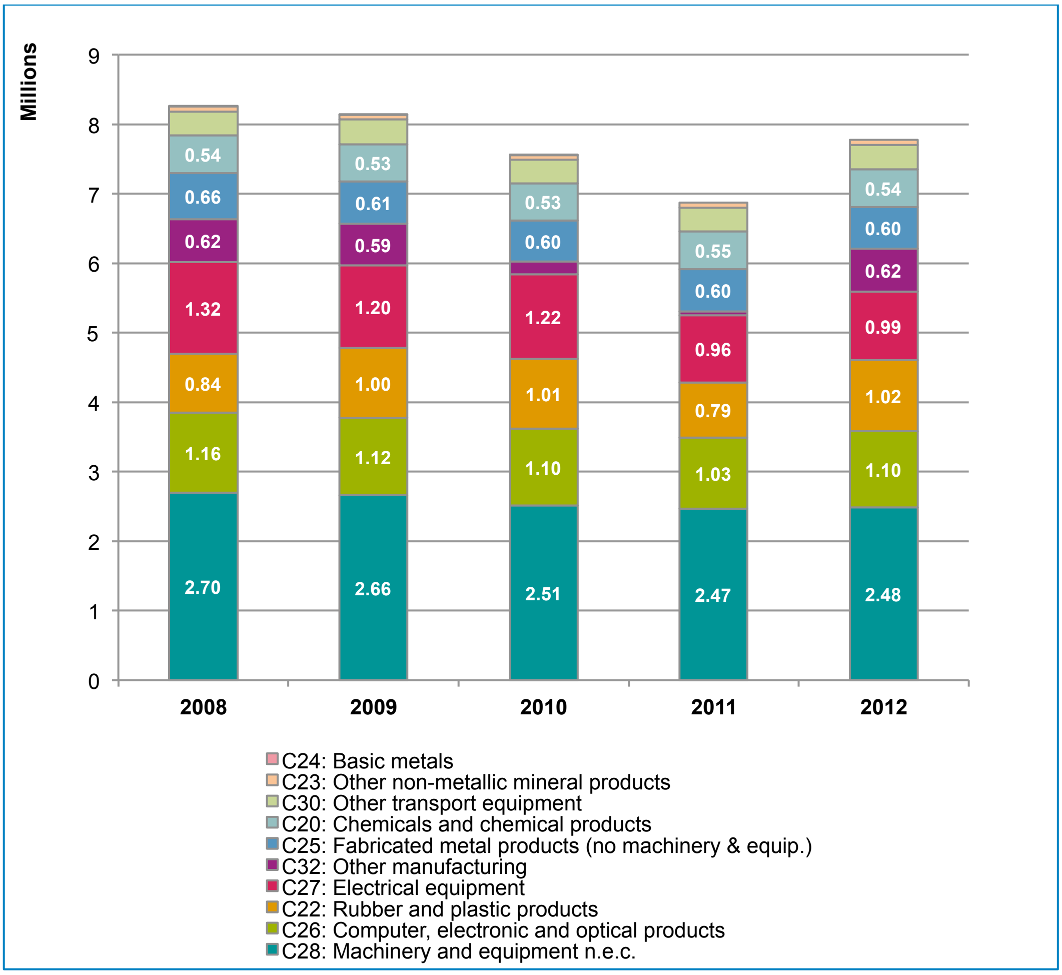
Figure 4.5. Number of enterprises in dual-use related NACE sectors in the EU [2008 - 2012]



Source: Ecorys calculations based on the Structural Business Statistics database (SBS), 2008-2012

The results on employment in dual-use related sectors in the EU from 2008-2012 are summarized in Figure 4.6 and show a relatively similar pattern in terms of importance compared to Figure 4.5. In 2012, there were 2.5 million people employed in the 18 dual-use related NACE 4-digit sectors within sector C28 [*Manufacture of machinery and equipment n.e.c.*]. The sector with the second highest number of employees is C26 [*Manufacture of computer, electronic and optical products*]. In the Dual-use related sectors within this sector, in 2012, a total of 1.1 million people were employed. Of these people, 370,000 were employed in the *Manufacture of instruments and appliances for measuring, testing and navigation* (C2651). Another 400,000 were employed in the *Manufacture of electronic components* or the *Manufacture of communication equipment* (C2611, C2630). Within the dual-use related sectors in C22 [*Manufacture of rubber and plastic products*], 1 million people were employed in the EU in 2012. Similarly to the number of enterprises in dual-use related sectors, the number of employees in dual-use related sectors appear to be relatively constant over time. In the period 2008-2012, between 7 and 8.5 million employees were active in the dual-use related NACE sectors in the EU.

Figure 4.6. Number of employees in dual-use related NACE sectors in the EU [2008 – 2012]



Source: Ecorys calculations based on the Structural Business Statistics database (SBS), 2008-2012

4.6 EU dual-use industry from an international perspective

Given the intrinsic international dimension of export controls, it is highly relevant for the impact assessment to also consider the international dimension and potential impacts of the review of the EU Dual-use Regulation on the international competitive position of the EU dual-use industry. In order to prepare this analysis, this section provides a comprehensive trade performance analysis for the ten sectors with the highest value of dual-use related exports (as selected at the start of this chapter). While the true competitive strength of industries in the global market place is a complex assortment of factors, and trade is only one indication of competitive power, it does allow for a quick assessment of an industry's performance in the world market.

We present the position of the EU's dual-use related industry on the world market by means of two indicators:

1. **World export market shares:** The world market shares present the position of the EU's dual-use related industry on world markets by means of the share of its extra-EU exports in total exports in that sector in a given year.
2. **Revealed Comparative Advantage (RCA):** RCA is an index that is often used as a proxy for international competitiveness as judged by the value of exports in a given sector on the world market (the 'revealed' competitive position with respect to main competitors). The index compares the share of an industry's exports in the total country's value of exports with identical domestic export shares of main competitors in the world. When the share of exports of an industry in the total exports of the country is larger than the share of exports of that same industry in another country's total exports, the industry is believed to have a comparative advantage versus that country due to its relatively larger share of exports. For this study, the RCAs of the EU-28 as an aggregate have been calculated for the top-10 dual-use related sectors and against the main global competitors per sector for the years 2004-2013.

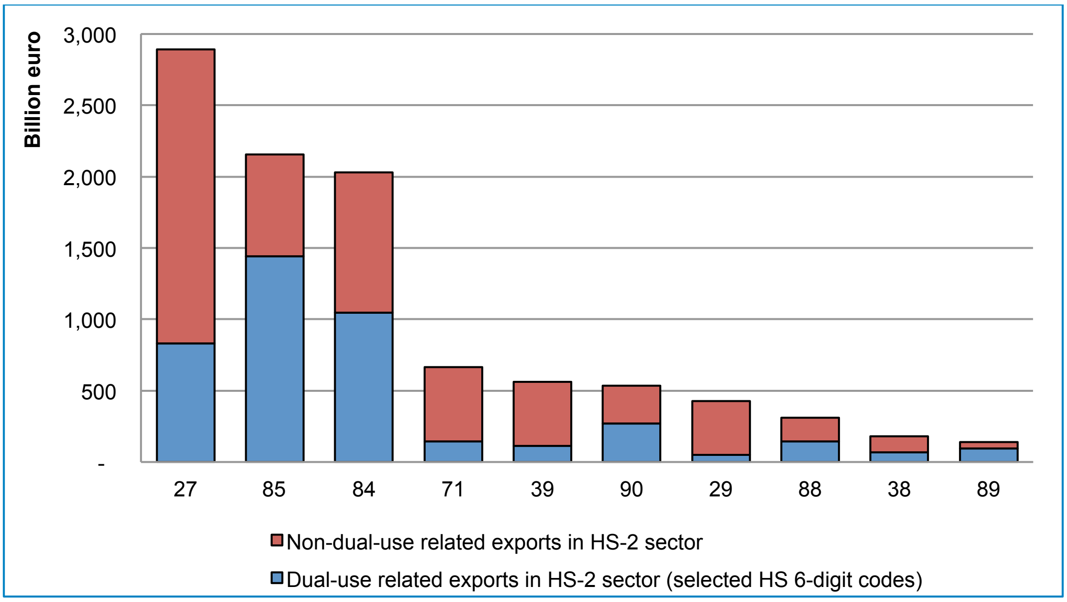
For both these analyses the results should be interpreted with care. As with the previous sections, there are several limitations that need to be taken into account when interpreting the results. Since this analysis is also based on the DG TAXUD correlation table, we need to remember that there is no one-to-one relationship between dual-use codes and HS codes as explained in Section 4.2. However, this limitation becomes (even) more important here as the trade analysis conducted at international level can only go into an (even more) restricted level of detail.

The highest level of detail for harmonised custom trade statistics is 6-digit at international level as opposed to 8-digit data in the sections above. Therefore, selected HS codes at the 6-digit level are likely to contain not only dual-use products, but also a (very) large share of non-dual-use related products. The analysis conducted by Versino (2015) already showed that the dual-use industry estimated through customs trade data could be overrepresented by a factor of 6.2. This estimate is certainly even higher for an analysis at 6-digit level. Similar to the employment analysis in the previous section, the previously calculated range of 3-8% as share of actual dual-use trade is likely to be also too high for this analysis since the level of aggregation in this section is at six digits (not eight). The reader should take this limitation into account when interpreting the results below. For this international analysis, UN COMTRADE data was used, because COMEXT trade data is only available for EU Member States.

4.6.1 Share of EU dual-use related exports in world exports

Before we proceed to the results of the market share of EU dual-use related exports on the world market, we show the relative size of the ten selected largest dual-use related exports in Figure 4.7. This figure indicates that the value of dual-use related exports varies widely across the sectors. However, in line with the previous assessment at EU level, the 'machinery' (HS-84) and 'electrical equipment' (HS-85) sectors show the largest dual-use related extra-EU exports. For illustration purposes, we have also included the value of the non-dual-use HS codes included in the HS-2 digit sector, but of course these have not been included in the remainder of the analysis. To reiterate, within each HS-2 sector, all dual-use relevant product groups (blue shaded area) will include (large) shares of non-dual-use related exports, and these shares in turn are likely to be smaller than 8% as found in the Dutch Customs statistics due to the higher level of aggregation. Still, it is relevant to consider Figure 4.7 while interpreting the different world market shares as well as the revealed comparative advantages across the ten largest sectors.

Figure 4.7. World (non-)dual-use related export values per HS-2 sector in 2013



Source: UN COMTRADE, Ecorys calculations

In order to calculate the share of EU dual-use exports in total world exports, we aggregated all relevant HS 6-digit values per HS-2 sector for each country in the world, based on the DG TAXUD correlation table of Jan-2015. Figure 4.8 (Annex 1) displays per sector the relative export shares of the EU-27 [only extra-EU exports considered], its five largest competitors and the rest of the world. In addition to the general limitations discussed above, it is also important to note that this exercise was conducted with *gross* export values, and is not based on *value added content* of exports. The case-in-point that illustrates this limitation is the large share for Singapore [for example in the case of HS-27 covering fuels such as oil]. Singapore functions as a global shipping hub, generating a large volume of re-exports, which in turn results in an overrepresentation of its share in the global market. In addition, we should reiterate that intra-EU trade is excluded from this analysis as, with the exception of items in Annex IV, these trade flows are not subject to the provisions of this export control Regulation.

For the three largest sectors in terms of value (HS 27 'minerals', HS 84 'machinery' and HS 85 'electrical machinery'), the EU accounts for roughly 10 to 20% of world exports and this share is relatively stable over time. The USA becomes an increasingly large player in the 'minerals' market, while China has expanded its share of the global export market for the 'machinery' and 'electrical machinery' markets over time.

Similar results appear in the smaller sectors for HS 39 'plastics', HS 89 'ships' and HS 90 'optical, measuring and medical equipment'. Noteworthy are the large shares for the EU in HS 29 'organic chemicals' and HS 88 'aircraft'. The volatile nature of the EU and US market shares in HS 88 could possibly be explained by the average size and value of individual export transactions in this sector, which are likely to be very high. Regardless, both of these are sectors in which the EU appears to be a major player with on average roughly 40% of the global market.

Across all sectors, most competition tends to come from China, Japan and the United States. In all sectors (except for HS 27 'oil and minerals' and HS 71 'precious metals') those three countries together with the EU make up more than half of world exports. The sectors HS-27 and HS-71 can also be considered somewhat special cases as they mostly concern exports of raw materials. Exports in oil, minerals and precious metals are strongly tied to the location of natural reserves of these products, which make the export origin pattern more scattered compared to products that can be produced at larger scales in central locations (such as many manufactured products). Moreover, we know that only a few dual-use codes are relevant in these large sectors. Therefore, we conclude that the competition from the USA, China and Japan is most important in the context of the review of the Regulation. Of these competitors, the US share of the global export market tends to be stable over the last decade. Japan and China, on the other hand, move in opposing directions, where the former tends to see its market share declining. This is especially visible in HS 89 'ships' and HS 29 'organic chemicals'. China's market share increases in virtually all relevant sectors.

4.6.2 Revealed Comparative Advantage

A Revealed Comparative Advantage (RCA) is a measure that compares the relative share of exports of a country to that of its competitors: in this case the relative share of exports of the EU in a single HS-2 sector with the relative share of exports for the five largest competitors (countries with the largest shares on the world export market) in that sector. This can be derived from the following formula:

RCA = $(E_{ij} / E_{it}) / (E_{nj} / E_{nt})$, where E = exports, i = the EU, j = all dual-use related HS codes in the selected top-10 sector, t = total exports, n = a country from the reference group with largest exporters in that sector.

In cases where the RCA takes up a value higher than 1, the EU is said to enjoy a revealed comparative advantage in that sector. This means that the relative share in total exports of the EU in that sector is larger than the relative share of their competitor(s).

Figure 4.9 (Annex 1) shows that the EU does not have a comparative advantage in most of the sectors. Only in the relative small sectors HS 29 and HS 88 does the EU enjoy a comparative advantage against its major competitors. For most other sectors, the EU has a comparative advantage only vis-à-vis a single country. The reasons that could explain the development of the EU's comparative advantage could be multiple (it would take a different type of research and study in order to reveal these reasons), but we should take into account that due to the construction of the reference group of the RCA (taking the five largest competitors), one always compares the EU performance against the countries that export the largest share of these products on the world market, which are in turn likely to also constitute large shares of their domestic export basket. The value of the RCA is (in turn) highly dependent on a country's export profile. Countries with a diversified portfolio of exports (such as the EU) will automatically have smaller sector's export shares compared to a country with a less diversified portfolio (in given sectors).

When analysing the three main competitors identified in the previous section (China, Japan and the USA), some preliminary conclusions can be drawn. The EU's RCA vis-à-vis China shows either of two scenarios. On the one hand, in the chemicals sectors (HS sectors 29, 38 and 39), the EU has a comparative advantage. On the other, China has a revealed comparative advantage in the manufacturing sectors (HS sectors 84, 85 and 89).

Japan seems to have a revealed comparative advantage vis-à-vis the EU in all sectors in which Japan is represented in the figure below, except for HS 29 'Organic chemicals' and the resource dependent HS 71 'pearls and stones', which is likely triggered by the more 'unbalanced' export structure of Japan as compared to the EU. Japan has traditionally been strong in exporting products in the selected sectors, which thus constitute large shares in their total export profile. On the world market, the export share of Japan is in fact very slowly diminishing. Finally, the comparative position of the USA vis-à-vis the EU is strengthening in two sectors (HS 27 'mineral fuels' and HS 29 'organic chemicals'). In HS 84 'machinery' and HS 88 'aircraft', the roles are reversed and the position of the EU vis-à-vis the US is strengthening over time.

4.7 Synthesis and conclusions

In this chapter, we analysed the EU dual-use industry from a quantitative perspective in order to provide estimates on the size, scope, breadth and characteristics of the dual-use industry in the EU. It is important to collect data on the value and volume of dual-use transactions in the EU, as well as the related production and employment involved so that the impacts of the review of the export control regulation can be put into perspective. In this chapter, we collected data on:

- The number and value of **export licences** granted;
- The value and characteristics of **dual-use related exports;**
- The value of **production** in dual-use related economic sectors;
- The number of **employees** and number of **enterprises** active in dual-use related economic sectors;
- International export market shares and Revealed Comparative Advantages (RCAs) for the EU vis-à-vis its main global competitors in dual-use related exports.

No central database covering economic indicators on dual-use goods and technologies exists and therefore the above indicators had to be collected from a variety of sources. However, all (except for the data on export licences) have in common that they are based on the Annex I to CN codes correlation table developed by DG TAXUD, which matches Annex I dual-use codes to the closest matching products defined in customs trade statistics classification (Common Nomenclature). We have used the latest correlation table, made available on 1-Jan-2015.[48] Even though it provides a very helpful match between all dual-use items covered by the Regulation (thus relevant for the impact assessment of the review of this Regulation), it suffers from several limitations that complicate the data analysis conducted in this chapter.

Most importantly, the correlation is a many-to-many relationship and even though statistics at eight-digit level are the most detailed available, the relevant CN-8-digit codes also include non-dual-use related products. As a result, most of the estimates presented in this chapter overestimate the actual size of the dual-use industry in the EU. In order to circumvent this limitation, we have compared the estimates on the dual-use industry with the value of export licences granted for dual-use item and conducted a complementary analysis based on detailed trade data from the Dutch Customs Office, including information on whether or not the product was included on the EU dual-use list. Based on a study simultaneously conducted for the JRC by King's College London (Stewart, 2015), we are also able to compare the production estimates with his estimates that have been validated using additional expert judgement. **Table 4.26 (Annex 1) lists the main indicators for the collected data in this chapter.**

On the precise value of dual-use exports, the analysis in this chapter showed that the value of dual-use *related* exports (intra- and extra-EU) was approximately €1,100 billion in 2013. However, total export licence authorisations in 2013 equalled €49.2 billion, constituting approximately 1.1% of total EU exports. Versino found that dual-use related exports might overestimate dual-use exports by a factor of 6.2.[49] This implies that actual dual-use exports account for around 3.9% of total EU exports, close to EUR 180 billion.

Licensing authority data also has its limitations as not all Member States report in equal detail and not all cover all licence types. To get a better insight into the size of actual dual-use exports, we made use of data provided by the Netherlands and Denmark. The Netherlands supplied customs data for dual-use exports from the Netherlands (extra-EU) in 2014, as well as data on actual dual-use exports, sourced from Box 44 of the SAD. Based on this data, the value of *actual* dual-use exports is calculated to be 2.3% of total extra-EU exports, or 7.8% of dual-use related extra-EU exports for the Netherlands. For Denmark, based on data provided by the Danish Licensing Authority, the actual exports of Danish dual-use goods subject to licence applications is calculated to be 0.1% of total Danish exports (intra- and extra-EU), and 1.2% of extra-EU dual-use related exports. These figures show that actual dual-use exports are only a small part of dual-use related exports and the overestimation in these two cases is larger than found by Versino.[50] It should be noted that the share of dual-use exports of an individual country is highly dependent on the export structure

[48] See: <http://trade.ec.europa.eu/doclib/html/153050.htm>.

[49] Versino (note 28).

[50] Versino (note 28). This difference stems from the fact that Versino only uses licensing data while the case studies for Denmark and the Netherlands are based on customs data. The overestimation of six times is based on the assumption that all products that obtained a license are exported, while in reality often only part of them are actually exported. The overestimation is therefore likely to be larger than six times.

of an economy (whether or not a country has a dual-use industry and/or what the share of other exports are), and could therefore significantly differ by Member State.

The more detailed trade data analysis based on dual-use related (CN-8) exports showed that the sectors HS84 [Machinery and mechanical appliances], HS85 [Electrical machinery and equipment] and HS88 [aircraft & spacecraft] make up the three most important sectors in terms of total value of dual-use related exports. The Dutch Customs data confirmed that the 'Machinery' (HS84) and 'Electrical machinery' (HS85) remain the most important exporters of dual-use items also when correcting for the overestimation in the trade data analysis using the correlation table. In the global market place, the EU has a market share of approximately 20% in dual-use related machinery exports and approximately 10% in electrical machinery exports. Both market shares have been relatively stable in the past 10 years. In both markets, the global market share of China is increasing strongly. In terms of relative revealed competitiveness (RCA) in these markets, the EU is increasing its competitive advantage over the USA in the 'machinery' sector, but is not running a relative comparative advantage in the 'electrical machinery' market vis-à-vis all of the four major global competitors.

The analyses on domestic EU dual-use related production, employment and enterprises suffered from an even greater lack of detail in the sectoral disaggregation of the data, so that the data for these indicators is likely to be even more approximate than the dual-use related export data based on the correlation table (which is likely overestimated approximately tenfold as explained above). According to our analyses, production in dual-use related products in the top-10 sectors (based on extra-EU export value) in the EU-28 equalled more than €600 billion in 2013. However, we need to consider that the use of the correlation table overstates the actual value of dual-use goods. If we account for that, production is roughly equal to €102 billion in 2013. According to Stewart (2015), who applied expert judgement to estimate the share of *actual* dual-use products contained in the PRODCOM database and finds that for most PRC product codes only 2-5% of production is dual-use related, the total dual-use production value in the EU lies between €27 and €36 billion in 2013.

The number of people employed in dual-use related economic sectors (based on NACE classification) equalled 7.8 million in 2012, up from 6.9 million in 2011. The number of active enterprises in the same dual-use related NACE sectors in the EU-28 equalled between 374,000 and 382,000 in 2011 and 2012. For both these indicators, however, it should again be noted that the shares of *actual* dual-use related employment and enterprises are likely to be a small fraction of this (likely even smaller than 3% due to a probably higher share of non-dual-use related activity included in the NACE 4 digit classification).

Therefore, we must conclude that there is very little accurate data on the EU dual-use industry. Even though the obtained estimates on the likely share of actual dual-use exports of a country's total exports (~3%) in this study is in line with other literature, improving data collection on the dual-use industry in the EU will be required to enhance research to support policy making and impact assessments. The case study using data from the Dutch Customs Office showed that gathering much more detailed trade statistics, including the information in Box 44 of the SAD supplied by exporters, generates very relevant and accurate data on actual dual-use exports and could be interesting to conduct at the EU level. But it also revealed that data preparation and collection at the level of customs authorities in the EU could further improve. A very useful next step in dual-use export research would be to analyse the detailed customs data from all EU-28 Member States separately or in a harmonized manner in order to improve estimates on dual-use exports than what is currently known at the European level.

5. Analysis of review options

5.1. Introduction

One deliverable of this study is an analysis of the review options presented by the European Commission in the April 2014 Communication 'for the modernisation of EU export controls and their adaptation to rapidly changing technological, economic and political circumstances'. While the results of the data collection on the impact of the review options on stakeholders in the private and public sector are compiled in Chapter 6, this chapter seeks to unpack the actions under these options.

In order to collect data and information regarding the impact of the review options on the different stakeholders, we analysed the Commission Communication and the Roadmap of the review process. We structured them into review options, issues and actions, for greater ease of reference in the consultation process, and to enable the gathering of comparable qualitative and quantitative data. We also sought to identify the relevant issues and actions for specific stakeholder groups as some issues are more relevant to companies, while others more directly impact licensing authorities.

The roadmap for the review process categorises the different review actions into five broad review options: (1) No policy change; (2) Implementation and Enforcement Support; (3) EU System Update; (4) EU System Modernisation; and (5) an EU System Overhaul. The Roadmap specifies that elements of Option 2 could also be included in Option 3. Similarly, Option 4 may also contain elements of the previous options 2 and 3, but would add controls on exports of cyber-surveillance technologies from the EU. Option 5 (the 'full harmonisation and centralisation of controls'), is not further detailed in the Communication. Options 2 through 4 include a substantial number of review actions, which are grouped under review issues. Issues relating to the potential impact of Review Option 4 are discussed in Chapter 7.

The analysis below is first considers the review options from the perspectives of different stakeholders to highlight that some would affect some more than others (Chapter 5.2.). It then looks at the review actions structured according to four 'priorities' of the Commission Communication (Chapter 5.3.): (1) 'adjust to the evolving security environment and enhance the EU contribution to international security'; (2) 'promoting export control convergence and a global level-playing field'; (3) 'develop an effective and competitive EU export control regime'; and (4) 'support effective and consistent export control implementation & enforcement'.

5.2 Impact of review options on different groups of stakeholders

5.2.1 General observations

One of the key messages conveyed during interviews is that compliance costs increase with the vagueness of legal provisions, since a substantial amount of time has to be invested in exploring whether a company is affected, or captured by certain legal provisions. A related distinction applies to the catch-all for cyber-surveillance: if governments have a legal possibility to impose control requirements on specific products, this may have some impact on competition and exports, but minimal impact on compliance costs. If the catch-all includes a responsibility for companies to inform the authorities if they have reason to believe that human rights or human security may be compromised, they will have to include human rights competences into their compliance staff, which has additional training costs and resource implications.

As regards the measurement of compliance costs, companies appear reluctant to measure compliance costs. First, it seems impossible to separate compliance costs for sanctions[51] and other countries' export control regulations (in particular the US) from compliance costs with the EU Dual-use Regulation. Second, for sectors that are subject to various regulatory regimes (transport, health, safety and environmental regulation; or import controls in addition to export controls as is the case for the chemical sector based on the CWC), they would at most measure compliance costs overall. Third, compliance costs are cross-cutting, and can either be narrowly defined in terms of the salary cost of the compliance officer(s) (in which case differences may reflect variations in salary costs more than for compliance efforts); costs for relevant software (which however would include screening for listed entities based on sanctions); or the percentage in terms of salary costs for all employees and IT programmes, where the philosophy is to mainstream compliance into all company routines. Fourth, compliance controls are built into the everyday business processes spread over multiple functional activities such as finance, sales, procurement and operations. This makes it difficult to measure the true cost of compliance, even where there is a compliance department within a company that is clearly budgeted.

Finally, many stakeholders interviewed or consulted had little awareness or in-depth knowledge of the Commission Communication and the associated review options. A number of those who did commented on the vagueness of the options at this stage and the resulting difficulty to predict impact.

5.2.2 Implications for the transport sector

Today's complex trading environment encompasses a wide range of supply chain actors, including integrators, shipping lines (from ocean liners to smaller shipping companies that may be subcontracted by larger carriers), shipping agents, freight forwarders and customs agents, as well as air carriers, road transport, fast parcel operators and postal services, brokers, and even insurance companies and financial institutions. Some of these terms and associated activities overlap, and are understood differently in different countries and communities, but tend to relate to different functions and degrees of responsibility. As explained in Chapter 3.3, these actors are not the manufacturers of the commodities and only rarely act as surrogate owners or exporters. They therefore tend to have very little or no information about the products they transport or trade.

One stakeholder called the transport sector the 'forgotten piece of export control regulations'. The transport sector is one example of a sector that is directly affected

[51] Sanctions include a range of measures, which may include dual-use trade control elements. While the latter fall within the scope of dual-use export controls, although regulated through instruments complementary to the EU Dual-use Regulation, many other sanctions measures clearly lie outside the scope of dual-use export controls.

only by a limited number of review options, although the overall review and changes in the dual-use industry may have indirect implications. The transport sector would be impacted by a 'clarification' of the export and exporter concepts; possible convergence of Internal Compliance Programme (ICP) requirements with the AEO status; ICP requirements; and a 'clarification' of brokering (see also Chapter 3.3). The Dual-use Regulation explicitly exempts transport as ancillary services from the coverage of brokering activities.

The current EU Dual-use Regulation only defines the exporter. The role of the transport provider in relation to dual-use exports is regulated in the context of standard customs processes. In the US, the Export Administration Regulations (EAR) define export compliance as a responsibility of all parties in transactions subject to the EAR, but clearly state that acting through a forwarding or other agent, or delegating or redelegating authority, does not in and of itself relieve anyone of responsibility for compliance with the EAR. The EAR also distinguishes between the exporter and exporting carrier.

In this context, the practicalities of transit controls need to be kept in mind. A transporter completes his obligations under the customs regime in the country in which he is located for this transaction. This involves submission of a customs declaration and supporting documentation as supplied by the owner/exporter, including export invoices and, where required, an export licence. If no export licence is supplied by the exporter, and there is no further indication of a licence/control requirement on the export invoice or via the TARIC code, the shipment is submitted to the relevant Customs Authority and once released, shipped accordingly. Additionally, while export control is the main focus of most EU Member States, transit (including transhipment) is the main concern in other EU countries, mainly as a function of industrial structures and trade flows. This also has implications for the transport sector.

There are a number of processes involving the transporter at the point of export that are possible areas for the development of internal compliance guidance or requirements specifically for this sector. These include the information provided on commercial invoices; customer statements; restricted party screening; transit routes; the provision of tools for commodity identification; and support. It was mentioned that: 'the regulatory authorities at European and country level provide very little for the transportation industry in the form of tools, communication, outreach training or help desk support'. Therefore both the clarification of legal responsibility and the design of appropriate compliance guidelines and tools were identified as useful options during stakeholder consultations.

The responsibility of the transporter to manage dual-use items largely depends upon the definition of 'export' and 'exporter'. A transportation company would not usually consider themselves as being the exporter of the goods unless the transportation company was acting as an 'exporter of record' on behalf of the owner of the goods being exported. A transport company or a customs broker, completing customs export formalities, would consider themselves to be acting as an appointed agent on behalf of the owner/exporter of the goods, based upon documentation and data provided by the owner/exporter. In context of the EU Dual-use Regulation there are no direct or indirect references to the responsibilities of a transportation company in relation to a dual-use export. There is therefore scope for clarifying the concept of 'export' and 'exporter' and to further define the responsibilities of the actors in the supply chain.

5.2.3 Implications for academia of ITT controls

The review issues include controls of intangible transfers of technology. There is currently a discussion to what extent research falls under 'basic scientific research', which according to 428/2009 means 'experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical objective.' This definition has been considered open to interpretation. In academia, there are concerns that interpretations may negatively impact the freedom of academic research and exchange, for example as regards biological research conducted by the Erasmus Medical Centre in Rotterdam on the transmissibility of H5N1 virus in ferrets. The Dutch authorities decided that a licence was required for publication for this research group, lead by Ron Fouchier and based in the Netherlands. The export licence was issued and the article published in June 2012.[52]

Fouchier subsequently challenged the licensing requirement in court. The district court in 2013 confirmed the approach taken by the authorities, citing the EU Dual-use Regulation. It referred to the rationale behind the Regulation according to the preamble, which refers to 'international commitments and responsibilities (…) especially regarding non-proliferation'.[53] The court argued that:

> "It is apparent from the recitals in the Regulation (…) that the Regulation imposes (…) an obligation (…) to prevent (…) the proliferation of biological weapons and that this control system should be effective and appropriate. The recitals to the Regulation make no mention of exceptions to which the controls do not apply. The importance of basic scientific research is not mentioned in them. The same applies to the enacting provisions of the Regulation. Not until the list in Annex I to the Regulation (…) is there a General Technology Note (GTN) (…). The last paragraph of this GTN states that controls on 'technology' transfer do not apply to information 'in the public domain', to 'basic scientific research' or to the minimum information necessary for patent applications."[54]

While the 'District Court endorses the defendant's view that the exceptions to the authorisation requirement should be interpreted restrictively', it states that the 'obligations which the Regulation imposes on the member states cannot be adequately observed in the case of the non-proliferation of the items specified in Annex I if it is left to the researchers themselves to determine whether their work falls under basic scientific research in a general sense, without taking note of the context of the Regulation.' The court concludes that publication delays due to licensing requirements are outweighed by security interests. It argued that: 'When competing interests are

[52] Enserink, M., 'Dutch appeals court dodges decision on hotly debated H5N1 papers', *Science*, 16 July 2015.
[53] Haarlem district court, Ruling of 20 Sep. 2013, unofficial translation.
[54] Ibid.

weighed, the interests of (…) adequate non-proliferation controls must take precedence.'

However, the court of appeal annulled the ruling of the lower court, although not on substantive grounds. Rather, this was based on the reasoning that Fouchier had been granted an export licence and used it. The ruling argued as follows: 'The court is of the opinion that, if appeal in a specific case can't lead to a favourable decision for the appellant, no legal assessment can be given on the basis of the significance of possible future cases.'[55]

It appears that no similar case has so far occurred in the EU. A number of cases in non-EU countries are however relevant.

A US group led by another scientist was conducting similar research. Following longer discussions and involvement of the US National Science Advisory Board for Biosecurity (NSAAB), their research was published without an export licence, before Fouchier's publication.[56] It appears that this may have been also due to difference between their research approaches and the substance of the publication, not only due to differences in control approaches. In 2013 two California researchers decided to withhold some methodology information required to permit others to reproduce the research until such time as effective treatments were developed.[57] Australia recently introduced a licensing requirement for those that put controlled technology into the public domain, although penalties for non-compliance will only enter into force 2 years after the provisions themselves. This has also been subject to controversy in academia in Australia.

The H5N1 case is key to the consideration of control and oversight of basic research. Concerns about the impact on academic freedom relate partly not only to the need to publish in the academic world, where publication is the modus operandi, but also due to the inherent interest to the first to publish a new methodology or approach. There is thus an inherent interest in a level playing field between academics regarding control requirements.

In addition to concerns about controls inhibiting academic freedom and the consequent need to balance this with security, a number of practical considerations arise. One of them is the required expertise in a very wide range of highly advanced research areas on the part of licensing authorities. This point was raised by one stakeholder interviewed, who stated that the competent licensing authority lacked the technical expertise to understand the research undertaken. This issue was illustrated in the case of a US professor who was arrested based on charges that he had shared confidential information with a foreign student. However, this professor has since been

[55] Appellate court of Amsterdam, Ruling of 18 June 2015, unofficial translation.
[56] Enserink , M., 'Dutch appeals court dodges decision on hotly debated H5N1 papers', *Science*, 16 July 2015.
[57] Jason R. Barash and Stephen S. Arnon, 'A novel strain of Clostridium botulinum that produces Type B and Type H botulinum toxins', *Journal of Infectious Diseases*, 7 Oct. 2013. Article received 17 May 2013 and accepted on 5 August 2013.

released. According to media reports the technology he had shared was not in fact the technology which investigators claimed he had shared.[58]

A different approach to ITT controls is the imposition of classification requirements. In the commercial world, there will also be issues related to intellectual property rights, but that necessarily is a separate issue since commercial research clearly falls into the area of applied research and is therefore subject to control.

Yet another possible, complementary approach is the development of codes of conduct for scientists, which is also included in the review options. In fact, the issue of ITT controls is closely related to research ethics as well as biosafety and biosecurity considerations (see Chapter 3), for example regarding research in the life sciences through which scientists re-create extinct or create new pathogens.

Less controversial is the requirement for all entities, including universities, to apply for a licence to export controlled biological items. Biological agents are mainly items that are not commercially traded with the exception of biorepository items from biobanks, for which most items are unlikely to be controlled. Also non-commercially traded biological items require a licence if they leave the EU. There appears to be a low degree of awareness of this, and more broadly of the EU Dual-use Regulation with those involved in the transfer of biological materials, in particular in academia. This touches upon another review action, the 'targeted and coordinated outreach to academic research communities throughout the EU'.

One issue that is closely related, concerns the way of transmitting the information. While the Dual-use Regulation covers the export of technology through electronic means as well as through the physical export via a laptop or USB-stick, the export in a scientist's brain, so to speak, and subsequent oral explanation at a conference outside the EU is regulated through technical assistance provisions. The EU Joint Action on technical assistance of 2000[59] has not been implemented by all EU Member States as yet, and moreover is implemented in different ways. Generally, controls are however limited to technical assistance for WMD purposes or a military end-use in an embargoed destination, not to the sharing of controlled technology for civilian purposes.

[58] 'U.S. Drops Charges That Professor Shared Technology With China, *New York Times*, 12 Sep. 2015.

[59] 'Council Joint Action of 22 June 2000 concerning the control of technical assistance related to certain military end-uses. 2000/401/CFSP', *Official Journal of the European Communities*, L159, 30 June 2000, pp. 216–217.

5.2.4 Impact of Annex II and Annex IV[60]

EU General Export Authorization EU001 permits the export of certain items to seven countries with a notification procedure. Those are all items listed in Annex I of the Dual-use Regulation except for the items on Part 2 of Annex II and Annex IV. Moreover, Annex IV items require a permit for intra-Community transfers. To explore the size of the EU industry affected by the current scope of Annex II and Annex IV, SIPRI has analysed trade data to estimate the upper threshold of the intra-EU and extra-EU exports, using the methodology outlined below.

First, we estimated the value of extra and intra-EU exports of dual-use goods which are outside the scope of the EUGEA EU001, that is to say the total value of exports of items on Part 2 of Annex II, including Annex IV. The EU correlation table was used to identify the CN codes falling under the relevant Export Control Classification Numbers (ECCNs). The data for the export values of those CN codes were obtained from the trade database provided by Eurostat.

As was explained in Chapter 4, the CN code and ECCN based research entails difficulties in precisely estimating the size of dual-use exports due to the limitation in revealing the dual-use nature of the traded items based on CN codes. Moreover, some CN codes fall under multiple ECCNs. The former makes the size of dual-use exports look far greater than actual dual-use exports. Moreover, it is difficult to estimate the size of a particular industry sector as CN codes can be categorized under different industries. However, as mentioned, since this study focuses on the upper threshold of the size of exports subject to Part 2 of Annex II and Annex IV, the method applied here still produces a useful data set.

Table 5.1 provides the total values of exports of items potentially related to Part 2 of Annex II and Annex IV by ECCN by year. The upper threshold of such exports is between €120.6 billion and €138 billion in the period 2010-14. As mentioned, a number of CN codes exist across multiple ECCNs, so the figures for those items are shown under the cross-cutting item categories in the table. For instance, the export values for CN codes which are subject to the ECCN 1A102, 9A009a and 9A117 of Annex II are incorporated into the 'Cross-cutting Items between Annex II and Annex IV' section of the table, given that those CN codes also include items falling under ECCN 9A117 of Annex IV. The value for 'Cross-cutting Items within Annex IV' means the total value of exports of items related to multiple ECCNs within Annex IV, such as CN36030090 which includes items classified as ECCN 3A229, 3A232, 1A007a and 1A007b of Annex IV.[61]

Setting aside those cross-cutting items, the total upper threshold export value of the items of Annex II shows a constantly decreasing trend in the period of 2010-14. In 2010, the total value of exports was approximately €4.2 billion and plunged to about €2.4 billion in 2014. This drop can be attributed to the decrease in the exports of

[60] SIPRI Guest Researcher Hyuk Kim contributed this section.

[61] CN 30029050 in ANNEX II ('cultures of micro-organism') overlaps with ANNEX IV; however, it was left in ANNEX II due to its representativeness covering both toxic chemicals and biological items. CN30029090 was included in 'Cross-cutting items between ANNEX II and ANNEX IV' since it also covers MTCR technology.

special fissionable materials of which the export value declined from €3.24 billion to €1.38 billion between 2010 and 2014. The other ECCNs have minimal impact on the generally decreasing trend due to their relatively minor values.

Conversely, the export value of items for Annex IV presents an increasing trend between 2010 and 2014. The upper threshold of those exports increased by about €11.3 billion, from €105.1 billion to €116.5 billion during the referenced timeframe. Among many categories under Annex IV, the items with significantly increased export values are 'Noise reduction systems for use on vessels', 'Re-entry vehicles and equipment', and 'Cross-cutting Items within Annex IV'. The exports of items possibly related to the 'Noise reduction systems' increased from €4.7 billion in 2010 to €6.7 billion in 2014, and the main items within that category are vulcanized rubber, cranks and its shafts, and gears and related equipment, which are unlikely to be intended only for noise reduction purposes.

With regard to 'Re-entry vehicles and related equipment', the upper threshold of the value of exports increased from €5.4 billion in 2010 to €8.6 billion in 2014. The items comprising this category are aluminium and beryllium, numerical control panels, programmable memory controllers and boards or cabinets for electric control. In particular, the exports of boards and cabinets were a driving factor for the increasing trend of this category, as the value of such exports increased from approximately €3 billion to €5 billion between 2010 and 2014. The CN codes representing spacecraft, satellites, and sub-orbital and spacecraft launch vehicles were not considered in this sector, as those codes are also subject to ECCN 9A004, which means the figures for those items were incorporated into 'cross-cutting items within Annex IV'.

The export of 'cross-cutting items within Annex IV' increased from €31.5 billion to €37.8 billion in the period 2010-14. This makes it the second largest category of Annex IV, after the 'Equipment designed to perform cryptanalytic functions'. A number of items comprise this category, and most of those items are listed under the Missile Technology Control Regime (MTCR). A broad range of items falls under this category. For example, while CN codes representing space vehicles, radar sets, inertial navigation systems and parts of reaction engines are apparently related to the dual-use items, it is likely that the majority of ICT sector-related items falling under this category (such as data-processing units, keyboards and printers) have no missile-related applications. Among this category, the most notable item with increased export value is CN 85176200, which represents machines for the reception, conversion and transmission or regeneration of voice, images or other data: its export value increased from €5.3 billion to €8.1 billion between 2010 and 2014.

The exports of cross-cutting items from Part 2 of Annex II and Annex IV also show an increasing trend between 2010 and 2014. Most items in this category are also MTCR related items, such as parts for aircraft, suborbital and spacecraft, and helicopters. CN 30029090, which represents toxins and similar products, also falls under this category since it is not only associated with the pathogens of Annex II but according to the correlation table is also related to materials for stealth technology. Under this category, the value of exports under CN 88033000, which represents parts of aeroplanes or helicopters, accounts for approximately 75% of total exports. The exports of CN 88033000 increased from €8.5 billion to €11.7 billion between 2010 and 2014.

Table 5.1. Upper threshold of total exports of items listed in Annex II and Annex IV by EU Member States

SCHEDULE	CATEGORY		ECCN	2010	2011	2012	2013	2014
ANNEX II	Nuclear materials (and ores)	Source materials	0C001	568,936,214	638,947,989	341,017,875	398,965,964	448,658,180
		Special fissionable materials	0C002	3,244,162,112	2,823,416,866	2,966,040,745	1,984,927,852	1,378,474,451
	Cultures of micro-organism	Human pathogens	1C351	370,724,085	416,518,430	482,412,874	515,596,511	567,744,726
		Animal pathogens	1C352					
		Genetic elements and genetically modified organisms	1C353					
		Plant pathogens	1C354					
		ANNEX II TOTAL		**4,183,822,411**	**3,878,883,285**	**3,789,471,494**	**2,899,490,327**	**2,394,877,357**
ANNEX IV	Items of stealth technology	Materials or devices for reduced observables	1C101	128,109,107	88,882,335	83,916,124	78,389,855	106,103,175
		Materials speciallly designed for use as absorbers of eletronicmagnetic waves	1C001	33,164,029	33,560,561	27,816,561	25,116,565	23,767,195
	Items of the Community strategic control	Acoustics	6A001	5,867,094,360	6,845,606,118	7,240,754,427	7,108,296,233	7,824,222,155
		High explosives	1C239	57,935,893	44,609,488	48,800,822	50,119,104	55,297,012
		High-current pulse generators	3A229	204,020,303	205,004,049	195,047,967	187,241,366	179,590,455
		Noise reduction systems for use on vessels	8A002o	4,733,602,027	5,654,266,001	6,056,855,524	6,258,241,551	6,668,768,226
	Items of the Community strategic control-Cryptography	Equipment designed to perform cryptanalytic functions	5A002	43,798,082,057	46,853,151,158	43,942,003,339	40,236,133,359	38,720,364,940
	Items of the MTCR technology	Guidance sets	7A117	1,336,025,463	1,551,849,914	1,695,280,437	1,854,350,474	2,004,937,171
		Production facilities for guidance sets	7B103	103,117,216	146,134,684	174,062,461	165,158,696	179,206,732
		Reentry vehicles and equipment	9A116	5,441,483,914	6,328,224,299	7,164,854,028	7,838,234,721	8,624,723,747
		Specially designed production equipment for rockets	9B115	157,871,157	195,611,277	204,548,919	198,019,646	226,593,845
		Systems usuable in missiles	9A106c	889,165,088	950,911,176	1,208,505,594	1,260,497,650	1,012,087,314
	Items of the NSG technology	Priviously separated neptuni	1C012b	39,962,185	41,826,211	39,788,075	47,423,164	44,237,654
		Lithium isotope separation facilities	1B233b	1,085,713,251	1,167,283,303	1,231,826,226	1,243,574,356	1,311,389,066
		Lithium	1C233	18,263,126	18,764,786	27,254,505	20,273,226	21,842,017
		Tritium production facilities	1B231b	1,253,064,098	1,525,306,360	1,705,586,746	1,733,594,741	1,832,683,134
		Tritium	1C235	168,151,712	169,230,232	204,033,913	157,082,336	154,503,344
		Switching devices	3A228	1,149,320,057	1,210,881,212	1,253,291,695	1,324,772,777	1,211,526,327
		Neutron generator systems	3A231	31,705,159	36,083,198	58,387,682	35,158,710	30,310,299
		Cameras and components	6A203	4,042,939,634	4,391,204,093	4,865,027,948	4,672,227,317	4,782,554,259
		Pressure sensors	6A226	2,324,108,075	2,498,282,315	2,854,495,597	2,973,937,524	3,200,526,832
		Velocity interferometers	6A225	753,188,930	552,262,935	170,994,583	329,973,801	442,221,530
	Cross-cutting Items within ANNEX 4			31,514,995,512	34,764,487,699	38,935,324,477	37,984,876,410	37,802,751,398
		ANNEX IV TOTAL		**105,131,082,353**	**115,273,423,404**	**119,388,457,650**	**115,782,693,582**	**116,460,207,827**
Cross-cutting Items between ANNEX II and ANNEX IV				**11,305,509,338**	**12,386,911,202**	**14,765,343,391**	**14,946,090,760**	**15,234,371,806**
GRAND TOTAL				**120,620,414,102**	**131,539,217,891**	**137,943,272,535**	**133,628,274,669**	**134,089,456,990**

Although Table 5.1 illustrates an approximate picture of the exports of items subject to Annex II and Annex IV, this still does not fully cover exports related to CGEA E001, since the exports of cross-cutting items or items with low correlation account for significant portions of the total value in that table. Moreover, this CGEA is available for only seven countries listed in Annex II (Australia, Canada, Japan, New Zealand, Norway, Switzerland and the United States). Therefore, in order to have a clearer estimate of the size of exports currently outside the scope of this authorization, it is necessary to conduct a data analysis with CN codes having a relatively better correlation by country listed in Annex II.

For that purpose, five item categories were selected based on the dual-use nature that can be deduced from the official description of each CN code: Spacecraft and parts; Guidance sets; Items of stealth technology; Nuclear materials; and Pathogens. Some CN codes falling under those categories were omitted as the scope of the descriptions of those codes is too broad to be categorized as dual-use items. For instance, CN 90318038, which classifies traded items as 'Electronic instruments, apparatus and machines for measuring or checking', was omitted from the 'Items of Stealth technology' category while CN 85261000, 'Radar apparatus', remains under that category. The list of CN codes used for this research is listed in Table 5.2.

Table 5.3 presents the export values of items listed in Table 2 by item category and by each country. The total value of such exports increased from approximately €7 billion to €9.4 billion between 2010 and 2014, except for the dip in 2012. In other words, exports of selected items that could possibly be affected by a prospective revision to CGEAs and to Annex IV were generally increasing in value for the last five years.

In most cases, the United States accounts for more than 70% of exports for each item category, while the exports to the other six countries are relatively minor. In the case of nuclear materials exports, Japan could be considered as a significant trading partner for the EU, as the Japanese share of that category is more than 20%. Among the CN codes related to the nuclear materials category, the main items exported to Japan are CN 26209995 (Slag, ash and residues containing metals), 72029980 (Ferro-alloys), 84013000 (Fuel elements) and 28442035 (Uranium enriched in U 235 and its compounds) and the descriptions of those CN codes show that the last two items are clearly representing the export of nuclear materials. As to the export of items of stealth technology (essentially radar apparatus) between 2010 and 2014, after the United States, Canada, Switzerland and Japan were the main trading partners. While the Canadian and Swiss shares tended to decrease after 2012, Japan remained as a constant significant trading partner for the EU.

Even though Table 5.3 shows a relatively clearer picture than Table 5.1, it is still not possible to estimate the exact size of exports related to the General Authorization, as some CN codes used for this analysis are still too broad to be classified as dual-use items. For example, CN26121010 and CN26121090, which represent uranium ore products, are not categorized as nuclear material in practice since the IAEA definition of nuclear materials excludes ores and their residues. Also, it is unclear if the two CN codes 26209995 and 72029980 mentioned in the previous paragraph always represent nuclear materials. In regard to the pathogen category, it is uncertain that items declared under the CN codes in that category are actual pathogens.

Table 5.2. List of CN codes for analysis

CATEGORY	CN CODE	DESCRIPTION
Items of stealth technology	85261000	Radar apparatus
Guidance sets	85269120	Radio navigational receivers (excl. radar apparatus)
	85269180	Radio navigational aid apparatus (excl. receivers and radar apparatus)
	85269200	Radio remote control apparatus
	90141000	Direction finding compasses
	90142020	Inertial navigation systems for aeronautical or space navigation (excl. compasses and radio navigational equipment)
	90142080	Instruments and appliances for aeronautical or space navigation (excl. inertial navigation systems, compasses and radio navigational equipment)
	90148000	Navigational instruments and apparatus (excl. for aeronautical or space navigation, compasses and radio navigational equipment)
	90149000	Parts and accessories for compasses and other navigational instruments and appliances, n.e.s.
Nuclear Materials	26121010	Uranium ores and pitchblende, with a uranium content of > 5% by weight [Euratom]
	26121090	Uranium ores and concentrates (excl. uranium ores and pitchblende, with a uranium content of > 5% by weight)
	26122010	Monazite; urano-thorianite and other thorium ores, with a thorium content of > 20% by weight [Euratom]
	26122090	Thorium ores and concentrates (excl. monazite, urano-thorianite and other thorium ores and concentrates, with a thorium content of > 20% by weight)
	26209995	Slag, ash and residues containing metals or metal compounds (excl. those from the manufacture of iron or steel and those containing primarily zinc, lead, copper, aluminium, nickel, niobium, tantalum, tin or titanium, those containing arsenic, mercury, thallium or their mixtures of a kind used for the extraction of arsenic or those metals or for the manufacture of their chemical compounds and those containing antimony, beryllium, cadmium, chromium or their mixtures)
	28441010	Natural uranium, crude; waste and scrap, of natural uranium [Euratom]
	28441030	Natural uranium, worked [Euratom]
	28441050	Alloys, dispersions incl. cermets, ceramic products and mixtures containing natural uranium with iron or compounds of natural uranium with iron "ferro-uranium"
	28441090	Compounds of natural uranium; alloys, dispersions incl. cermets, ceramic products and mixtures containing natural uranium or compounds of natural uranium [Euratom] (excl. ferro-uranium)
	28442025	Alloys, dispersions incl. cermets, ceramic products and mixtures containing uranium with iron enriched in U 235 "ferro-uranium"
	28442035	Uranium enriched in U 235 and its compounds; alloys, dispersions incl. cermets, ceramic products and mixtures containing uranium enriched in U 235 [Euratom] (excl. ferro-uranium)
	28442051	Mixtures of uranium and plutonium with iron "ferro-uranium"
	28442059	Mixtures of uranium and plutonium [Euratom] (excl. ferro-uranium)
	28442099	Plutonium and its compounds; alloys, dispersions incl. cermets, ceramic products and mixtures containing plutonium or compounds of this product (excl. mixtures of uranium and plutonium)
	28443011	Cermets containing uranium depleted in U 235 or compounds of this product
	28443019	Uranium depleted in U 235; alloys, dispersions, ceramic products and mixtures, containing uranium depleted in U 235 or compounds of this product (excl. cermets)
	28443051	Cermets containing thorium or compounds of this product
	28443055	Thorium, crude; waste and scrap, of thorium [Euratom]
	28443061	Bars, rods, angles, shapes and sections, sheets and strips, of thorium [Euratom]
	28443069	Thorium, worked; alloys, dispersions, ceramic products and mixtures containing thorium or compounds of this product [Euratom] (excl. cermets and bars, rods, angles, shapes and sections, sheets and strips)
	28443091	Compounds of thorium or of uranium depleted in U 235, whether or not intermixed [Euratom] (excl. thorium salts)
	28443099	Thorium salts
	28444010	Uranium derived from U 233 and its compounds; alloys, dispersions incl. cermets, ceramic products and mixtures containing uranium derived from U 233 or compounds of these products
	28445000	Spent "irradiated" fuel elements "cartridges" of nuclear reactors [Euratom]
	72029980	Ferro-alloys (excl. ferro-manganese, ferro-silicon, ferro-silico-manganese, ferro-chromium, ferro-silico-chromium, ferro-nickel, ferro-molybdenum, ferro-tungsten, ferro-silico-tungsten, ferro-titanium, ferro-silico-titanium, ferro-vanadium, ferro-niobium, ferro-phosphorus and ferro-silico-magnesium)
	84013000	Fuel elements "cartridges", non-irradiated, in casing with handling fixtures, for nuclear reactors [Euratom]
Pathogens	30029050	Cultures of micro-organisms (excl. yeasts)
	30029090	Toxins and similar products, e.g. plasmodia (excl. vaccines and cultures of micro-
Spacecraft and parts	84121000	Reaction engines other than turbojets
	88026010	Spacecraft, incl. satellites
	88026090	Suborbital and spacecraft launch vehicles
	88031000	Propellers and rotors and parts thereof, for aircraft, n.e.s.
	88032000	Under-carriages and parts thereof, for aircraft, n.e.s.
	88033000	Parts of aeroplanes or helicopters, n.e.s. (excl. those for gliders)
	88039010	Parts of kites
	88039020	Parts of spacecraft, incl. satellites, n.e.s.
	88039030	Parts of suborbital and spacecraft launch vehicles, n.e.s.
	88039090	Parts of aircraft, n.e.s. (excl. of spacecraft, incl. satellites, and suborbital and spacecraft launch vehicles)

Table 5.3. Export of selected items from Annex II and IV

CATEGORY	COUNTRY	2010		2011		2012		2013		2014	
Spacecraft and parts	Australia	118,121,123	3.40%	223,407,667	5.92%	134,125,092	2.84%	145,669,790	2.96%	202,485,473	3.28%
	Canada	260,462,301	7.50%	253,959,828	6.73%	302,486,781	6.41%	335,475,395	6.81%	695,241,088	11.27%
	Japan	76,278,097	2.20%	109,734,534	2.91%	121,508,693	2.57%	116,525,374	2.37%	176,173,942	2.86%
	New Zealand	16,597,374	0.48%	24,658,718	0.65%	23,335,358	0.49%	27,296,541	0.55%	55,400,225	0.90%
	Norway	122,943,138	3.54%	126,013,315	3.34%	147,398,675	3.12%	111,147,236	2.26%	242,040,160	3.92%
	Switzerland	260,829,511	7.51%	284,738,741	7.55%	303,934,789	6.44%	337,382,567	6.85%	403,631,278	6.54%
	United States	2,616,130,398	75.36%	2,750,381,098	72.90%	3,686,148,769	78.11%	3,853,215,951	78.21%	4,394,772,932	71.23%
Spacecraft and parts Total		**3,471,361,942**		**3,772,893,901**		**4,718,938,157**		**4,926,712,854**		**6,169,745,098**	
Guidance sets	Australia	58,646,505	5.64%	43,256,164	4.13%	53,614,269	4.57%	52,900,483	4.16%	50,402,952	3.44%
	Canada	59,513,785	5.72%	69,235,777	6.61%	78,298,235	6.68%	72,444,646	5.69%	75,657,660	5.16%
	Japan	69,233,262	6.66%	78,962,906	7.54%	102,841,242	8.77%	91,312,622	7.17%	71,501,699	4.88%
	New Zealand	2,611,752	0.25%	3,128,110	0.30%	2,845,083	0.24%	4,070,085	0.32%	8,849,020	0.60%
	Norway	95,531,947	9.19%	88,149,603	8.42%	96,344,695	8.22%	97,152,535	7.63%	103,704,768	7.08%
	Switzerland	100,455,911	9.66%	110,630,099	10.57%	106,960,373	9.13%	148,171,725	11.64%	138,844,389	9.48%
	United States	653,753,558	62.88%	653,344,483	62.42%	731,250,911	62.39%	807,017,852	63.39%	1,016,270,913	69.36%
Guidance sest Total		**1,039,746,720**		**1,046,707,142**		**1,172,154,808**		**1,273,069,948**		**1,465,231,401**	
Items of stealth technology	Australia	5,767,496	5.69%	4,155,219	3.22%	10,030,391	4.66%	21,849,122	9.68%	6,745,250	2.87%
	Canada	16,273,725	16.05%	32,132,898	24.91%	13,632,682	6.34%	13,649,664	6.05%	15,978,607	6.80%
	Japan	19,334,222	19.06%	17,618,996	13.66%	49,810,150	23.16%	37,458,305	16.60%	36,160,331	15.39%
	New Zealand	511,224	0.50%	820,230	0.64%	681,675	0.32%	692,478	0.31%	279,797	0.12%
	Norway	6,104,648	6.02%	3,997,164	3.10%	9,889,251	4.60%	11,395,657	5.05%	7,531,282	3.20%
	Switzerland	10,723,157	10.57%	9,608,161	7.45%	13,719,905	6.38%	13,558,281	6.01%	13,830,499	5.89%
	United States	42,704,562	42.11%	60,673,434	47.03%	117,271,234	54.54%	127,004,849	56.29%	154,471,755	65.73%
Items of stealth technology Total		**101,419,034**		**129,006,102**		**215,035,288**		**225,608,356**		**234,997,521**	
Nuclear Materials	Australia	2,468,056	0.14%	5,293,873	0.32%	4,302,683	0.25%	1,595,426	0.15%	2,977,547	0.34%
	Canada	15,691,991	0.89%	3,508,422	0.21%	12,715,252	0.75%	10,617,552	1.02%	26,769,023	3.07%
	Japan	407,824,224	23.25%	546,369,644	32.77%	357,750,339	21.00%	177,855,226	17.04%	190,824,012	21.88%
	New Zealand	550,786	0.03%	391,900	0.02%	387,278	0.02%	520	0.00%	2,377	0.00%
	Norway	1,644,240	0.09%	1,311,917	0.08%	648,948	0.04%	568,160	0.05%	706,167	0.08%
	Switzerland	1,846,324	0.11%	56,754,976	3.40%	100,861,232	5.92%	42,727,964	4.09%	28,871,402	3.31%
	United States	1,324,076,049	75.48%	1,053,703,018	63.20%	1,226,820,503	72.02%	810,228,045	77.64%	621,810,955	71.31%
Nuclear Materials Total		**1,754,101,670**		**1,667,333,750**		**1,703,486,235**		**1,043,592,893**		**871,961,483**	
Pathogens	Australia	46,030,084	6.96%	60,880,370	9.07%	70,155,698	10.09%	63,879,986	8.85%	64,851,237	9.20%
	Canada	51,483,930	7.78%	53,020,210	7.90%	59,632,643	8.58%	64,805,051	8.97%	65,919,408	9.35%
	Japan	18,948,971	2.86%	20,721,772	3.09%	22,521,263	3.24%	29,535,736	4.09%	19,507,951	2.77%
	New Zealand	9,127,396	1.38%	9,557,453	1.42%	9,339,515	1.34%	10,835,082	1.50%	8,975,238	1.27%
	Norway	14,267,890	2.16%	10,261,853	1.53%	10,914,026	1.57%	11,908,384	1.65%	11,462,655	1.63%
	Switzerland	36,000,768	5.44%	29,464,427	4.39%	28,573,845	4.11%	35,197,000	4.87%	32,032,374	4.54%
	United States	485,587,650	73.41%	487,010,941	72.59%	494,031,872	71.07%	505,926,042	70.06%	502,274,870	71.24%
Pathogens Total		**661,446,689**		**670,917,026**		**695,168,862**		**722,087,281**		**705,023,733**	
GRAND TOTAL		**7,028,076,055**		**7,286,857,921**		**8,504,783,350**		**8,191,071,332**		**9,446,959,236**	

Second, we estimated the value of intra-EU exports of items on Annex IV. Table 5.4 presents maximum values of intra-EU exports by item category in Annex IV. The total value of intra-EU exports shows an increasing trend for the last five years, and the increases between 2010 and 2011 and between 2013 and 2014 are relatively greater than those for the rest of the period. The value of intra-EU exports is much larger than that of extra-EU exports of items in Annex II and Annex IV. While the extra-EU exports possibly related to Annex II and Annex IV increased from approximately €120 billion to €134 billion, the intra-EU market subject to Annex IV expanded from about €207 billion to €237 billion.

Among the items for Annex IV, the exports of items related to the CWC show a decreasing trend during the referenced timeframe. Although two CN codes, 30029050 and 30029090, can fall under that category, only the former was considered in this category since the latter also falls under MTCR related items as 'Materials or devices for reduced observables' according to the Correlation Table. However, the export values for both codes show a downward trend between 2010 and 2014. The intra-EU export value of CN 30029090, which represents 'toxins and similar products', was about €379 million in 2010 and €358 million in 2014, with a peak in 2013 at €405 million.

In regard to the category of cross-cutting items within Annex IV, it covers a narrower scope of items than that of Table 5.1, since cross-cutting items within one category were separately addressed. For example, CN 82073010, which represents interchangeable tools for pressing, stamping or punching for working metal, falls under ‘Production facilities for guidance sets’ and ‘Specially designed production equipment for rockets’, and both are within the MTCR category. Therefore, the export value for that CN code is reflected in the ‘Cross-cutting items within the MTCR category’ of Table 5.4 instead of ‘Cross-cutting items within ANNEX IV’. Conversely, as CN 84713000, which represents data processing machines, is under Cryptography and the MTCR categories, its export value was reflected in ‘Cross-cutting items within ANNEX IV’. Most of the items for ‘Cross-cutting items within ANNEX IV’ in Table 5.4 are computer-related goods, such as data processing machines and its input and output devices. The other items are electronic integrated circuits, direction finding compasses, navigation systems, vacuum cleaners and electrical machines or apparatus. If the same scope of items as ‘Cross-cutting items within ANNEX IV’ of Table 5.1 is applied to Table 5.4, it can be deduced that the export value of ‘Cross-cutting items within ANNEX IV’ of Table 5.4 increased from approximately €81 billion to €91 billion in the period of 2010-14.

Table 5.4. Upper threshold of intra-EU exports of items listed in Annex IV by EU Member States

ITEM CATEGORY	2010	2011	2012	2013	2014
Items of stealth technology	**1,124,101,065**	**1,004,324,047**	**1,638,932,335**	**1,863,547,845**	**1,841,146,300**
Materials or devices for reduced observables	553,955,769	516,590,644	514,408,594	602,257,450	583,399,270
Materials speciallly designed for use as absorbers of eletronicmagnetic waves	44,483,784	39,518,312	35,956,311	32,545,894	33,016,712
Cross-cutting items within the stealth technology category	525,661,512	448,215,091	1,088,567,430	1,228,744,501	1,224,730,318
Items of the Community strategic control	**11,511,936,635**	**13,254,450,835**	**13,610,074,793**	**13,658,503,231**	**14,558,522,219**
Acoustics	4,328,852,406	4,900,226,530	4,913,136,894	5,045,064,598	5,510,256,034
High explosives	43,182,315	45,946,016	45,216,226	57,913,901	60,016,561
High-current pulse generators	566,909,351	554,504,126	521,737,120	468,113,880	437,710,225
Noise reduction systems for use on vessels	6,418,036,183	7,624,153,651	7,974,503,060	7,922,539,919	8,377,585,206
Cross-cutting items within the community strategic control category	154,956,380	129,620,512	155,481,493	164,870,933	172,954,193
Items of the Community strategic control-cryptography	**87,172,903,399**	**89,213,376,740**	**92,601,673,188**	**94,096,963,270**	**99,248,091,364**
Equipment designed to perform cryptanalytic functions	87,172,903,399	89,213,376,740	92,601,673,188	94,096,963,270	99,248,091,364
Items of the MTCR technology	**29,228,988,714**	**33,974,628,847**	**35,848,569,324**	**36,975,144,630**	**38,940,300,844**
Guidance sets	2,844,253,204	3,093,972,496	2,986,620,437	3,011,146,366	3,054,699,633
Production facilities for guidance sets	297,224,867	325,374,553	399,847,872	404,773,359	442,970,397
Reentry vehicles	7,612,891,487	8,973,828,107	9,499,622,047	10,120,330,718	11,001,550,322
Specially designed production equipment for rockets	192,471,622	262,035,062	251,747,832	240,184,080	275,465,693
Systems usuable in missiles	497,777,310	466,245,798	502,081,852	559,454,819	568,330,992
Cross-cutting items within the MTCR category	17,784,370,224	20,853,172,831	22,208,649,284	22,639,255,288	23,597,283,807
Items of the NSG technology	**15,304,488,383**	**16,420,092,697**	**16,236,079,617**	**15,913,872,127**	**16,083,577,845**
Cameras and components	7,632,048,950	7,854,290,923	8,035,106,112	7,460,810,636	7,136,883,407
Lithium	22,472,676	24,845,987	592,644,795	656,627,132	537,594,623
Lithium isotope separation facilities	820,692,553	841,034,723	824,555,364	852,698,335	857,313,674
Neutron generator systems	35,941,149	103,210,232	17,221,114	17,296,830	15,598,764
Pressure sensors	2,475,628,270	2,668,469,366	2,638,310,135	2,761,712,166	2,920,931,316
Priviously separated neptunium-237	57,678,994	57,336,704	40,197,808	40,575,906	45,981,846
Switching devices	947,539,775	951,384,489	810,957,588	850,050,678	806,303,247
Tritium facilities	2,224,113,809	2,635,642,525	2,435,756,844	2,519,729,852	3,236,070,889
Velocity interferometers	751,346,430	727,970,330	452,560,855	341,003,728	297,136,546
Cross-cutting items within the NSG category	337,025,777	555,907,418	388,769,002	413,366,864	229,763,533
Items of the CWC	**594,636,760**	**582,007,769**	**333,703,827**	**394,766,620**	**453,687,177**
Cross-cutting items within Annex IV	**62,834,575,909**	**62,877,179,233**	**65,999,475,331**	**63,424,436,772**	**66,170,012,492**
GRAND TOTAL	**207,771,630,865**	**217,326,060,168**	**226,268,508,415**	**226,327,234,495**	**237,295,338,241**

5.3 Review options under the four European Commission Priorities

5.3.1 'Adjust to an evolving security environment and enhance the EU contribution to international security'

Dual-use export controls are a major component of the EU's 2003 Strategy on the Non-proliferation of Weapons of Mass Destruction (EU WMD Strategy) and the complementary New Lines for Action by the European Union in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems (New Lines for Action, NLA) of 2008. Complex procurement patterns for both illicit WMD programme and for legitimate trade flows, combined with technological developments, make proliferation-sensitive flows more difficult to control through the application of traditional legal concepts and enforcement methods. These developments require continual review and possibly adjustment of control systems, including outreach to stakeholders, legal provisions, control lists, as well as licensing and enforcement approaches.

Human security dimension

Application of human security criteria to exports of cyber-surveillance technologies; obligatory self-regulation on the part of industry producing cyber-surveillance technologies; introduction of an EU autonomous list for cyber-surveillance technologies (via a technical or descriptive list); and introduction of an EU cyber-surveillance catch-all mechanism), either through a dedicated catch-all for cyber-surveillance technologies or application of general catch-all.

These review actions are addressed in the dedicated chapter on cyber-surveillance technologies (Chapter 7), and will therefore not be further analysed here. It should be noted however, that the proposed human security approach is conceptualised as broader than the expansion of items and criteria in relation to cyber-surveillance. The 2014 Commission Communication specifically states that: 'The "human security approach" intends to place people at the heart of EU export control policy, in particular by recognising the interlinkages between human rights, peace and security'. It thus provides a conceptual framework for a broader range of measures. This could include the 'clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations'.

Response to technological changes

'EU technological reaction capacity', to make an active contribution to control list discussions in regimes, also involving 'structured engagement with industry' and guidance on emerging technologies.

The Commission Communication places the proposals for an appropriate response to technological developments under the heading 'smart security'. The adaptation of the legal-regulatory mechanisms governing the use or spread of certain goods and technologies through de-controlling or adding controls in turn requires the monitoring of technological changes and identification of appropriate responses from security, human rights, humanitarian law and other relevant perspectives. A technological response capacity however cannot function without technological expertise across a very wide spectrum, combined with knowledge of potential military application. The full range of such expertise is neither available to the European Commission nor to smaller or even most medium-sized Member States. To be effective, it may also require input from industry and academia, which could be obtained through the 'structured engagement with industry' mentioned in the Commission Communication. This study shows that the dual-use industry is very diverse, and includes SMEs as well as large multinationals, which would need to be represented in such an engagement. The project furthermore showed differing degrees of awareness in the various sectors, which would also need to be taken into consideration.

Certain projects funded by different EU research programmes may also be subject to dual-use export control provisions without those involved being aware. While some guidelines have been developed to make applicants and evaluators more aware of obligations under dual-use export controls, there is no EU-wide approach to this.[62] This issue also closely relates to ITT controls and the possible impact on academic research discussed in Chapter 5.2.3 above.

One of the areas of rapidly evolving technology is ICT. Examples of this include not only cyber-surveillance technologies, but also additive or 3D printing technologies which is not only affecting the biological sector but also expected to transform parts of the transport sector. As a consequence, items may no longer be physically transported, but produced in-country based on technology that has been transmitted electronically.

The EU's active contribution to control list discussion in the export control regimes faces several challenges. First, not all EU members are represented in all the regimes. Second, not all Member States have technical expertise for all parts of the control list, as mentioned above. Third, stakeholder discussion also indicated some concerns about institutional competence and the representation of EU governments through EU institutions in the export control regimes.

Swift integration of regime list changes into Annex I of the EU Dual-use Regulation has already been addressed through a fast track mechanism agreed between the institutions after the Commission Communication was published. This also has implications for international convergence as well as for international capacity-building, since increasingly more countries uses the EU control list structure as a model.

[62] 'Explanatory note on the control of "export" for "dual-use items", including technology transfers, under Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', <https://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-drs-2015/1645163-explanatory_note_on_the_control_of_export_for_dual-use_items_en.pdf>.

Intangible transfers of technology (ITT)

The Commission Communication considers providing guidance; outreach to the academic research community; codes of conduct for scientists; and Community General Export Authorisations (CGEAs) for intra-company ITT transfers.

Technological developments have led to substantial changes in export controls as they have expanded beyond the export of goods to include the transmission of technology through intangible means (thus referring to the means of transport, export or transmission) and transfers of intangible technology (where the technology itself is not and has not previously been tangible, such as oral transmission/technical assistance). ITT includes electronic transfers through email attachments, but also server up/downloads or making technology available for a end-user in another country via cloud computing or other internet sharing platforms. These developments pose challenges not only for licensing but also for enforcement, since customs officers traditionally deal with goods rather than intangibles or technical assistance. Only those customs or other services (e.g. the licensing authority) that dedicate resources to company audits on dual-use export controls may have a clear role to play in enforcing ITT controls, since their audits will include computers and email transactions. The traditional control function of physical borders is not applicable in this case. Audits are given an increased priority in some of the review options, through an emphasis on facilitated export procedures for exporters in exchange for enhanced reporting or record-keeping requirements. These, in turn, may require enhanced auditing capacities by Member States.

Some stakeholders interviewed emphasized that the intangible transfer of technology is central to routine business interactions, not only within companies but also through participation at international meetings and increased use of technical solutions such as cloud computing. In the view of a number of companies, the legal situation in the EU is insufficiently clear (see Chapter 6). Demands were also made for facilitation of intra-company ITT transfers.

ITT are also essential to academic research, exchange and publications. It is part of academic life through the transmission of know-how at lectures, in joint research programmes and in academic publications. A number of Member States have undertaken specific initiatives to reach out to academia and other research institutions. However, this aspect of stakeholder outreach appears to still be in its initial stages compared to outreach to companies that export dual-use products, and stakeholder consultations indicate that control authorities and academics in natural sciences do not usually see eye-to-eye or speak the same language. The review actions include outreach to the academic research community and codes of conduct for scientists. The latter as a bottom-up approach are likely to be preferable by the academic community over licensing requirements. A limited number of universities and research institutes in the EU currently have internal compliance programmes or guidelines/codes of conduct. Codes of conduct have been developed in a number of research communities. Furthermore, as was explained earlier, stakeholders from government and academia raised a need to clarify the term ‘basic scientific research’.

ITT present special enforcement challenges, because, like brokering, they are unlikely to be detected through border customs procedures. Detecting this type of unlicensed transfer will require information (for example, a voluntary disclosure by the company), intelligence about the offence or audit methods. The latter involve specialized electronic data processing auditors, which in turn requires training and resources. Moreover, good compliance procedures within the companies who produce or have access to controlled dual-use technology are essential.

Legal clarifications and amendments

Legal concepts and definitions that may be revised include: the notion of export and exporter; determination of the competent authority (especially for non-EU companies); the control of technical assistance; ITT controls; transit and brokering provisions; and extraterritorial provisions for EU persons (to prevent circumvention).

Stakeholder perceptions on legal clarifications vary, but a number of demands were made to clarify key provisions.

Currently the core concepts of the Dual-use Regulation are those of export and exporter. While brokering and transit controls have been made possible through the 2009 amendments to the Regulation, the precise nature and responsibility of the 'transiter' is not defined in the EU Dual-use Regulation. This is relevant given the complexity of the supply chain (explained in chapters 4 and 5.1) and of both legal and illegal dual-use transactions. The implications for the transport sector were considered earlier in this chapter, and implications for exporters are included in Chapter 6, which summarises stakeholder perceptions. At present, there are differences of terminology between the Dual-use Regulation and the EU Customs Code regarding transit, which according to some stakeholders has led to confusion. Even internationally, there is no agreed definition of the terms transit and transhipment.

Technical assistance is generally understood to comprise manual services and the oral transfer of know-how. However, the term has no internationally agreed definition. Such technical assistance falls within the scope of ITT, but is legally distinct in the EU because it concerns services involving the cross-border movement of persons. Instead, it was covered by a Joint Action of 2000 (2000/401/CFSP), which provides for controls of technical assistance through a prohibition or an authorisation requirement. Most but not all Member States have implemented corresponding provisions in national law. Moreover, in the context of EU restrictive measures, technical assistance measures have been included in a number of Council decisions and Council regulations, together with controls on a range of activities involving dual-use items as well as financial sanctions. Technical assistance is therefore another element that requires consideration as to how to enhance convergence between the various elements of the EU export control regime (see below).

While enforcing extraterritorial provisions for EU persons poses practical enforcement challenges in terms, such controls enable legal action should evidence emerge that an EU person is involved in a WMD programme abroad or brokering dual-use items for a WMD end-use abroad. Regarding dual-use brokering, the Dual-use Regulation covers transactions between two or more non-EU countries facilitated by a person established within the EU if the items concerned are or may be intended for a WMD end-use, and the brokering activities takes place from EU territory. If the items are located in the EU and exported from there, export control provisions apply rather than brokering controls (so as to order to avoid double regulation). In the dual-use area, arranging transactions is normal business practice for companies that operate internationally. Some Member States have additional extraterritorial provisions in specified cases if the brokering activities take place outside of EU territory. According to the review options this may be considered as an EU-wide provision.

5.3.2 'Promoting export control convergence and a global level-playing field'

Licensing architecture

Guidelines for consistent licensing practices (e.g. best practices for processing times); reviewing parameters for existing EUGEAs; introducing additional EUGEAs, e.g. for low-value shipments; encryption; intra-company technology transfers for R&D; intra-EU transfers of Annex IV items large projects; a regular review of National General Export Authorisations (NGEAs) and discuss possible transformation into EUGEAs; standardised IT support tools and electronic licensing systems across the EU; and emphasis on end-use monitoring.

Stakeholder consultations showed that licensing authorities tend to resist a pre-determined timeline for all licensing decisions, while processing times rather than denials appear to be the main concern of dual-use exporting companies. Interviews indicated that there is scope to optimise routine licensing processes in some EU countries through more staff resources, more frequent decision-making opportunities where inter-agency committees take decisions and/or electronic or otherwise faster procedures. Agreed targets or guidelines for routine cases and a formal obligation to have sufficient staff to meet them could assist licensing authorities in securing sufficient resource from their national or institutional budget. There also seem to be substantial differences in the situations in which national authorities use individual, global or national general licences. This affects compliance costs and processing times.

To enable a focus on more sensitive transactions, the Commission Communication considers an increase in the range of routine and non-sensitive transactions subject to facilitated procedures through additional CGEAs or modified conditions of existing ones. While those reforms would generally be favourable for companies, the benefits of a given type of general licence for a company depend on the type of dual-use items exported, the specifics of the sector and trading patterns (e.g. high value or low value shipments, products with a short shelf life, frequent exports to the same customer or occasional one-off shipments, regular supplies of spare parts), as the use of such licences nevertheless requires keeping track of shipments and following notification procedures. Measures that facilitate non-sensitive export enable companies and authorities to focus on potentially sensitive transactions. However, security concerns may arise concerning certain facilitation measures. For example, the commercial value of an item may be disproportionate to its utility for a WMD programme. Moreover, facilitation measures could also be used for fraudulent shipments. Facilitation measures therefore must be combined with audit and verification measures.

End-user monitoring or verification could increase certainty over the final end-use. However, this will have resource implications for authorities, as existing embassy staff typically lack dual-use expertise. Moreover, political and legal questions arising from such activities in non-EU countries will need to be addressed.

Electronic licensing systems for submission and processing of license applications are in place in many but not all EU Member States.[63] To support effective enforcement, such systems must be compatible with the customs risk management system and enable automatic checking whether the licence number provided is valid, and if authorised volumes have been reached or exceeded, as is the case in the UK for example. Finally, as with all electronic systems, IT security is a key issue, not only for governments but also for industry that provides a wealth of commercially sensitive data in licence applications. This in turn requires investments in IT maintenance.

An issue raised by a number of stakeholders relates to the classification of dual-use items, and differences between Member States in this regard. Some industry stakeholders have proposed making common interpretations of the control list mandatory.

Outreach, cooperation and assistance to partner countries and dialogue with key trading partners

International capacity-building (in the EU context often referred to as outreach) not only contributes to international security but also to international convergence and thus to levelling the playing field. It has also increased the international and EU-internal exchange of information, experience and practices. The EU acknowledged the need for international cooperation to prevent and combat WMD proliferation in 2003, when it introduced a range of measures to strengthen its approach to security in general and WMD proliferation in particular. The establishment of export control systems can also open up new markets to foreign investment and technology transfers. International cooperation and capacity-building can also enhance the effectiveness of controls, especially since the supply-side control approach is increasingly undermined by wider foreign availability of technology, which puts certain controls into question and regularly leads to deregulation of controls.

Since 2005 the EU has developed the world’s second biggest dual-use trade control capacity-building programme, after that of the USA. Such efforts include cooperation with countries in Europe, Africa, Asia and the Middle East. However, resource constraints among EU Member States’ licensing and enforcement officers and specialised legal and technical experts limit the resources available to participate in international activities, be it through receiving delegations in-country or traveling abroad. Until August 2015, the EU programme ‘Cooperation in Dual-use Export Control’ was implemented by the German export licensing authority, the German Federal Office of Economics and Export Control BAFA, with a pool of legal, licensing,

[63] 60% of the business associations indicated that the current dual-use export controls give rise to significant distortions between companies located in different EU Member States and 14% of the companies indicated that they received a denial for a licence application, when another EU exporter fulfilled the deal through an identical export.

industry outreach and enforcement practitioners drawn from Member States across the EU. The successor programme is managed by a French-led consortium.

The development of export control dialogues with key trading partners aims to avoid 'conflicting regulatory requirements' and to reduce the 'administrative burden on export-oriented industries'. This actually overlaps with outreach and assistance, since some trading partners may also be partner countries in EU-funded capacity-building programmes.

Promoting global convergence

While difficult to achieve, global convergence remains a key objective, motivated both by security and economic interests. A need for such convergence was highlighted by a substantial number of industry stakeholders. The definition of items, activities and actors subject to controls varies across the globe. The area in which convergence among suppliers has probably progressed the farthest is the list of items subject to control. This has been partly achieved through the inclusion of common lists in some dual-use related UN sanctions, and through the adoption of lists negotiated in the international export control regimes and consolidated into the EU list structure which has been adopted by an increasing number of countries, including in Asia.

The Commission Communication proposes the promotion of coherent, comprehensive, unified EU representation in the regimes. Not all EU Member States are represented in all export control regimes, in particular the MTCR. However, since accession to these regimes requires consensus, this is a political decision outside of the scope of the EU dual-use export control policy review.

5.3.3 'Develop an effective and competitive EU export control regime'

While there is one common legal basis for export controls on dual-use items in the EU, there are 28 different implementation and enforcement systems and approaches. This poses challenges through different application and interpretation, but also creates opportunities through the possibility to adjust systems to particular national factors such as the industrial structure, geographical location and volume of exports. The goal of a level playing field for R&D, competitiveness and technology within the EU and internationally is often referred to by industry.

Common risk management framework

A common risk management framework (discussed in the Commission Communication under the heading of effectiveness and competitiveness), is also directly relevant for the EU contribution to international security (Priority 1). Risk management for dual-use items is conducted both by licensing authorities (in the licensing process) and by customs (in the transit and export process).

The proposed development of common risk management tools and framework is in progress in the relevant customs working groups, but it appears that to become a reality requires a further increase in trust and information sharing.

However, customs can only share the information they own, not classified information they received from other services. In those cases, Member States can therefore be assumed to use bilateral rather than EU-wide channels of communication. This may create gaps and opportunities for illegal exports of dual-use goods through those Member States that are not aware of the risks that have been identified in other Member States. At the same time, while a common risk strategy will enhance the effectiveness of the EU-wide regime, risks still need to be tailored to and prioritised at national level, reflecting trade flows, procurement patterns and industrial structures in the individual countries.

Potential breaches of the controls can be separated into those that occur due to ignorance, lack of knowledge, understanding or awareness of dual-use trade controls, and those that occur as a result of deliberate evasion of trade controls. While outreach to industry and other stakeholders and other transparency measures (see below) is an effective way to reduce the risk of inadvertent breaches, effective enforcement, including penalties may be necessary for deliberate breaches.

Convergence of catch-all controls

The way in which the catch-all provisions of the EU Dual-use Regulation are interpreted and applied across the EU varies substantially. This has led to concerns regarding distortion of competition within the EU, as well as the effectiveness of controls.

Differences relate to the way the catch-all is translated into procedures and information is communicated to companies – formally or informally, and how narrowly or widely the imposed licensing requirement is formulated. First, a catch-all may be published and apply to all producers of the same product, or only be delivered to a particular company. Second, it may apply to a whole destination country or only to a specified end-user. Third, it may be delivered in response to a shipment being stopped by customs, who request the company to apply for a licence with the competent authority. Alternatively, the company may be notified in response to intelligence information, regardless of whether or not it intended or attempted to export a certain product.

Challenges in catch-all implementation were specifically raised by one Member State in the on-line survey. While many issues and challenges related to catch-all implementation are not EU-specific, some aspects are unique to the EU common market context. This variance may be due to different access to intelligence information or risk assessments. This situation also raises issues regarding clarity and predictability for exporters, although this is a broader issue also applicable to listed items.

Currently denials are exchanged, but not notifications. The Commission proposal to increase information exchange through a catch-all database and to partly make catch-all information public will however need to consider that this sharing of information between Member States in some cases is considered sensitive; while others are concerned about information overload. Finally, an issue raised in consultations wasthe consequence of receiving the information and next steps to take. A country may issue few catch-all notifications, based on rather certain information about a potential WMD end-use and thus normally result in a denial and entry of the information into the customs risk management system. If this country receives many notifications from a Member State that uses this tool as a precautionary measure for transactions that would in most cases not be denied, this could be confusing and result in unnecessary delays and controls.

Intra-EU transfer controls for Annex IV items

The options proposed by the European Commission comprise a review of Annex IV to update the list and limit it to the most sensitive items, and to introduce EUGEA for intra-EU transfers. This would include technology transfers and be combined with post-shipment verification. Free intra-Community transfers of Annex IV items has been a demand notably from nuclear companies, who are most affected by these provisions. A review of Annex IV and its reduction to the most sensitive items seems uncontroversial. Concerns may be raised either in connection with international requirements on nuclear controls, notably those imposed by the IAEA, and by suppliers (such as the USA) that prefer to make decisions on the eligibility of certain EU Member States for certain transfers rather than treating the EU as one recipient. This is illustrated by the fact that the USA has excluded some EU Member States from certain export facilitation measures.

5.3.4 'Support effective and consistent export control implementation & enforcement'

This issue overlaps with the previous section in as far as effective export control implementation and enforcement is what an effective EU export control system is about. Competitiveness is also linked to consistency across the EU. While Priority 3 is aimed at creating a level playing field within the EU, Priority 4 is focused more on enabling practical implementation both by the authorities and by the private sector.

EU Export Control Network

Under the heading of developing an export control network in the EU, the Commission proposes a range of measures to: enhance the scope and depth of information exchange, both electronically and in person; strengthen cooperation between export control practitioners in the EU; and build capacity. It also raises the issue of enhanced consistency between the different export control related instruments and competencies in the EU and in the Member States. In fact, this priority probably has the most elaborate and detailed set of proposals.

Enhance information exchange and develop IT infrastructure

Enhanced information exchange on licensing data and on other information (e.g. destinations, end-users, incidents and violations), and using the security IT system DUeS for this purpose.

Sharing information between and with enforcement agencies through an EU-wide information exchange system and developing standardised IT support tools and electronic licensing systems across the EU.

While substantial information is exchanged on denials, little information is publicly available or exchanged between Member States on dual-use licences granted or actual dual-use exports. In recent years, EU governments have begun exchanging some information on licences granted on an annual basis. These figures were used in aggregated form in Chapter 4. Figures on actual exports could possibly be derived from national customs databases, but are not currently collected by DG TAXUD. The feasibility of such collection depends on several factors. Box 44 of the customs declaration is a multi-purpose field, which inter alia is used to declare that a dual-use licence is required for a given export (coded as X002). Whether the information in the databases can be searched to identify dual-use exports depends on whether box 44 is broken down in different sub-fields in the electronic customs system, including a dedicated box for X002. Correct sharing of this information also requires correct usage of the box by the exporter, which is not always the case. Finally, whether national customs authorities are allowed to share this information with other national authorities or the European Commission may depend on fiscal secrecy and commercial confidentiality provisions.

There is no systematic information exchange at present on sensitive destinations, end-users, incidents or violations. Some information on these issues is exchanged in the international export control regimes, but not systematically at EU level. Incidents could include detections or interceptions of suspected violations, or transit shipments that are sent back because of a change of the declared destination, while violations could include investigated or prosecuted violations, which may result in compound penalties, administrative or criminal penalties if they result in a conviction. The UK is the only EU Member States at present to include statistics customs seizures and prosecutions in its Strategic Export Control Annual Report. It also includes summaries of enforcement policy, resources deployed and activities undertaken.[64] Reports about trade control-related prosecution cases are published on the ECO website.[65]

Information exchange on sensitive end-users and transactions also routinely involves classified information, in addition to data generated and owned by customs authorities themselves. Since customs authorities usually are not allowed to share classified information from their own or other countries' intelligence services with other customs agencies, this issue will need to be considered when exploring what information should be shared through DUeS, the EU's secure IT system for sharing information on dual-use export issues, and when setting up an electronic system for sharing information within and between enforcement authorities.

Finally, information exchange and managing of databases also absorbs substantial resources. This is an important point given that a number of Member States identified staff and IT resource constraints as a major challenge in implementing the EU Dual-use Regulation. It may also involve information held by a number of different enforcement agencies, depending on institutional responsibilities in Member States.

[64] The reports can be accessed online at <http://www.fco.gov.uk/en/about-us/publications-and-documents/ publications1/annual-reports/export-controls1> and are available in hard copy from the Stationery Office, <http://www.TSOShop.co.uk>.

[65] <http://www.bis.gov.uk/policies/export-control-organisation/eco-press-prosecutions>; <http://blogs.bis.gov.uk/exportcontrol/category/prosecution/>.

Finally, stakeholder consultations both showed that not all EU Member States have electronic licensing systems. For effective enforcement and to enable the extracting of accurate information, such systems must be compatible with electronic customs risk management systems.

Enhance strategic and operational cooperation with enforcement agencies

Integrating export control priorities in policy cycles; developing common risk management tools and framework; implementing joint operations; and enhancing the enforcement of transit and brokering provisions.

Article 24 of the Dual-use Regulation states that 'each Member State shall take appropriate measures to ensure proper enforcement of all the provisions of this Regulation'. In EU Member States, the different enforcement functions of customs controls, risk management, company audits, and investigations and prosecutions are divided between different agencies or combined within one agency. A first joint exercise was conducted in 2009 and a table-top exercise in 2014.[66] Follow-up activities will necessarily require an appropriate allocation of resources.

The allocation of resources to dual-use export control enforcement varies substantially across the EU. However, stakeholder consultations in the initial project phase indicated that collecting detailed statistics on these would take time, and also there may be hesitation to share all of these, for example regarding the number of intelligence staff working on dual-use export control related issues.

Transit (including transhipment) controls were introduced in the EU as a consequence of UN Security Council resolution 1540 (2004), which made transit and transshipment controls for WMD-relevant items mandatory for all states. Several other proliferation-related UN Security Council resolutions also require transit and transshipment controls for effective implementation.

For both transit and trans-shipment, implementation and enforcement fall within national responsibility and the Dual-use Regulation offers the possibility for Member States to extend brokering services on a national basis. This includes the extension to non-listed items and military end-uses, and the possibility to impose an authorisation requirement if the exporter has grounds for suspecting a WMD end-use.

Enhanced enforcement of transit faces a number of practical challenges and involves the coordination and cooperation of many actors with and between Member States. Enhanced enforcement of brokering provisions faces different challenges, as the detection of illegal brokering will usually require information sharing and co-operation with foreign enforcement or intelligence agencies, or may be detected during company audits.

[66] <https://export-control.jrc.ec.europa.eu/News-Events/Conferences/Articles/ArtMID/525/ArticleID/234/Pilot-Export-Control-Simulation-Exercise-for-European-Union-EU-Customs-and-Licensing-Authorities>.

Improved coherence between different EU institutions and Member States, and identification of synergies between security-related trade control instruments

This review action is motivated by seeking coherence between different elements of the complex EU export control regime. This is complicated by the horizontal nature of trade controls. The EU export control regime comprises a range of instruments and measures, including: EU restrictive measures; the anti-torture regulation; customs coordination on risk management; the Joint Action on technical assistance of 2000; and arguably also arms export controls.

Arms export controls overlap with dual-use export controls in several respects, including with regard to the assessment of export licence applications for conventional dual-use items. The EU Dual-use Regulation specifically refers to arms embargoes in connection with the catch-all for dual-use items destined for a military end-use in an embargoed destination, thus highlighting the connection. It also refers to the criteria developed for arms exports from the EU (Art. 12). Moreover, in many states the laws, administrative procedures, agencies and staff responsible for controlling transfers of dual-use items overlap with those for conventional arms and for the implementation of restrictive measures. This is relevant for common risk management, cooperation and information exchange, as well as for internal and external capacity-building. Additionally, there are technical linkages as some categories of goods and technologies are included on both conventional and WMD control lists, and some conventional arms can also be used to deliver WMD.

This highlights the challenge of the horizontal, cross-cutting nature of dual-use export controls, which involves different legal instruments, policy areas and institutional competencies, in Member States as well as in the EU institutions.

Currently proposed amendments to the Regulation 'concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment' would broaden the scope of application of Regulation (EC) No 1236/2005 by extending the definition of 'torture' and 'other cruel, inhuman or degrading treatment or punishment' and by introducing the control of brokering and technical assistance, as has already been done for dual-use items in 2009. Different types of authorisations and assessment criteria have also been proposed, some of which build on experience gained from the Dual-use Regulation.

A lack of coherence between different EU instruments and between Member State implementation may undermine the effectiveness of the regime. At the same time, it is important to keep in mind that different implementation approaches do not necessarily constitute a lack of coherence, but may rather be a way to tailor controls to a country's institutional set-up, geographical location, industrial structure and trading patterns and foreign and security policies.

Capacity-building within the EU

EU-wide capacity-building programme and training for officials; further development of EU pool of experts.

Currently no dedicated EU funds are available for EU internal training and capacity-building in the area of dual-use export controls. Moreover, a number of EU licensing authorities in EU Member States had to implement or are currently facing budget cuts and reductions in personnel, even as the range and complexity of the issues being tackled by export controls is increasing. One licensing authority pointed out that while their number of licences increased by 420% since 2008, no additional resources were allocated and additionally, the complexity of trade and of sanctions has increased. A feasibility study on an in-reach programme was produced for the European Commission by the German Federal Office of Economic Affairs and Export Control (BAFA) in 2010, but a decision to establish and fund such a programme has yet to be taken.

Private sector partnership

Clear private sector compliance standards for use of simplified mechanisms as a 'substantial benefit' for 'reliable exporters' through guidelines; transparency and coordinated outreach through publication of reports/non-sensitive control information, including guidance on good compliance practices; and promoting convergence with the AEO programme.

While the term 'industry outreach' is still commonly used by export control officials, today's technological and scientific reality means that non-industry actors, such as academia and research institutions, also 'export' controlled items, both in tangible as well as intangible forms. Even individuals such as 'garage companies' or 'do-it-yourself' individuals in the biological area may export controlled items. The precise range of relevant actors in a given country or region depends not only on the industrial, research and academic structures, but also on the geographical situation in relation to trade flows – e.g. countries with external EU borders, land-locked transit countries or major sea- or airports that are transhipment hubs.

The stakeholder consultations showed that within and between the different dual-use relevant sectors, the organisational structures, ways of conducting R&D, forms and extent of collaboration with academia and research institutes, and levels of awareness regarding security issues vary substantially. The transport sector provides many different types of service in addition to the physical transportation of a commodity, including customs processing and documentation. However, their role and responsibilities differ fundamentally from that of the exporter (see Chapter 3.3).

Companies are motivated to put compliance systems in place by various factors, including wanting to: avoid penalties; maintain a favourable image and avoid reputational damage; avoid delays in licensing application procedures and during export; comply with licensing conditions; and prevent accidental contributions to WMD programmes.

Both options—the creation of EU-wide legal ICP requirements or mere guidance—are included in the Communication, although the latter are clearly favoured by industry, in particular SMEs. The need for tailoring of guidance and tools to different sizes, structures, sectors, functions and trading patterns was also emphasised during interviews.

Consultations also showed that the term ICP, while frequently used, can lead to confusion, as it is often associated with a formal programme or sophisticated IT solutions. Terms such as export compliance systems or procedures were more acceptable for smaller companies in particular.

The principle of trade facilitation for 'reliable companies' with solid internal compliance systems has been developed in a number of frameworks within the EU, both in the fields of military equipment and dual-use transfer controls. Under the EU Dual-use Regulation, granting a global export authorisation to a specific exporter inter alia has to take into account whether the exporter has 'proportionate and adequate means and procedures to ensure compliance with the provisions and objectives of this Regulation and with the terms and conditions of the authorisation' (Art. 12).

The Authorized Economic Operator (AEO) status was created by the 2005 amendments to the EU Customs Code. A working group was set up in the context of the WPDU to look into issues of potential convergence. This aspect will therefore not be analysed in detail here, but stakeholder consultation clearly revealed very different views on the benefits, risks and feasibility of creating synergies between AEO status and dual-use trade facilitation measures.

6. Stakeholder perceptions of dual-use export control policy and the review options

Given the limitations in the data, we have used a range of stakeholder consultation activities to develop a deeper understanding of the baseline situation and the possible implications of the review options that are currently being considered. As explained in Chapter 2, this includes interviews and online surveys with business associations, companies and licensing authorities. This chapter outlines the results of the first round of interviews and the surveys. Information on business perceptions regarding the impact of controls on cyber-surveillance technologies and the potential expansion of controls in this area are presented in Chapter 7.

In addition, interviews were held as part of case studies (e.g. cyber-surveillance, chemicals, etc.). The results of those interviews are included in Chapters 7 and 8. In this chapter we start by analysing the results of stakeholder consultations with business, and this is followed by the results of the consultations with licensing authorities.

6.1 Business perceptions: results of initial interview round

At the start of the project initial interviews were held with business associations to identify key issues and to help shape the online surveys. Before presenting the results of the survey, it is therefore relevant to identify some important points arising from these meetings, which can be summarised as follows.

Lack of specific knowledge on dual-use aspects

Almost all the associations contacted were interested in participating in the study. Nonetheless, despite the process of selecting the most relevant associations, the majority showed a general lack of knowledge of dual-use export control issues, even when they represented affected sectors. In fact, most associations were unable to provide specific information on the issues associated with the export of dual-use items, such as licensing procedures and internal compliance programmes. Only a small number of associations provided us with crucial insights to develop an initial profile of the dual-use sector.

The main outcomes relate to the lack of data on the dual-use industry and the limitations of the data available.

Associations were generally not able to provide us with detailed information on dual-use products in terms of importance for their industry, as they do not directly collect data on dual-use items from their members (e.g. on production, trade and employment). For this reason some of the associations could provide only a rough estimate of the importance of dual-use for the industry as a percentage of total exports or production. Moreover, there is generally limited information available on the quality of the match between the dual-use items listed in Annex I of the Dual-use Regulation and the customs codes (HS or CN). An exception is a medical technology industry association that provided us with a table matching the customs codes with the most important dual-use products of the industry. While a number of associations have members that are active in this area, there is no single industry association that represents the cyber-surveillance sector as such. The associations that do have members that are active in this area were able to identify dual-use and HS codes that cover certain types of cyber-surveillance technologies. However, they were not able to identify the percentage of exports covered by these dual-use and HS codes that would relate to cyber-surveillance technologies.

It should also be taken into account that the data collected from the business associations has important limitations for two main reasons. Firstly, most associations do not cover all EU Member States and some of them include countries outside the EU. Secondly, some companies are members of multiple associations, which can result in double counting. Therefore, with respect to the basic quantitative data collected in this phase, it can be used as a broad indication to outline the first picture of the dual-use industry, but these shortcomings imply that there is little or no room for further analysis.

Cooperation with other stakeholders not much affected by export controls

Another aspect discussed was the relationship between companies exporting dual-use items and other actors in their value chain.[67] The interviews highlighted that cooperation with research organisations and academia are relevant for many companies, but that export controls do not have a significant impact on such cooperation.[68] This issue was further investigated in the next stage of the study. The implications for the impact assessment are that collecting data on research and innovation expenditure, as was suggested in the inception phase, would not be helpful in the analysis.[69] Many companies would not be able to isolate the expenditure for the dual-use industry, and this data also does not provide information on the specific links with other stakeholders. The effect of export controls is therefore mainly assessed in qualitative terms.

Concerning other main players in the value chain—the transport companies, freight forwarders and brokers, which have recently been given a stronger, albeit still vaguely defined, responsibility in the export process—most associations did not raise any significant issues linked to dual-use trade controls. One association noted that when these players became subject to dual-use trade controls under the Dual-use Regulation in 2009 there had been temporary problems with some companies, but these issues have since been resolved. However, another association reported that the

[67] Porter, M. E., *Competitive Advantage: Creating and Sustaining Superior Performance* (The Free Press: New York, NY, 1985).

[68] The European Commission has developed extensive support mechanisms to foster research and innovation in the public and private sectors, including a range of financial instruments and procedures. Much of the mapping done in the context of such support mechanisms can, in principle, provide further insight in the mapping of dual-use sectors, particularly among SMEs. For example, the Enterprise Europe Network lists business offers and requests to support European SMEs. Enterprise Europe Network, <http://een.ec.europa.eu/>.

[69] The OECD has developed and implemented methods to identify and analyse main science and technology (S&T) indicators and innovation indicators. OECD, 'Innovation statistics', <http://www.oecd.org/innovation/inno/inno-stats.htm>; and OECD, Main science and technology indicators', <http://www.oecd.org/science/inno/msti.htm>.

requirements that transport companies use for their suppliers have increased significantly and generate high costs for producers of dual-use items.

The survey and case studies, including a section on the transport sector (Chapter 3.3), sheds more light on the role and implications of export controls in that sector. Importantly, one has to bear in mind that the increased compliance requirements on transport companies arise also from dual-use related UN and EU sanctions and the control systems of other countries (in particular transit and transhipment points), not from the EU Dual-use Regulation per se. However, since the EU Dual-use Regulation includes a requirement that Member States implement international commitments, one could argue that EU and UN sanctions are linked to the requirements of the Dual-use Regulation.

Administrative costs not always the main concern of industry

In the discussion on the impact of export controls on companies, it emerged that for many of the associations that did have some insights into this issue, the administrative costs associated with export controls generally represent a limited percentage of companies' total turnover, and depending on the level of price competition in the sector, these costs can vary in importance. According to some of the business associations, more important impacts are related to the risk of not obtaining the licence or not receiving it in time to close a deal successfully. The uncertainty of whether and when a company receives the licence could lead to a cancellation of sales and thus represent a potentially large financial loss (e.g. for an SME that relies on just-in-time delivery in its supply chain).[70] This was also a key issue addressed in the follow-up interviews and surveys with business.

Limited knowledge of review options

Except for Option 4 'EU system modernisation' on cyber-surveillance technologies, we could not obtain detailed information from the business associations on the potential impact of the review options. As noted above, most of the business associations could not provide us with specific data on all the aspects covered during the interview. Business associations nevertheless have different levels of knowledge on the topic (partly due to their mandate or association priorities, as well as the previous or current roles in a company of association staff or representatives). Few were aware of the review options and they could only partially elaborate on this topic. Implications for the further research were that questions on the review options needed to include explanations and that not too much detail in response could be expected.

Social and environmental impacts beyond those related to production

Finally, the potential impacts of dual-use products on the environment and society were very difficult to identify, not least because often businesses do not want to highlight possible problems. It was pointed out that the environmental effects should

[70] The EU defines an SME by the number of employees and turnover/balance sheet total. Medium sized companies have fewer than 250 employees, while small companies have fewer than 50 employees. European Commission, <http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm>.

be assessed not only in terms of production but also in terms of use of the final product. Implications for the research were that questions on these issues needed to be clear and limited.

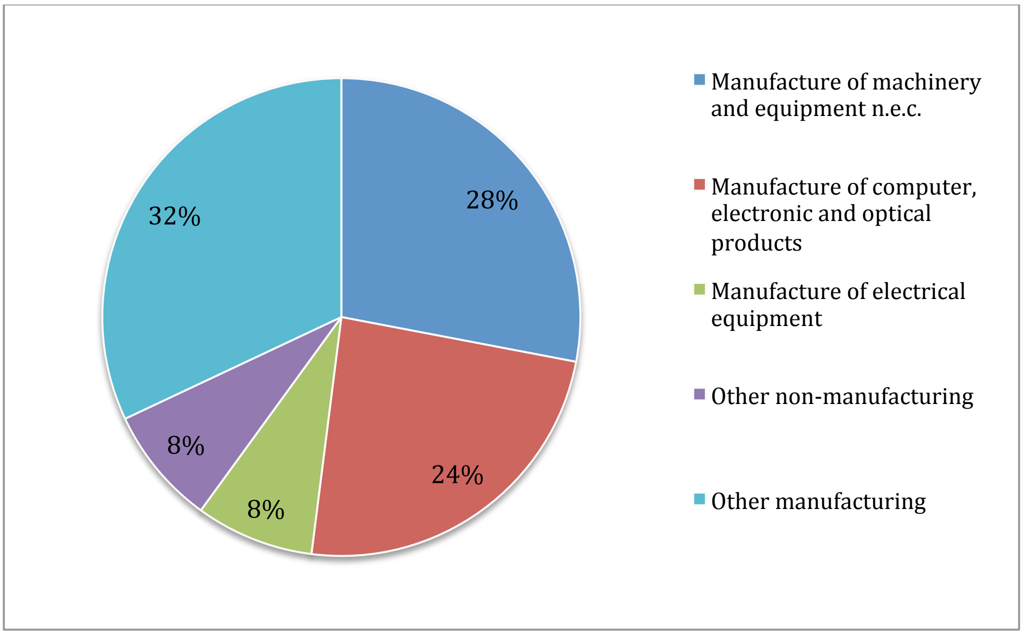
6.2 Business perceptions: results of the online survey

Two online surveys for business were designed: one for business associations and one for companies. More details about the survey set up, organisations and responses were presented in Chapter 2 explaining the methodology. In the following section we present the results of both surveys and, more specifically, we compare the company results by size, location and industry. The full results of the survey are presented in the Annex.

6.2.1 Characteristics of respondents

The sample of both surveys together covers 16 Member States with one quarter of the associations based in Germany and companies mainly located in Germany, Denmark and the United Kingdom. The majority of the companies are large enterprises (62%) and are part of a multinational corporation. As shown by figure 6.1, the industries most represented by the business associations are *other manufacturing* (32%), *manufacture of machinery and equipment* (28%) and *manufacture of computer, electronic and optical products* (24%). The general category '*other manufacturing*' includes among others the defence and security industry and aerospace manufacturers. The category '*other non manufacturing*' includes retail and wholesale trade and laboratory networks, diagnostic and research.

Figure 6.1. Industries represented by the business associations



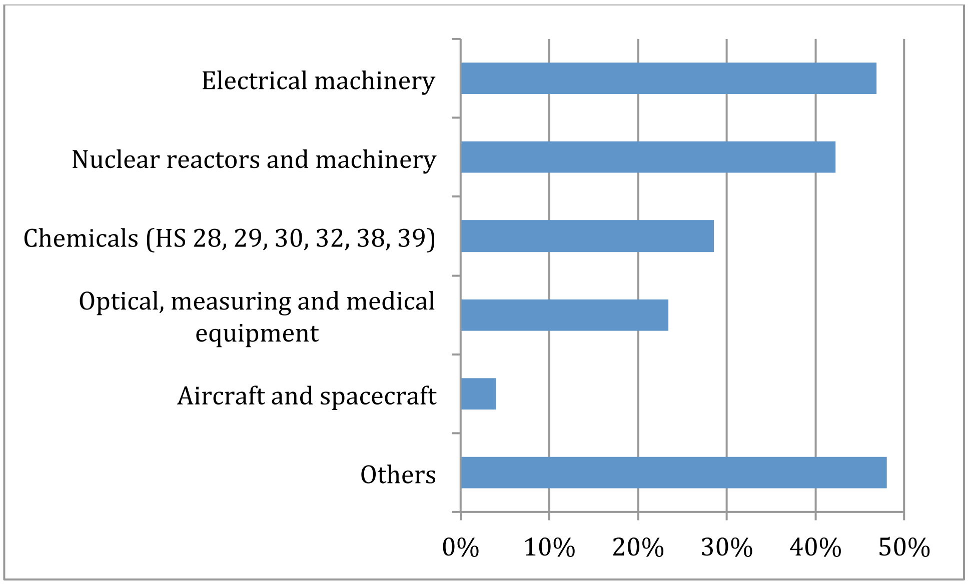
Total respondents=25

Source: SIPRI/Ecorys business association survey

6.2.2 Dual-use products exported and importance of dual-use items

In order to assess the importance of dual-use for the industries, it is relevant to present the dual-use products that are usually exported by companies.[71] As shown by Figure 6.2, 47% of the companies export electrical machinery and 42% nuclear reactors and machinery. Chemicals[72] are exported by 29% of the respondents. The category 'others' includes articles of iron, steel and aluminium and articles thereof.

Figure 6.2. Dual-use products exported by the companies



Total respondents=175

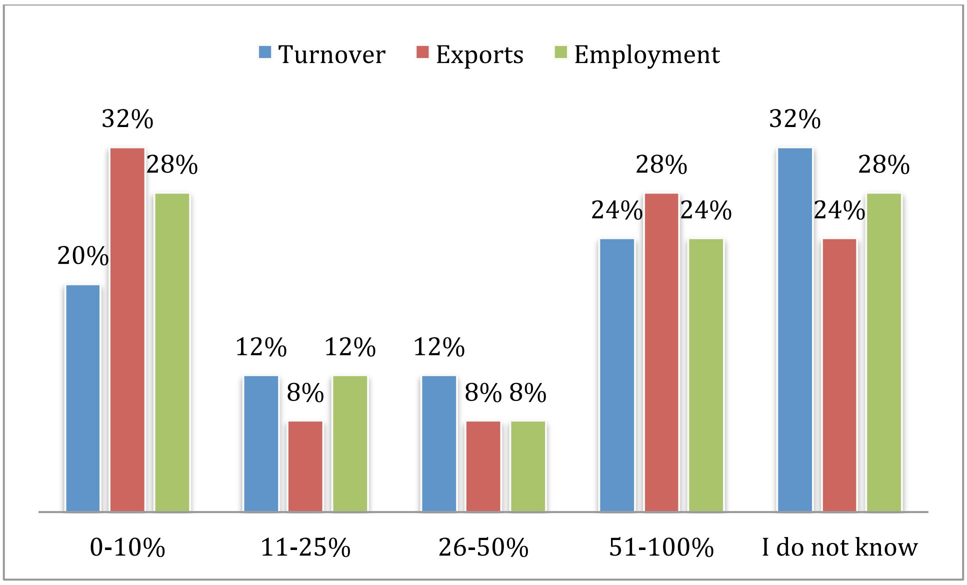
Source: SIPRI/Ecorys company survey

Despite the low sample of only 25 respondents, Figure 6.3 shows the importance of dual-use items in terms of turnover, exports and employment according to the business associations.

[71] It should be noted that 65% of the companies that completed the survey export dual-use items and 14% of the companies export military items in the EU Common Military list. The remaining 35% do not export dual-use items mainly because the products exported to non-EU countries do not contain dual-use items.

[72] In our analysis the chemical sector includes the following HS codes: 28, 29, 30, 32, 38 and 39.

Figure 6.3. Share of dual-use items in terms of turnover, exports and employment

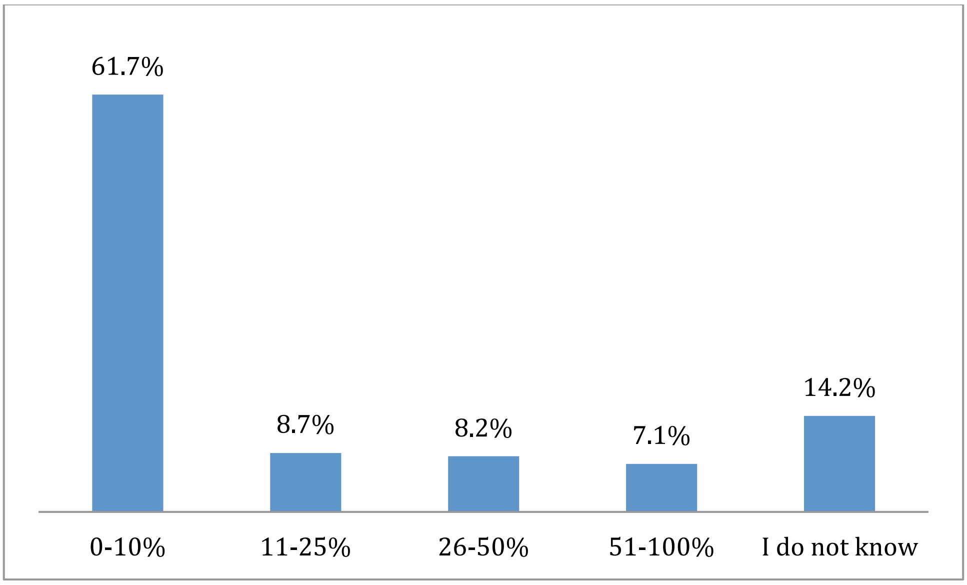


Total respondents=25

Source: SIPRI/Ecorys business association survey

The share of dual-use exports in the turnover of the companies (figure 6.4) presents a different situation (to the share of dual-use in turnover, in figure 6.3): in the majority of the companies less than 10% of the turnover is generated by dual-use exports. Although this could be due to the group of respondents that participated in the survey, given the limited knowledge of business associations on the specifics of dual use (as observed in the first round of interviews), the responses from companies are likely to be more reliable.

Figure 6.4. Share of dual-use exports in companies' turnover



Total respondents=183

Source: SIPRI/Ecorys company survey

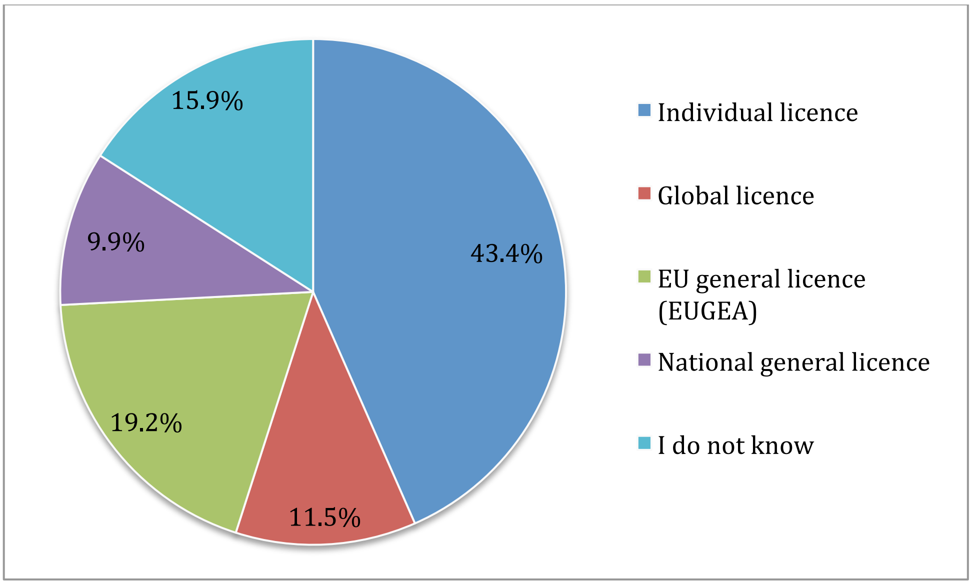
6.2.3 The licensing of dual-use items and export control management

To comply with Dual-use Regulation 428/2009, almost all the companies have an Internal Compliance Programme (ICP) in place (95%) and manage the export control licensing process internally with dedicated staff (97%). A formalised programme is more common in large enterprises but it is present also in SMEs. 10% of the SMEs do not have an ICP, and in 7% of the SMEs the obtaining and managing of licences for dual-use items is done externally.

As shown by figure 6.5, the type of licence that is mostly used by the respondents is the individual licence, followed by the EU general licence and the global licence, with no significant differences across sectors or by company size (Figure 6.6). [73]

[73] About half of the associations do not have information or insights into the compliance programmes of their company members and 44% of them are not aware of the types of licences used most often by companies. This confirms the general lack of knowledge of dual-use export control issues among the business associations representing sectors that are affected by dual-use export controls (see Chapter 6.1).

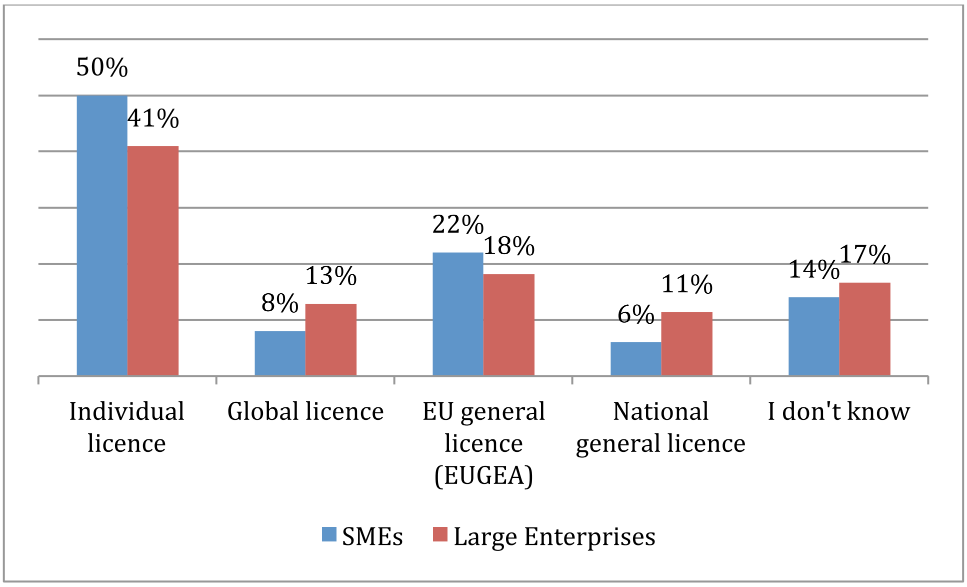
Figure 6.5. Types of licences for dual-use exports



Total respondents=182

Source: SIPRI/Ecorys company survey

Figure 6.6. Types of licences for dual-use exports by size of companies



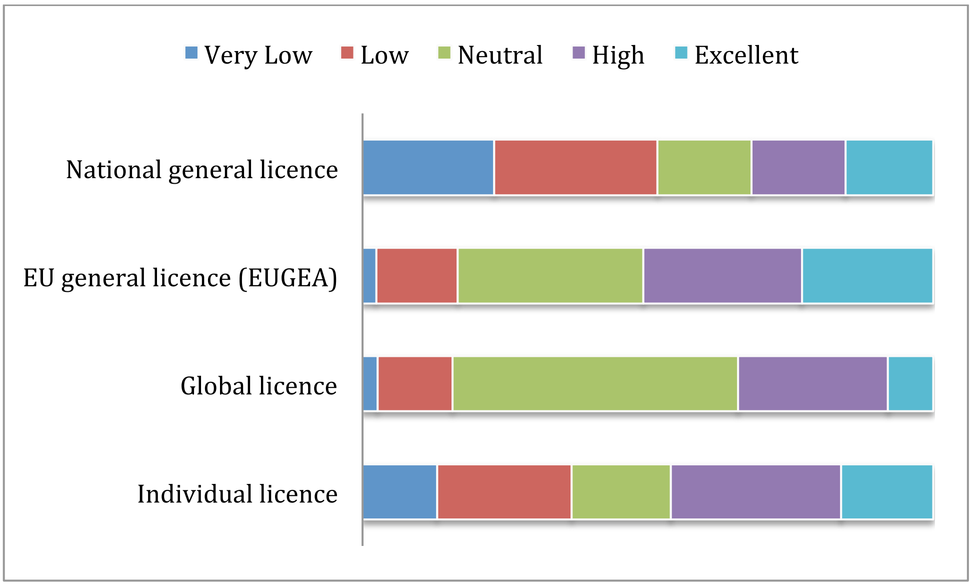
Total respondents=182

Source: SIPRI/Ecorys company survey

Among these types of licences, most companies consider the EU general export licence efficient in terms of export control process with 51% of the companies rating its efficiency as high and excellent. The national general licence presents the lowest value with 52% of the companies (located mainly in Northern European countries) rating its efficiency as very low and low (Figure 6.7). More generally, on average Southern

European companies consider the export control process less efficient than the companies located in other parts of Europe.

Figure 6.7. The efficiency of the export control process by types of licences



Total respondents=91-161

Source: SIPRI/Ecorys company survey

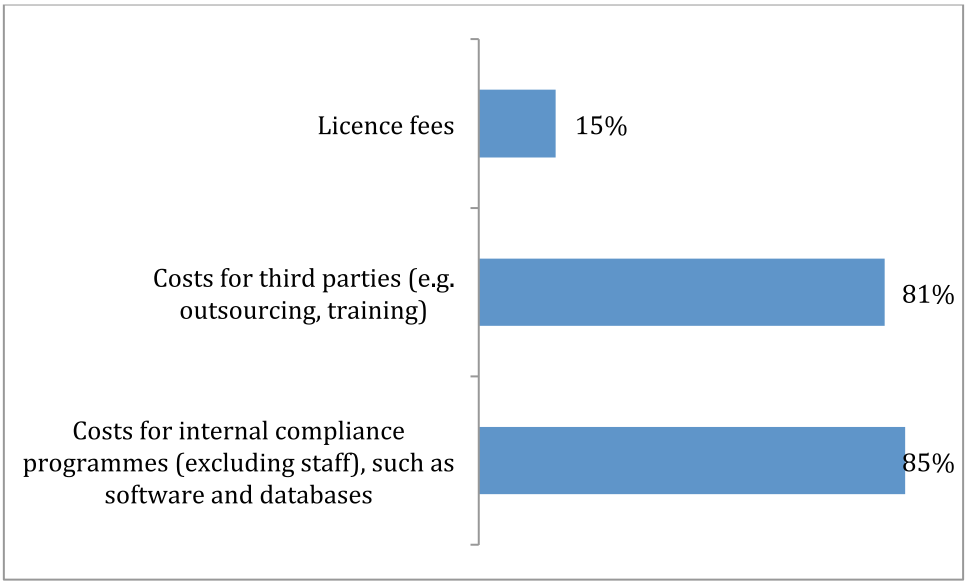
6.2.4 Economic effects of the current dual use export control policy: compliance costs and competitive effects

Going into detail on the issues related to the export control process, 81% of the companies affirmed that the administrative burden related to compliance with the dual-use export requirements is heavy and time-consuming and 74% reported that the procedures are complex. The latter percentage is lower if we consider companies located in the Southern and Eastern Europe, respectively 55% and 58%.

Compliance costs faced by companies are mainly related to the staff involved in the export control management. 77% of the companies declare that they have up to 10 full-time equivalent (FTE) staff in charge of dealing with the export control process and that related costs range from €500 to €4 million per year. More specifically, SMEs have up to 4 FTEs with a maximum related cost of €200,000 per year.

As shown in Figure 6.8 below, the other costs are mainly related to aspects of the internal compliance programmes, such as software and databases. These are relevant for 88% of large companies and 68% of SMEs. Costs for third parties such as outsourcing and training are relevant for 81% of the companies with no differences between SMEs and large companies. In the companies that responded to the survey, the costs for ICPs (excluding staff) range from €2,000 to €300,000 and the costs for third parties from €2,000 to €100,000 per year.

Figure 6.8. The types of costs related to compliance with dual-use export controls

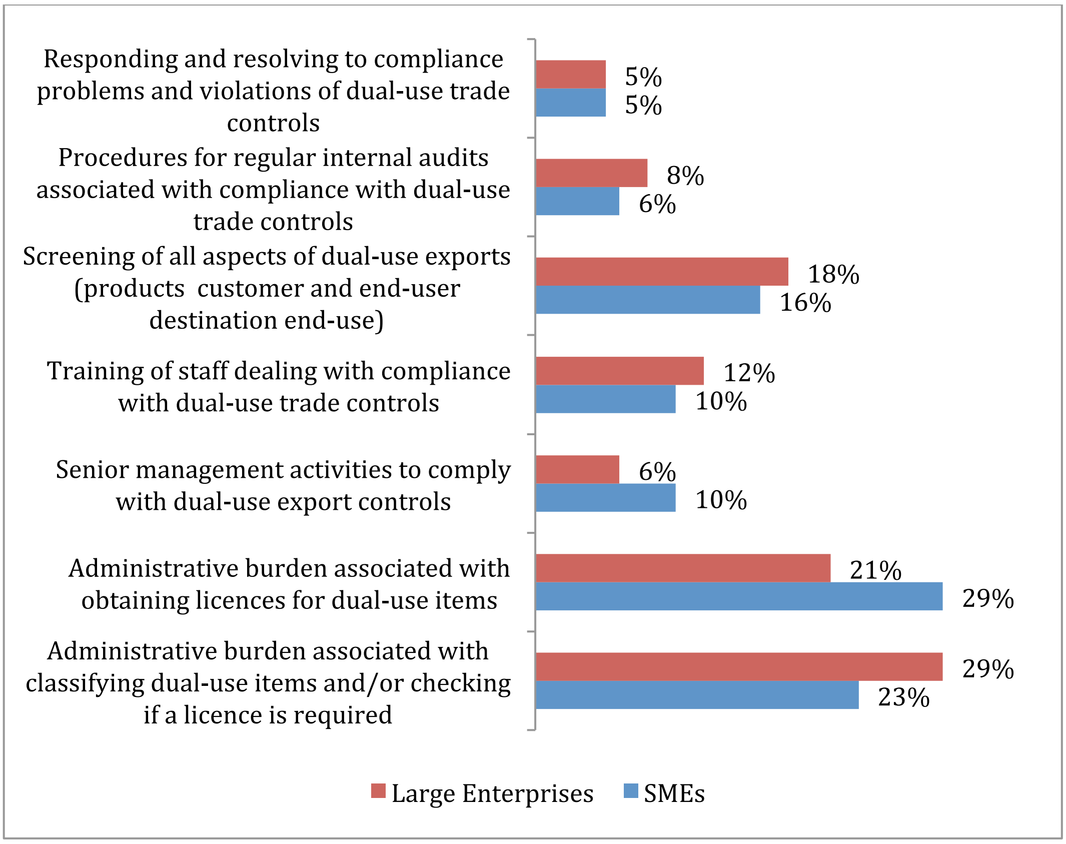


Total respondents=123

Source: SIPRI/Ecorys company survey

The costs are mainly related to the administrative burden associated with classifying dual-use items and/or checking if a licence is required, especially for large enterprises; and with obtaining licences for dual-use items, especially for SMEs. The third activity that influences costs is the screening of all aspects of dual-use exports, such as products, customer and end-user, destination and end-use. Figure 6.9 presents how the costs of complying with dual-use export controls are distributed among the above-mentioned activities comparing the results of SMEs and large enterprises.

Figure 6.9. Distribution of the costs of complying with dual-use export controls among the activities



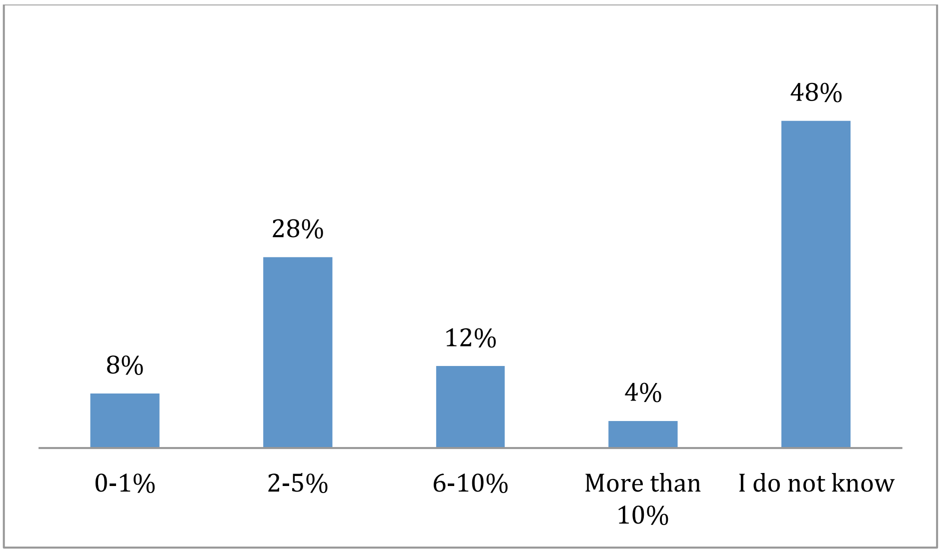
Total respondents=139

Source: SIPRI/Ecorys company survey

Figure 6.10 shows an estimation of the share of the compliance costs in total turnover at industry level.[74]

[74] Almost half of the associations could not indicate the share of compliance costs.

Figure 6.10. Share of compliance costs in total turnover at industry level



Total respondents=25

Source: SIPRI/Ecorys business association survey

With respect to other costs related to dual-use export controls, on average companies, specifically more SMEs than large enterprises, declared that only on very few occasions/sometimes they lost a deal (47% of companies) or money (54% of companies) due to the length of time it took to obtain licences. 42% of the companies have never lost a deal and 34% have never lost money.

The majority of the associations declared that with respect to competition from third countries, similar items are produced both in countries where export controls apply or where these are not in place. With regard to the level playing field, about 20% of the companies declared that they have received a denial for a licence application when another exporter fulfilled the deal through an identical export. Among the EU companies that received a denial, 54% declared that an essentially identical export was made from another Member State and the remaining 46% affirmed that the export was done from a third country.

Concerning the level playing field in the EU, 60% of the associations declared that the current dual-use export controls give rise to significant distortions between companies located in different Member States, in terms of different application of the regulation and of the requirements imposed by the licensing authorities. The situation in which a certain type of licence (individual, national general, or global) is offered also differs between EU Member States. Some companies also confirm this situation reporting that EU countries differ considerably in interpretation of laws, regulations and catch all clauses, with the consequence that export approvals can be unpredictable and non-comparable among Member States.

Moreover, the information that has to be provided to the licensing authorities to obtain the licence has varying levels of detail across different Member States. However, during the interviews, few companies were able to provide specific examples of this from their own experience. Finally, according to some companies distortions of competition can arise between a company that can get a national general licence and a company that cannot apply for its national licence. It is important to note that 52% of the companies that responded to the survey consider the process of obtaining a national licence to have low and very low efficiency.

Concerning the situation with third countries, most of the associations (76%) affirm that the current dual-use export controls give rise to significant distortions between EU companies and third country competitors such as China, USA, India and Russia. Among the factors that can give rise to this distortion, the associations mentioned the fact that some competitors are not members of international export control conventions and/or have a more streamlined system with licence exemptions. More specifically, in the semiconductor industry the distortion of competition with the USA is related to national US export legislation and licence exemptions (for semiconductor products with cryptographic features). Concerning the machinery industry, the distortion is particularly accentuated with China, one of the most important destination countries, as many kinds of dual-use items listed in Annex I of the Dual-use Regulation are produced by Chinese companies. However, it was pointed out that currently this was the case more for lower-end products, but this is in the process of changing (see case study in Chapter 8). Finally, in addition to the export control issues, companies mentioned applied sanctions (e.g. EU and US sanctions against Russia) as a critical aspect that negatively influences competition with third countries.

6.2.5 Effects of export controls related to other value chain actors: Technology transfer, brokering and transit controls

Half of the companies work with academia and research institutes and, according to one third of them, export controls affect this co-operation and the innovative capacity of the company. In this regard, large enterprises seem to be more affected than SMEs. One of the reasons is that research institutes located outside the EU are often unaware of the procedures to follow and of the licensing requirements. This can lead to delays in execution of projects and can hamper cooperation with European companies, especially in the chemical sector.

Moreover, export controls slow down the interactive process between companies and these stakeholders, and in the case of intra-technology transfers they limit the innovative capacity of companies.

Finally, the export control process can influence the decision as to whether to introduce a new product. When designing and developing new products, companies refer to the Dual-use Regulation and the list of controlled items to ensure that the product is developed in such a way as to avoid becoming subject to subsequent export controls—or at least that it only becomes subject to export controls as a result of a deliberate decision. This limits the companies' freedom to innovate and entails regulatory compliance costs for companies.

An example is given by the semiconductor industry, which is one of the most innovative industrial sectors in Europe and consistently ranked among the very top R&D intensive sectors by the European Commission. Export control policies and regulations form part of the framework conditions within which businesses operate. As such, export controls play an important role in investment decisions by companies and in Europe's attractiveness for the semiconductor industry. According to the survey response, the slow reactivity of the EU export controls to market developments risks affecting semiconductor businesses, and therefore innovation, on a daily basis. According to one business association, this was especially true in areas such as cryptographic goods, where controls exists in the EU, but not in other regions, including the USA. This association reported that the lack of a level playing field vis-à-vis third countries put EU semiconductor exporters at a disadvantage compared to competitors from third countries. In the long run it also affects their ability to innovate.

Regarding the cooperation with brokers/freight forwarder/transporting companies, about half of the respondents declared that there are no changes in relation to these actors as a result of the regulation. The most common change recognised by 39% of the companies is the increase of administrative requirements, especially in the chemical sector.

6.2.6 Social and environmental impacts of the dual-use export control policy

This section aims at identifying the potential impacts and effects of the dual-use items produced by the associations' industries on society and the environment.

More than half of the associations do not know about any social effects related to the dual-use items produced by their members and almost 7 out of 10 do not know about any environmental effects related to the production and trade of dual-use items. More specifically, 28% of the associations indicated that the use or consumption of dual-use items generate positive effects on security.

According to 28% of the associations, the use and consumption of the dual-use items of their members generate mainly positive environmental effects, mainly on air pollution and emissions, and energy and resource use. Over half of the respondents could not specify whether the use and consumption of dual-use products could have an impact, either positive or negative, on the environment.

6.2.7 Assessing the impact of review options

Review issue 'Develop EU export control network'

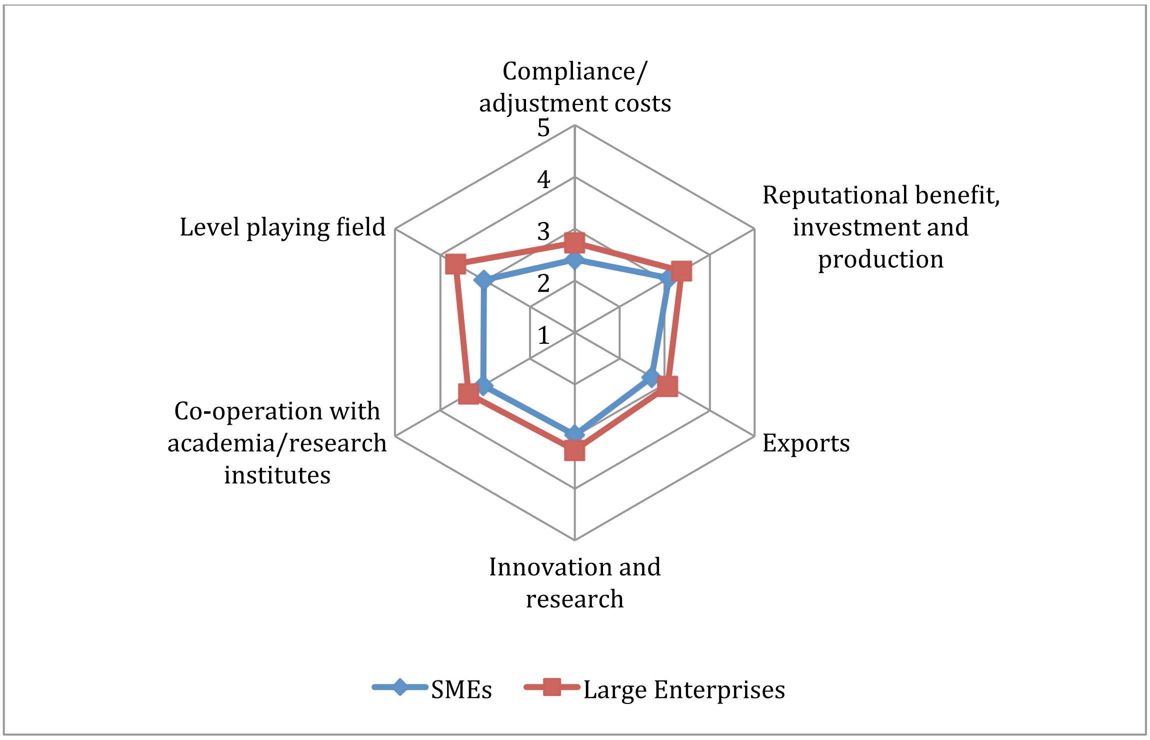
The Communication 'The Review of export control policy: ensuring security and competitiveness in a changing world' identifies options to enhance information exchange and develop IT infrastructure. In this context, on the one hand, half of the companies (among which there are more SMEs than large enterprises) declared that they can apply for licences electronically and significantly benefit from it. On the other hand, almost one fourth of these companies can apply for licences electronically but say they do not significantly benefit from it. Most of the companies that cannot apply for licences electronically are located in Southern European countries.

Review issue 'Private Sector Partnership'

The majority of the associations affirmed that their members reported distortions of competition associated with varying levels of industry compliance both within the EU and in third countries. And in view of supporting and facilitating the dual-use export procedures and ensuring a level playing field, the associations declared that their members would benefit more from EU-wide soft law measures than from EU-wide legal requirements. Consistent EU-wide legal requirements are considered both by associations and companies to have a negative impact on the compliance and adjustment costs. However, 28% of the companies consider EU-wide legal requirements to have a positive/very positive impact on the level playing field.

Figure 6.11 presents the impact of consistent EU-wide legal requirements for industry compliance, combined with transparency and outreach on SMEs and large enterprises. It presents average values of impact on a scale that ranges from 1 (very negative impact) to 5 (very positive impact). In general large enterprises would experience a more positive impact than the SMEs, especially on the level playing field and the reputational benefit, investment and production. More specifically, SME exports would be negatively impacted. Both SMEs and large enterprises would have a negative impact on compliance/adjustments costs.

Figure 6.11. Impact of consistent EU-wide legal requirements for industry compliance*



*1=very negative impact; 3=neutral; 5=very positive impact

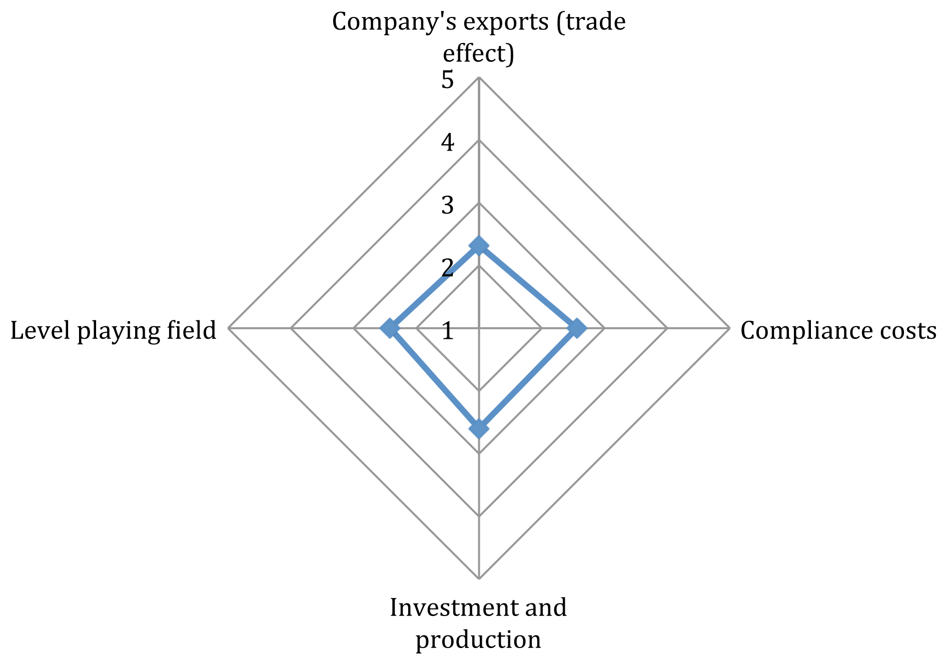
Total respondents=177-182

Source: SIPRI/Ecorys company survey

Review issue 'Catch-all controls'

Six out of every ten associations declared that their members have reported divergent applications of catch-all controls in the EU. About one third of the companies affirm that the differences in applications or interpretations of catch-all controls across the EU generate legal uncertainty and loss of business to the benefit of another company. More specifically, as shown in figure 6.12 below, divergent applications have a general negative impact on companies. It should be noted that almost half of the companies could not indicate the impact of the differences in applications or interpretations of catch-all controls in EU Member States.

Figure 6.12. Impact of the differences in applications or interpretations of catch-all controls in EU Member States*



*1=very negative impact; 3=neutral; 5=very positive impact

Total respondents=166-167

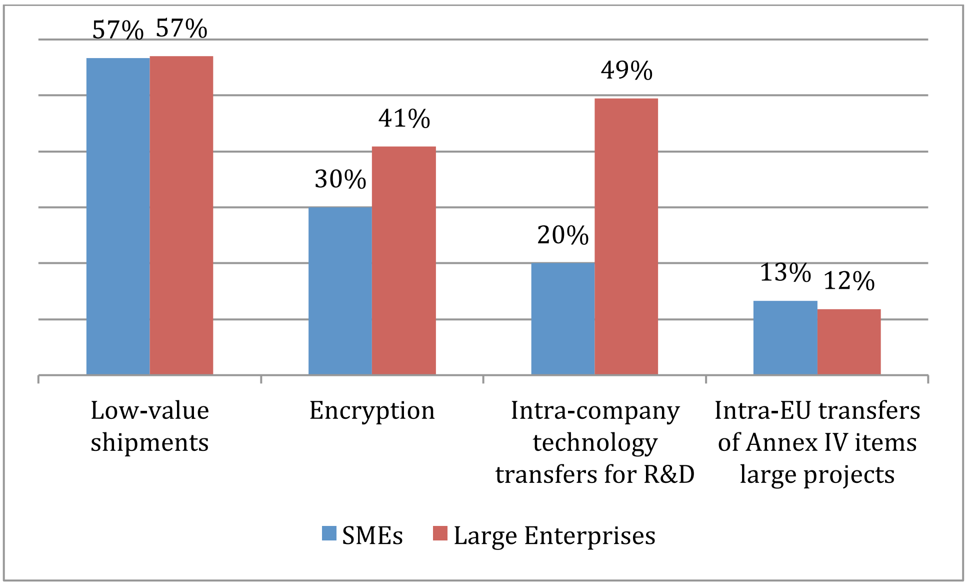
Source: SIPRI/Ecorys company survey

Review issue 'Optimisation of licensing architecture'

Companies would expect to highly benefit from an EU General Export Authorisation (EUGEA) for low-value shipments (57%) and for intra-company technology transfer for R&D (42%), with a positive impact especially on the level playing field and the company's exports. 37% of the companies would benefit from an EUGEA for encryption and 12% from an EUGEA for intra-EU transfer of Annex IV items large projects, with a positive impact on their export and compliance costs. More specifically, companies producing electrical machineries would particularly benefit from an EUGEA for encryption. Results from business associations are in line with the information collected from the companies.

Figures 6.13 and 6.14 below present the EUGEAs from which SMEs and large enterprises would expect to highly benefit, and the type of impact expected by companies. It should be noted that large enterprises compared to SMEs would have a more positive impact from the introduction of the EUGEAs. SMEs consider that the EUGEA for intra-EU transfer of Annex IV items large projects would have either a negative or no impact at all.

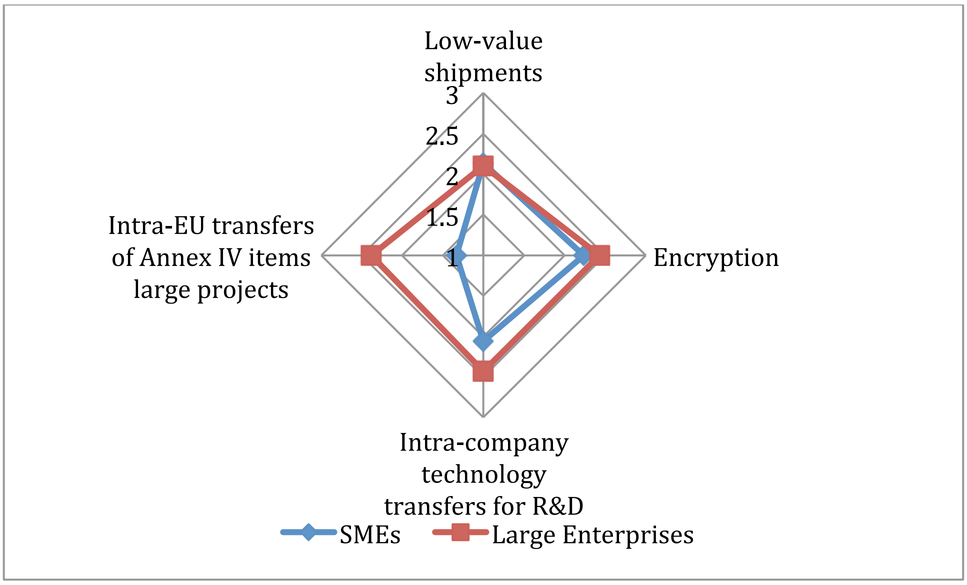
Figure 6.13. EU General Export Authorisations from which companies expect to highly benefit by company size



Total respondents=123

Source: SIPRI/Ecorys company survey

Figure 6.14. Impact of the introduction of EU General Export Authorisations by company size[75]



*1=no/negative impact; 3=very positive impact

Total respondents=15-70

Source: SIPRI/Ecorys company survey

Review issue 'Legal clarifications/amendments'

The majority of the associations see a need for legal clarification on control of technical assistance (67%) and control of intangible technology transfer (ITT) (64%). This is confirmed by companies: 42% of them would like to have a legal clarification on control of ITT and 35% on control of technical assistance. These figures increase to 47% and 41% if we consider only large enterprises.

More specifically, according to some companies the term "technical assistance" is not exhaustively defined in the main text of the regulation. Companies reported that it can be difficult to assess what is covered by the reference to technical assistance and in order to prevent differing national interpretations, including a clear definition in the regulation, preferably with practical examples, could provide more legal certainty.

Concerning the basic notions, the survey indicates a need for clarification and harmonisation of the definition of exporter, as the actual definition can be and is interpreted differently among companies and Member States.

Table 6.1 below presents the review issues and the aspects that would have a strong economic and security impact on companies. Regarding the negative impact on security, a few companies reported vague aspects that do not refer to any review issues. For this reason, these are not included in the table.

[75] The impact of the introduction of the different EUGEAs was rated by the companies that selected the specific EUGEAs in the previous question.

Table 6.1. Review issues and aspects impacting companies

Strong positive economic impact
- Review issue 'Optimisation of licensing architecture': an EUGEA for encryption, low-value shipments and Intra-company technology transfer for R&D - Review issue 'Catch-all controls': harmonization of treatment of catch-all controls between EU countries - Review issue 'Develop EU export control network': electronic application - General harmonization within the EU member states (e.g. concerning licensing and enforcement)
Strong negative economic impact
- Increasing requirements for reporting and documentation in respect of export control regulations (e.g. AEO) - Different rules within EU and external (e.g. US law for companies based in the United States) - Political embargo regulations - Each review which does not ensure a level playing field
Strong positive security impact
- Self-regulation - Electronic list of blacklisted customers or institutes - Clear rules on modern IT infrastructure - Increased clarity in legislation

6.3 Perceptions of licensing authorities: survey results

The survey to licensing authorities sought to obtain information on the administrative burden of the current system and that of potential changes. 14 licensing authorities, representing 12 Member States, completed the survey. Information on EU Member States perceptions regarding the impact of controls on cyber-surveillance technologies and the potential expansion of controls in this area are presented in Chapter 7.

6.3.1 Current system

Resources dedicated to dual-use export control

The total budget of each export licensing authority (as per Art.9 of the EU Dual-use Regulation 428/2009) differs markedly from one Member State to another. In interpreting these budgets, the very different institutional settings in Member States should be kept in mind. Licensing authorities may be dedicated authorities, a unit within a larger department, or a dedicated department within a Ministry. Some countries, notably Belgium and Sweden, have more than one authority dealing with licences for dual-use exports. Moreover, there are different ways to calculate the proportionate budget, and not all Member States maintain statistics on this.

EU Member States that provided relevant data indicated that the budget dedicated to dual-use export controls ranges from €70,000 to €5.9 million. In Sweden for example, the total budget of ISP is 1.2 million €, of which 86% is estimated to be spent on dual-use export controls. The number of export licence applications in 2013 ranged from 26 to more than 16,000 in EU Member States.[76] It can be assumed that staff resources will partly be a function of the size of the country and dual-use industry. However, data provided by EU Member States indicates that there is no direct correlation between the number of export licence applications and staff numbers.

Data provided by EU member states indicates that the highest share of total resource, on average between 20% and 50%, is dedicated to the activity of issuing licences, including going back to applicants for more information due to mistakes or insufficient information. The other activities that impact most on the total resource, on average 5-20%, are in order of importance advisory opinions/informal or formal pre-inquiries and other communication with industry, and information management. Some licensing authorities also mentioned the implementation of international and EU sanctions among other activities that have a high impact on the budget.

Similarly, the number of internal staff of the licensing authorities that are involved in the activities related to dual-use export control varies considerably across the EU. The FTE staff ranges from 2,5 to 24. In addition to dedicated staff, most licensing authorities have a substantial number of internal staff that only work on dual-use export control for a majority or a small percentage of time.

Additionally, a substantial number of combined staff from other government departments, agencies and ministries are involved in the implementation and enforcement of the Dual-use Regulation. While on average very few of them work on dual-use export control full-time (up to 11 for the Member States that participated in the survey), a substantial number (up to 15) devote the majority of their time to this issue. Up to 14 spend a small percentage of their time.

Of the EU Member States that provided relevant data, 86% indicated their licensing authorities use external expertise, mainly for technical classification, and regime proposals and statements. External expertise either does not generate other costs or they are not quantifiable.

Regarding the share of costs related to the scope of the current legislation, the share of costs related to the Dual-use Regulation is between 45% and 98% of total costs. Costs for UN and EU sanctions range from 10% to 37%. The category 'other' includes costs related to national regulations and legislation, the participation in regime meetings and administrative issues.

Implementation challenges

The main challenges linked to the management of dual-use export controls based on the EU Dual-use Regulation 428/2009 are listed in Table 6.2 below. The responses show clearly that insufficient staff resources are a major challenge, closely related to

[76] Confidential data from EU licensing authorities, 2013.

the lack of technical expertise and staff, and challenges in the technical and risk assessment. All other issues highlighted also present current implementation and enforcement challenges. While some of them are considered in the current review options, the main challenge of staff resources is not directly addressed.

Table 6.2. Main challenges linked to management of dual-use export controls

List of challenges	**N.***
Lack of staff resources	6
Technical expertise and technical staff	5
Technical and risk assessment, gathering of end-use(r) related information and guarantees	4
Efficient/short processing of export licence	3
IT-resources, IT infrastructure, e-licensing tools	2
Harmonized view with other Member States and level-playing field for all national applicants with regard to overall implementation within and outside the EU	2
The number, diversity and complexity of sanctions	1
Implementation of some provisions of the Reg. 428/2009, such as Article 8	1
Assessment of human rights aspects	1
Securing a short case processing time, and at the same time keeping track of multiple consultations to other authorities and other Member States in the licensing procedure	1
Lack of technical knowledge in the customs authorities	1
Unclear link between the HS-codes and the dual-use control codes for the companies and for customs	1

*N.=number of times that the challenge was mentioned by the authorities

6.3.2 Review options

Review option 2: Implementation and enforcement support

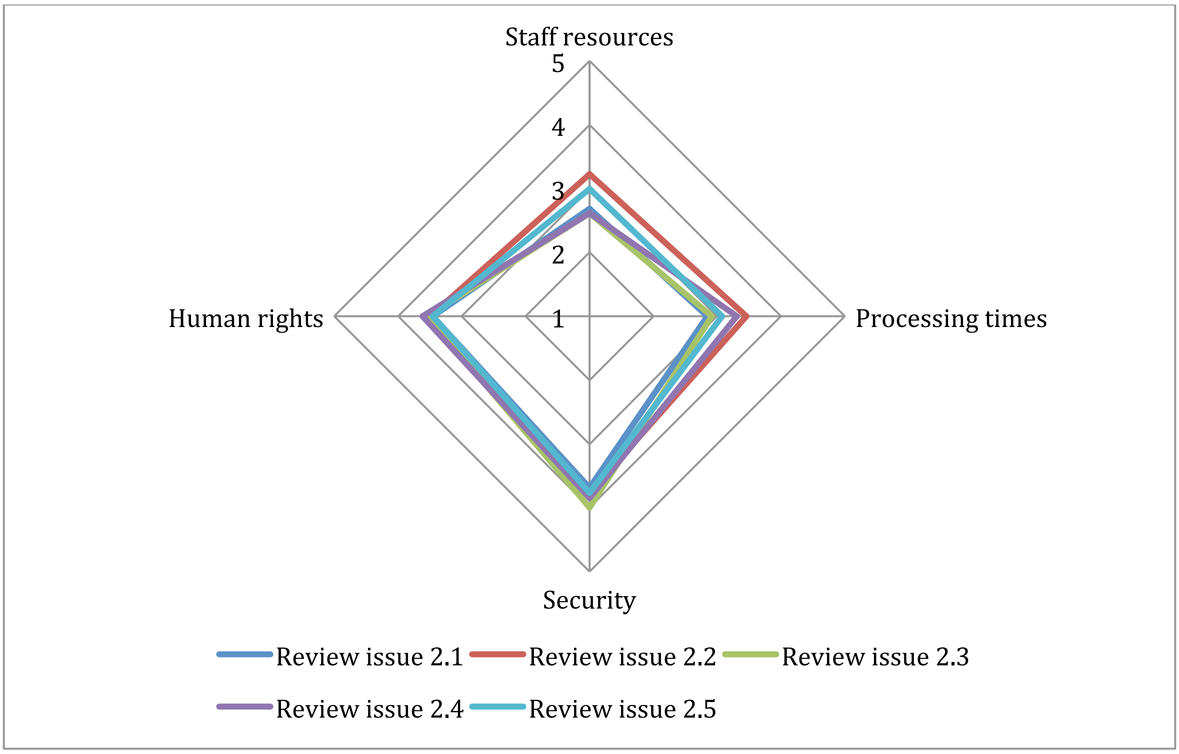
According to the licensing authorities, review issues 2.1 and 2.3 ('development of EU export control network' and 'strengthening implementation of ITT controls') would have a negative impact on staff resources and processing time. Additionally, review issue 2.4 ('rapid reaction to technological changes and active contribution to control list discussions in regimes') would negatively impact staff resources. More specifically with regard to staff resources, all three issues are expected to have a negative impact on information management, while private sector partnership and the promotion of global convergence of export controls are considered neutral from this perspective (see Table 6.8 below). Security and human rights would benefit from review option 2 overall (Implementation and Enforcement Support). The average scores, ranging from 1-very negative impact to 5-very positive impact, are presented in Table 6.3 and Figure 6.15.

Table 6.3. Impact of review issues under review option 2 in terms of administrative burden and human rights*

	Staff resources	Processing times	Security	Human rights
Review issue 2.1: Develop EU export control network	**2,69**	**2,85**	3,69	3,46
Review issue 2.2: Private Sector partnership	3,23	3,46	3,77	3,5
Review issue 2.3: Strengthen implementation of ITT controls	**2,62**	**2,92**	4	3,54
Review issue 2.4: Rapid reaction to technological changes and active contribution to control list discussions in regimes	**2,62**	3,31	3,85	3,62
Review issue 2.5: Promote global convergence of export controls	3	3,08	3,77	3,46

*1=very negative impact; 3=neutral; 5=very positive impact

Figure 6.15. Impact of review issues under review option 2 in terms of administrative burden and human rights*



*1=very negative impact; 3=neutral; 5=very positive impact

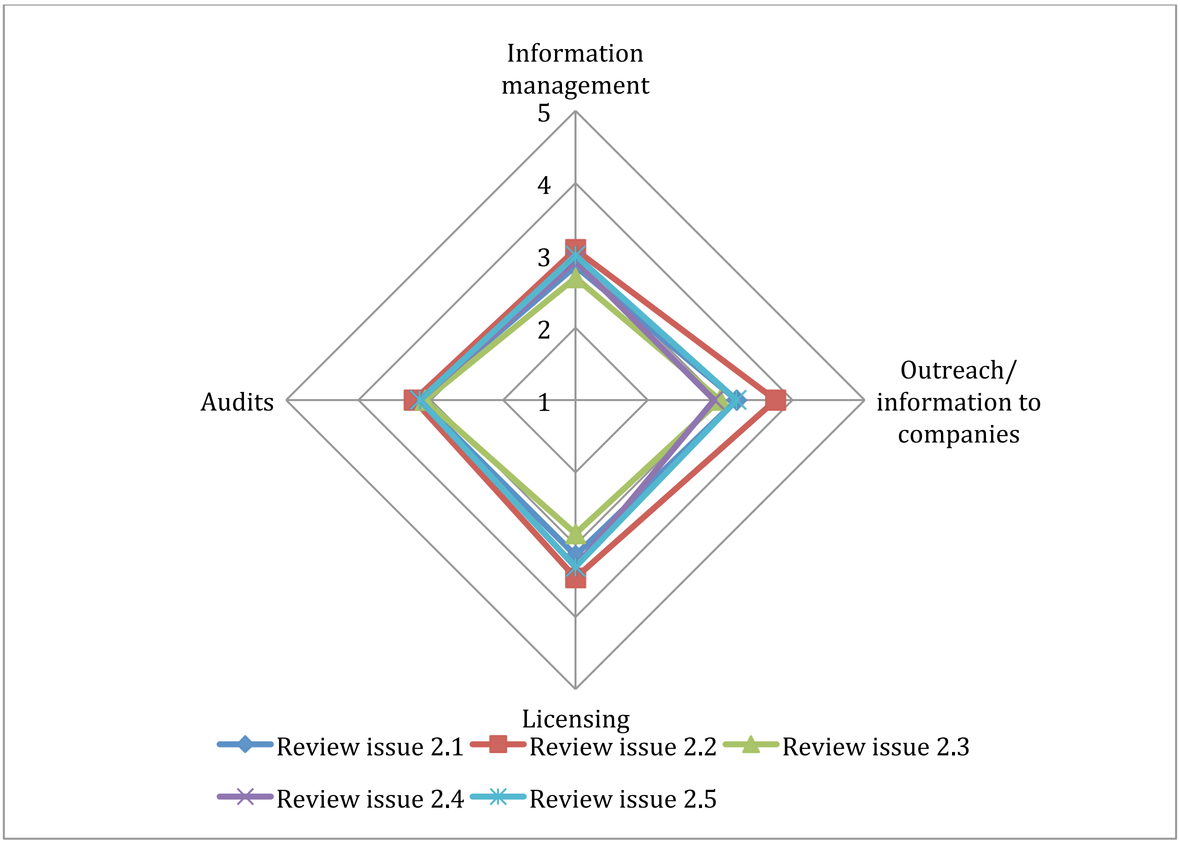
According to survey result on the impact of review option 2 on staff resources, the aspect of outreach/information to companies would on average be slightly negatively impacted by review issue 2.4: Under the heading 'rapid reaction to technological changes and active contribution to control list discussions in regimes', the actions proposed include an EU technological reaction capacity mechanism and guidance on emerging technologies. Licensing authorities therefore expect that a slight increase in staff resources would be needed to take this issue forward as proposed. No impact is expected on this aspect with review issue 2.3 (strengthened ITT implementation) and the remaining review issues, especially 2.2 (private sector partnership), would positively impact it. It is expected that staff resources for the licensing process would be negatively impacted by review issue 2.3 (enhanced implementation of ITT controls), as a result of higher requirements for staff time. Finally, audits in general would experience a slightly positive impact from the review option 2 as a whole. Information management demands are apparently expected to somewhat increase since the impact was assessed as slightly negative for all issues listed in Table 6.8 below, except for the private sector partnership which would have a slightly positive impact. The average scores, ranging from 1-very negative impact to 5-very positive impact, are presented in Table 6.4 and Figure 6.16.

Table 6.4. Impact of review issues under review option 2 with respect to staff resources*

	Information management	Outreach/information to companies	Licensing	Audits
Review issue 2.1: Develop EU export control network	**2,85**	3,23	3,15	3,15
Review issue 2.2: Private Sector partnership	3,08	3,77	3,46	3,23
Review issue 2.3: Strengthen implementation of ITT controls	**2,69**	3	**2,85**	3,08
Review issue 2.4: Rapid reaction to technological changes and active contribution to control list discussions in regimes	**2,92**	**2,92**	3,31	3,15
Review issue 2.5: Promote global convergence of export controls	3	3,23	3,31	3,15

*1=very negative impact; 3=neutral; 5=very positive impact

Figure 6.16. Impact of review issues under review option 2 with respect to staff resources*



*1=very negative impact; 3=neutral; 5=very positive impact

Table 6.5 below presents the impact, ranging from 1-very negative to 2-very positive, associated with each action included in the review option 2. It shows that most actions under this option, would have a very positive or positive impact, notably 'enhanced information exchange and development of IT infrastructure through use of DUeS' (the EU's Dual-Use Electronic System), 'training and capacity-building', and 'effective mechanisms for regular updates of the EU control list'. These were closely followed in popularity by 'ICP requirements through guidelines' and 'enhanced cooperation with enforcement agencies'. A range of other measures intended to enhance cooperation and information exchange also received positive scores. Only 'transparency and coordinated outreach' receives on average a neutral score, and 'promotion of convergence with the AEO programme' is the only one to receive a negative score.

Table 6.5. Impact of actions of review option 2*

Impact		Review actions
Very positive	2	2.1.1.c Enhance information exchange and develop IT infrastructure: Use DUeS to this purpose
	2	2.1.3 Training/capacity-building (EU-wide capacity-building programme and training for officials and further develop EU pool of experts)
	2	2.4.3 Set up effective mechanism for regular update of EU control list drawing on MS expertise
	1,91	2.2.1 Due-diligence/ICP requirements through guidelines: Set clear private sector compliance standards for use of simplified mechanisms as a 'substantial benefit' for 'reliable exporters' through guidelines
	1,9	2.1.2.b Enhance strategic and operational cooperation with enforcement agencies: Develop common risk management tools and framework
	1,83	2.1.1.e Enhance information exchange and develop IT infrastructure: Develop standardised IT support tools and electronic licensing systems across the EU (see also 3.3.6)
	1,82	2.3.1 Provide guidance
	1,8	2.1.1.b Enhance information exchange and develop IT infrastructure on other information e.g. destinations, end-users, incidents and violations
	1,78	2.4.2 Guidance on emerging technologies
Positive	1,75	2.1.1.d Enhance information exchange and develop IT infrastructure: Share information between and with enforcement agencies through an EU-wide exchange system (see also 2.1.2)
	1,75	2.1.2.e Enhance strategic and operational cooperation with enforcement agencies: Enhance enforcement of brokering provisions
	1,75	2.3.3 Codes of conduct for scientists

Impact		Review actions
	1,75	2.5.2 Active outreach, cooperation and assistance to partner countries
	1,71	2.1.2.a Enhance strategic and operational cooperation with enforcement agencies: Integrate export control priorities in policy cycles
	1,71	2.1.2.c Enhance strategic and operational cooperation with enforcement agencies: Implement joint operations
	1,71	2.1.2.d Enhance strategic and operational cooperation with enforcement agencies: Enhance enforcement of transit provisions
	1,71	2.4.1 'EU technological reaction capacity' mechanism (based on expertise in EU MS authorities and structured engagement with industry)
	1,7	2.5.3 Develop export control dialogues with key trading partners: To avoid 'conflicting regulatory requirements' and reduce 'administrative burden on export-oriented industries'
	1,67	2.1.1.a Enhance information exchange and develop IT infrastructure on licensing data
	1,67	2.3.2 Outreach to the academic research community
	1,57	2.5.1 Promote coherent, comprehensive, unified EU representation in the regimes
Neutral	1,5	2.2.2 Transparency: Transparency and coordinated outreach through publication of reports/non-sensitive control information, including guidance on good compliance practices
Negative	1,4	2.2.3 Promote convergence with the AEO programme

*1=very negative; 2=very positive

Review option 3: EU system update (option 2 + upgrades of existing regulations)

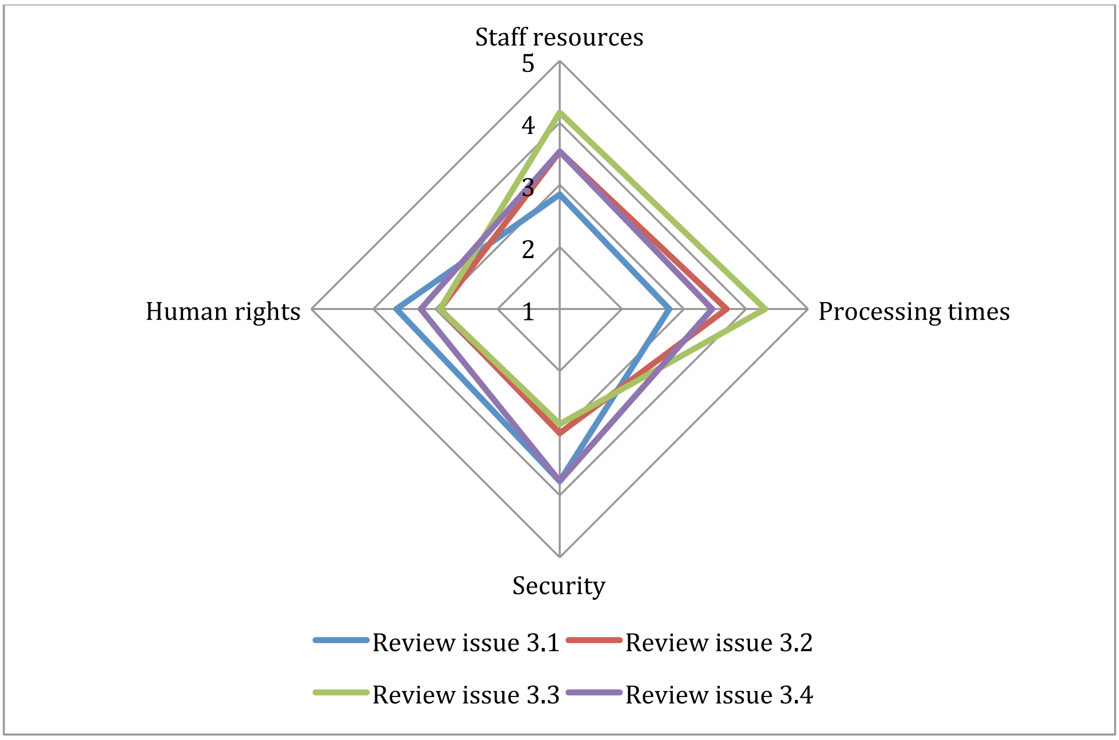
According to the licensing authorities, the actions proposed to achieve catch-all convergence would have a slightly negative impact on the staff resources and the processing time but a positive impact on security and human rights. On the contrary, review issue 3.3 (the actions proposed to optimise the licensing architecture, such as additional EU GAEs) would negatively impact security and human rights, while staff resources and processing time would highly benefit from it. Legal clarifications and amendments (review issue 3.4) would have a general positive impact on each aspect. A critical re-evaluation of intra-Community transfers is expected to positively affect staff resources and processing times, while the impact on security would be neutral, and for human rights neutral to slightly negative. The average scores, ranging from 1-very negative impact to 5-very positive impact, are presented in Table 6.6 and Figure 6.17.

Table 6.6. The impact of review issues under review option 3 in terms of administrative burden, security and human rights*

	Staff resources	Processing times	Security	Human rights
Review issue 3.1: Catch-all convergence	**2,85**	**2,77**	3,77	3,62
Review issue 3.2: Critical re-evaluation of EU transfers	3,54	3,69	3	**2,92**
Review issue 3.3: Optimisation of licensing architecture	4,17	4,31	**2,85**	**2,92**
Review issue 3.4: Legal clarifications and amendments	3,54	3,46	3,77	3,23

*1=very negative impact; 3=neutral; 5=very positive impact

Figure 6.17. Impact of review issues under review option 3 in terms of administrative burden and human rights*



*1=very negative impact; 3=neutral; 5=very positive impact

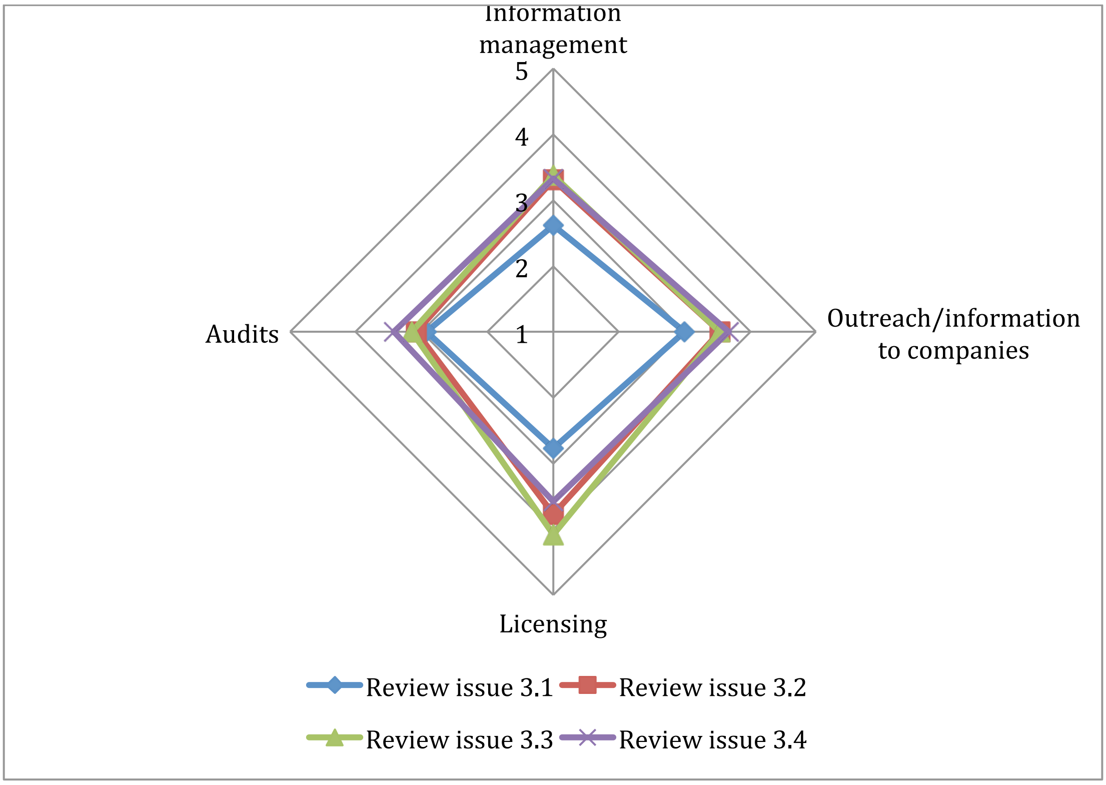
With respect to staff resources, review issue 3.1 would negatively impact information management, licensing and audits. Review issues 3.2, 3.3 and 3.4 would have a positive impact on all the aspects analysed, especially on the licensing process. The average scores, ranging from 1-very negative impact to 5-very positive impact, are presented in Table 6.7 and Figure 6.18.

Table 6.7. Impact of review issues under review option 3 with respect to staff resources*

	Information management	Outreach/information to companies	Licensing	Audits
Review issue 3.1: Catch-all convergence	**2,62**	3	**2,77**	**2,92**
Review issue 3.2: Critical re-evaluation of EU transfers	3,31	3,54	3,77	3,08
Review issue 3.3: Optimisation of licensing architecture	3,38	3,54	4,08	3,15
Review issue 3.4: Legal clarifications and amendments	3,33	3,67	3,58	3,42

*1=very negative impact; 3=neutral; 5=very positive impact

Figure 6.18. Impact of review issues under review option 3 with respect to staff resources*



*1=very negative impact; 3=neutral; 5=very positive impact

Table 6.8 below presents the impact, ranging from 1-very negative to 2-very positive, associated with each action included in the review option 3. Again, most review actions under this option are expected to have an overall positive impact, notably 'clarifications of key terms in the Regulation' as well as a 'review of the parameters of existing EUGEAs'. Only the action that would introduce 'extraterritorial provisions for EU persons' has a neutral score, while 'information exchange and establishment of a catch-all database that would partly shared with customs and partly made public and thus accessible to companies' is the only action that is expected to have a negative impact.

Table 6.8. Impact of actions of review option 3*

Impact		Review actions
Very positive	2	3.3.1 Review parameters for existing EUGEAs
	2	3.4.1 Clarify notion of export and exporter
	2	3.4.2 Review determination of competent authority (especially for non-EU companies)
	2	3.4.3 Update control of technical assistance
	1,9	3.4.4 Review/clarify legal framework on ITT controls and adjust control modalities
	1,89	3.2.2 Introduce EUGEA for intra-EU transfers: Including technology transfers, combined with post-shipment verification
	1,89	3.4.8 Legal ICP requirements
	1,83	3.3.4 Facilitate exports: introduce regular review of NGEAs and discuss possible transformation into EUGAEs
	1,83	3.3.6 Develop standardised IT support tools and electronic licensing systems across the EU
	1,82	3.2.1 Review of Annex IV: Update list and reduce to most sensitive items
	1,8	3.1.1 Definition: Harmonise notion of catch-all controls across the EU
	1,8	3.3.2 Introduce additional EUGEAs: e.g. for low-value shipments, encryption, intra-company technology transfers for R&D
	1,8	3.3.7 Shifting emphasis on end-use monitoring
Positive	1,75	3.3.3 Introduce ITT facilitation tools: e.g. EUGEAs for intra-company research and development, combined with focus on pre-transfer

		control (registration, self-auditing) and post-transfer monitoring (compliance audits)
	1,75	3.3.5 Prepare guidelines for consistent licensing practices: e.g. best practices for processing times
	1,75	3.4.6 Enhance consistency of brokering provisions
	1,71	3.4.5 Enhance consistency of transit provisions
	1,62	3.1.3 Consultation process: Strengthen consultation to ensure EU-wide application and reinforce no-undercut policy
Neutral	1,5	3.4.7 Extraterritorial provisions for EU persons (to prevent circumvention)
Negative	1,43	3.1.2 Information exchange: Regular information exchange and establish EU catch-all database (partly shared with customs and partly made public and thus accessible to companies)

*1=very negative; 2=very positive

7. The cyber-surveillance sector

7.1 Introduction

During 2011, companies based in the EU (as well companies based in other parts of Europe and North America) were identified as having been involved in the supply of cyber-surveillance goods, services and technologies (hereafter 'cyber-surveillance technologies') to states in the Middle East and North Africa. In some cases, these technologies were used by law enforcement agencies (LEAs) and intelligence agencies in connection with violations of human rights. Existing EU and Wassenaar Arrangement strategic trade control lists did not cover many of the goods, services and technologies involved.

In late 2011 and early 2012, the EU arms embargoes on Iran and Syria were both updated to include prohibitions on the sale of surveillance technologies. In December 2011, the EU embargo on Syria was updated to include a ban on the 'sale, supply, transfer or export of equipment or software intended primarily for use in the monitoring or interception by the Syrian regime, or on its behalf, of the Internet and of telephone communications on mobile or fixed networks', as well as the provision of associated services.[77] In March 2012, equivalent language was inserted into the EU embargo on Iran.[78]

In 2012 and 2013 certain categories of surveillance technologies—specifically, 'mobile telecommunications interception or jamming equipment', 'IP network surveillance systems' and 'intrusion software'—were added to the Wassenaar Arrangement's dual-use control list. In December 2014, these items were added to the EU's dual-use list. The EU and its Member States are currently debating whether and how to create an expanded set of controls on cyber-surveillance technologies via the EU Dual-use Regulation.

These developments have fed into a broader discussion about the potential need to expand both the items covered by the EU's dual-use export controls and the considerations that Member States take into account when assessing export licences. This would involve making more items subject to control on the basis of a broader range of human rights and security risks and taking a broader range of human rights and security considerations into account when making licensing assessments. One way to facilitate this expansion would be to apply a 'human security' approach to export controls for dual-use goods. According to the European Commission, this would potentially involve 'a clarification of control criteria to take into consideration broader

[77] Council Decision 2011/782/CFSP of 1 December 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP, Official Journal of the European Union, 2 Dec. 2012.
[78] Council Decision 2012/168/CFSP of 23 March 2012 amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran, Official Journal of the European Union, 24 Mar. 2012, p. 85.

security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations'.[79]

This section of the study presents data that is intended to help assess the impact of current controls on cyber-surveillance technologies and the potential impact of the further expansion of controls in this area via the implementation of relevant review options.

7.1.1 Mapping the 'cyber-surveillance' sector

There is no agreed definition of 'cyber-surveillance technology' nor is there any agreed definition of what constitutes the 'cyber-surveillance sector'. Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, one stated that that it had a national definition of 'cyber-surveillance technologies'.

The word 'cyber' means anything that takes place through the use of computers or information and telecommunication networks.[80] Cyber-surveillance could hence be defined as surveillance through the use of computers and telecommunication networks. It entails the monitoring and exploitation of data or content that is stored, processed or transferred via information and communications technologies. This includes devices like computers and mobiles phones but also telecommunications networks.

However, since this meaning has not been agreed upon by a standard setting body, different actors interpret the term 'cyber-surveillance' in different ways. Meanwhile, some actors seek to avoid using the term cyber-surveillance technologies altogether, arguing that it is either too narrow or too vague. Instead, they prefer alternative terms, such as 'information communication technology (ICT) surveillance', 'electronic surveillance' or 'digital surveillance'.[81]

One way of defining the cyber-surveillance sector is to situate it at the cross section of the 'ICT sector' and the 'surveillance sector'. This sub-section of the report attempts to describe 'cyber-surveillance sector' by situating the concept in relation to the more established concepts of the 'ICT sector' and the 'surveillance sector'. The sub-section gives an overview of the size and composition of both the ICT sector and the surveillance sector, as well as a brief assessment of how each is affected by EU dual-use export controls. It concludes by outlining the size and scope of the cyber-surveillance sector before outlining the specific cyber-surveillance technologies that will form the focus of this chapter of the report.

[79] 'The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World', (European Commission, 24 Apr. 2014).
[80] Mriam Dunn Cavelty, 'Cyber-security', in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies,* (Routledge, 2010), pp. 154–55.
[81] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015).

ICT sector

The European Commission defines the ICT sector as 'a complex ecosystem', with actors ranging from telecommunications service providers to large equipment manufacturers to small software designers of Web-based start-ups. Individual companies in the sector may also play multiple roles: for example, manufacturing mobile phones and network components, or providing both telecommunications and Internet access services.[82] The sector is large and fragmented but can be broken down into specific sub-segments.[83] These include:

- Manufacturing of consumer and business end-user devices;
- Manufacturing of telecommunications components and networks;
- Telecommunication services;
- Web-based or cloud-based services platforms; and
- Software.

To a certain extent, all of these sub-segments have a role to play in the manufacture and delivery of cyber-surveillance technologies. However, certain companies can be seen as directly involved in the production of cyber-surveillance goods and services, because they produce items that are designed to be used for this purpose. Other companies are indirectly involved because the goods or services they produce have an inherent surveillance potential (e.g. content services providers, network equipment manufacturers, and web-based 'over the top' messaging services).

ICT sector: Data

Generating reliable data regarding the size of the ICT sector at the global level has proven difficult due to problems with data availability. The United Nations Conference on Trade on Development (UNCTAD), developed one indicator on the economic value added provided by the ICT sector, but was only able to collect information from 47 countries.[84] One independent market report calculated that the amount of revenue generated through the ICT market worldwide was €3,169 billion in 2012. However, what this figure covers is unclear since the methodology used for the calculation is not publicly available.[85]

The size of the ICT sector in the EU can be estimated with official sources, such as the Statistical Office of the European Communities (EUROSTAT) and the Organisation for Economic Co-operation and Development (OECD). Since 2012, an EU funded project,

[82] 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', (European Commission, June 2013).
[83] 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', (European Commission, June 2013).
[84] UNCTAD, Information Economy Report 2011, ICTs as an Enabler for Private Sector Development, United Nations, New York and Geneva, 2011, p. 46.
[85] 'Global ICT revenue from 2005 to 2016 (in billion euro)' Statista, [N/D] <http://www.statista.com/statistics/268584/worldwide-ict-revenue-since-2005/>.

PREDICT, has produced an annual report on the size of the ICT sector in the EU based on these sources.[86] The 2014 report covered the period 2006-2011 and estimated that the value added (VA) to the EU by the ICT sector was €507.61 billion in 2011.[87] This figure was generated using the NACE Rev 2 definition of the ICT sector, which includes the ICT manufacturing industries, ICT trade industries and ICT services industries.

ICT services contributed €463.41 billion in 2011 (accounting for 91.29% of ICT VA and 3.65% of EU GDP), while ICT manufacturing contributed €44.19 billion in 2011 (accounting for 8.71% of ICT VA and 0.35% of EU GDP).[88] Within ICT services, the main sub-sectors are 'Computer programming, consultancy and related activities' and 'Telecommunications'. Combined, these two sub-sectors accounted for 2.86% of EU GDP in 2011. Within ICT manufacturing, the main sub-sectors are 'Manufacturing of electronic components and boards' and 'Manufacturing of communication equipment'. Combined, these two sub-sectors accounted for 0.26% of EU GDP in 2011.

ICT sector: Export controls

Transfers of ICT goods, services and technologies form a significant proportion of all dual-use related exports. Transfers of ICT goods, services and technologies are capture by ECCN Category 3 - Electronics, Category 4 - Computers, and Category 5 - Telecommunication and 'information security'. Especially significant is Category 5 - Telecommunication and 'information security', which accounts for the largest share of licences issued by EU Member States for the export of dual-use goods in terms of financial value and the third largest in terms of number of licences (see Chapter 4).

However, the correlation is far from perfect. Not all dual-use related exports of ICT goods, services and technologies are covered by ECCN category 3, 4 and 5 and not all items covered by ECCN category 3, 4 and 5 are ICT goods, services and technologies. For example, controls under category 5A002 on 'cryptography' cover a vast spectrum of goods, services and technologies, beyond both the 'ICT sector' and the 'surveillance sector'. One EU Member State noted that among the items controlled under category 5A002 are certain types of wind turbines due to the level of cryptography they employ.[89]

To generate a rough estimate of the value of dual-use related exports of ICT goods, services and technologies from EU Member States, SIPRI conducted a trade analysis using the EU correlation table and data provided by Eurostat. Eurostat CN codes were classified as correlating to either ECCN category 3, 4, or 5. Eurostat CN codes that correlated to more than one of these categories where classified as 'cross-cutting' (see

[86] See the PREDICT project on Joint Research Center of the European Commission, <http://is.jrc.ec.europa.eu/pages/ISG/PREDICT.html>.
[87] Mas Matilde and Juan Fernández de Guevara Radoselovics, 'The 2014 Predict Report: An Analysis of ICT R&D in the EU and Beyond', (European Commission, 2014), <http://is.jrc.ec.europa.eu/pages/ISG/PREDICT/PREDICT2014/documents/PREDICT2014.pdf>, p. 8.
[88] Mas Matilde and Juan Fernández de Guevara Radoselovics, 'The 2014 Predict Report: An Analysis of ICT R&D in the EU and Beyond" (European Commission, 2014) http://is.jrc.ec.europa.eu/pages/ISG/PREDICT/PREDICT2014/documents/PREDICT2014.pdf, p. 27.
[89] EU member state official, interview with the author, 16 June 2015

Table 7.1). Based on these figures, it is possible to say that dual-use related exports of Electronics were worth up to €31.7 billion in 2014, dual-use related exports of Telecommunications and 'information security' were worth up to €22.6 billion in 2014, and dual-use related exports of Computers were worth at least €2 billion in 2014.

To give a clearer view of the value of dual-use related exports of Telecommunications and 'Information Security' (the area with the highest relevance for the cyber-surveillance sector) the correlating Eurostat CN codes were re-categorized.

Table 7.1. Value of dual-use related exports ICT goods, services and technologies, 2010-2014

PRODUCT GROUP	2010	2011	2012	2013	2014
Computers	**1,071,600,970**	**1,296,135,685**	**1,517,559,637**	**1,672,466,379**	**1,961,629,471**
Systems, Equipment and Components	1,071,600,970	1,296,135,685	1,517,559,637	1,672,466,379	1,961,629,471
Electronics	**26,045,784,933**	**32,578,615,148**	**30,582,999,791**	**30,966,890,391**	**31,748,416,014**
Material	1,440,676,100	1,495,387,349	1,262,179,348	1,187,927,645	1,213,069,372
Systems, Equipment and Components	16,108,415,675	19,711,361,124	21,173,622,536	21,487,833,390	21,464,714,224
Test, Inspection and Production Equipment	8,496,693,158	11,371,866,675	8,147,197,907	8,291,129,356	9,070,632,418
Telecommunications and 'information security'	**24,621,995,082**	**28,781,652,218**	**27,193,949,536**	**25,015,129,194**	**22,649,476,884**
Systems, Equipment and Components	22,431,696,576	25,815,140,992	24,186,004,672	21,931,446,627	19,581,839,345
Test, Inspection and Production Equipment	2,190,298,506	2,966,511,226	3,007,944,864	3,083,682,567	3,067,637,539
Cross-cutting Product Groups	**57,042,868,226**	**60,552,945,617**	**61,927,366,589**	**60,293,559,730**	**62,048,500,891**
GRAND TOTAL	**108,782,249,211**	**123,209,348,668**	**121,221,875,553**	**117,948,045,694**	**118,408,023,260**

Source: Eurostat

First, Eurostat CN codes relating to materials or primary products that had applications for both the ICT sector and other industries—such as silicon, semiconductor devices, and electronic integrated circuits—were removed. Second, the Eurostat CN codes that were classified as cross-cutting products were carefully reviewed and, in certain cases, reclassified as Telecommunications and 'information security' items (see Table 7.2). Based on these figures, it is possible to say that dual-use related exports of Telecommunications infrastructure were worth up to €2.8 billion in 2014.

Table 7.2. Value of dual-use related exports of Telecommunications and 'information security' items, 2010-2014

ICT-Telecommunication	2010	2011	2012	2013	2014
Device	**21,939,595,064**	**25,452,746,388**	**24,617,779,967**	**21,431,454,162**	**19,522,525,503**
Broadcast	7,580,946,935	8,801,408,285	9,835,517,287	9,499,451,692	10,272,575,732
Telephone	14,350,493,165	16,646,737,230	14,776,276,034	11,927,032,939	9,247,397,045
Facsimile	8,154,964	4,600,873	5,986,646	4,969,531	2,552,726
Infrastructure	**6,739,156,962**	**7,200,420,552**	**5,080,448,506**	**4,686,823,518**	**4,779,047,507**
Broadcast	2,515,425,236	2,538,749,217	2,214,752,356	2,038,280,198	1,985,354,105
Telecommunication	4,223,731,726	4,661,671,335	2,865,696,150	2,648,543,320	2,793,693,402
GRAND TOTAL	**28,678,752,026**	**32,653,166,940**	**29,698,228,473**	**26,118,277,680**	**24,301,573,010**

Source: Eurostat

Surveillance sector

The surveillance sector covers goods, services and technologies used to monitor information, communication and people. These may be used for law enforcement and defence purposes, but also for commercial purposes, such as understanding customers' behaviour and preferences. As such, the surveillance sector is both a subset of the defence and security sector and an independent entity.[90]

The surveillance sector includes a highly fragmented patchwork of heterogeneous goods, services and technologies. However, it can be divided in two major segments: 'human surveillance'; and 'electronic surveillance' (see Figure 7.1). The 'electronic surveillance' segment can be further divided into three sub-segments:

(a) Information and communication interception and monitoring (e.g. mobile telecommunications interception equipment, intrusion software, Lawful Interception (data retention and mediation), social media monitoring, content filtering and blocking, deep packet inspection (DPI), and intercept access points (IAPs));

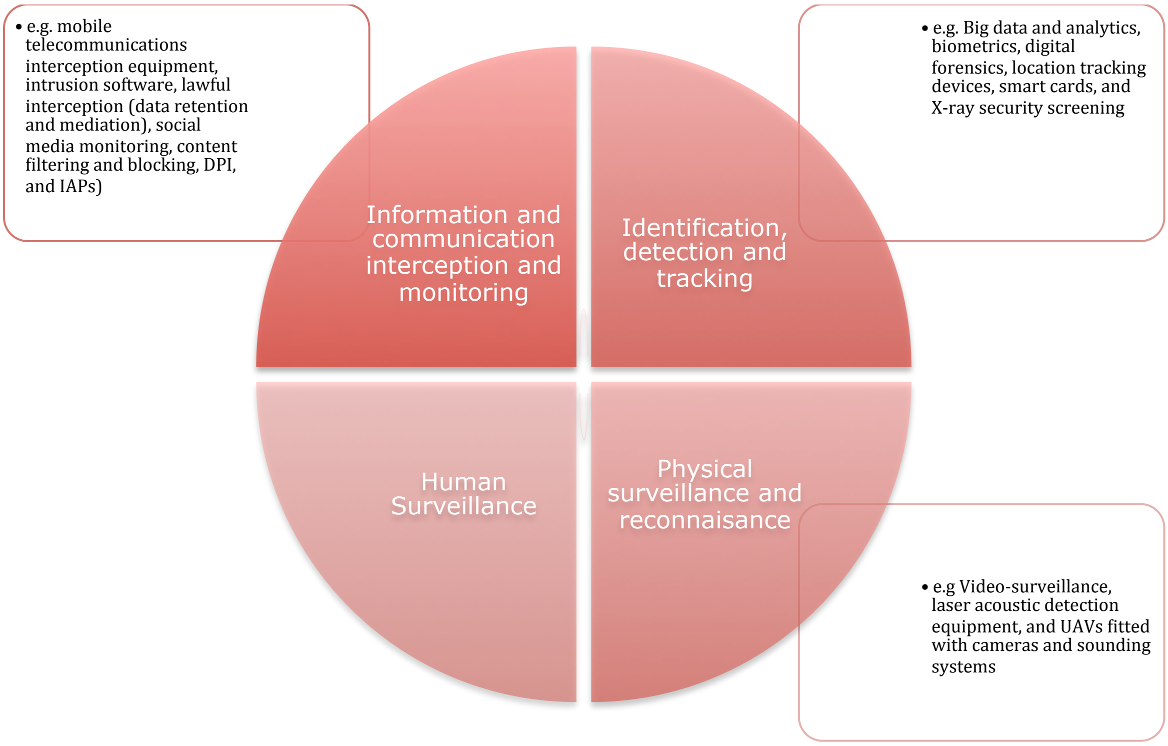
(b) Identification, detection and tracking (e.g. big data and analytics, biometrics, digital forensics, location tracking devices, smart cards, and X-ray security screening); and

(c) Physical surveillance and reconnaissance (e.g. video-surveillance, laser acoustic detection equipment, and UAVs fitted with cameras and sounding systems).

All of the goods, services and technologies covered by segment (a) and some of those covered by segment (b) could be classed as cyber-surveillance technologies. However, all of the goods, services and technologies covered by segment (c) lie beyond its scope since they are outside the remit of the ICT sector.

[90] Rowena Rodrigues, 'The Surveillance Industry in Europe', in *Surveillance, Fighting Crime and Violence*, (IRISS, 2012), p. 72.

Figure 7.1. The Surveillance Sector


• e.g. mobile telecommunications interception equipment, intrusion software, lawful interception (data retention and mediation), social media monitoring, content filtering and blocking, DPI, and IAPs)
• e.g. Big data and analytics, biometrics, digital forensics, location tracking devices, smart cards, and X-ray security screening
Information and communication interception and monitoring
Identification, detection and tracking
Human Surveillance
Physical surveillance and reconnaisance
• e.g Video-surveillance, laser acoustic detection equipment, and UAVs fitted with cameras and sounding systems

Surveillance sector: Data

Generating data on the size of the global and European surveillance sector has proven challenging since it is a highly fragmented patchwork of heterogeneous goods, services and technologies. Previous attempts to produce estimates are incomplete and only cover fractions of this sector. For instance, an FP7-funded research project, IRISS (Increasing resilience in surveillance societies), which discussed the surveillance industry, focused specifically on key surveillance areas and markets such as biometrics, deep packet inspection, smart cards, RFID, smart homes, unmanned areal systems, x-ray security screening and video surveillance.[91] It presented estimates provided by market research companies, but did not aggregate the figures to provide an overall estimate of the sector. Nevertheless, the study was able to conclude that the global surveillance market is developing at a rapid pace.

Surveillance sector: Export controls

Prior to the expansion of export controls at the Wassenaar Arrangement and EU levels that began in 2011, a range of different cyber and non-cyber surveillance technologies were subject to export control, via both the dual-use and military control lists. For example, DU Category 6A005g covers ‘Laser acoustic detection equipment’. DU Category 9A012 covers ‘Unmanned aerial vehicles (UAVs), associated systems, equipment and components’. Provided they meet the minimum capabilities set by the control list, this would include UAVs fitted with cameras or sounding systems.

[91] Rowena Rodrigez., ‘The Surveillance Industry in Europe’, Trilateral Research and Consulting LLP, Surveillance, fighting crime and violence, IRISS Project report, delivrable D1.1., 2012, pp.

In addition, several cyber-surveillance technologies are controlled by category 5A002 on 'cryptography' in the EU dual-use control list. These included certain types of intrusion software and Lawful Interception systems (see below). In addition, a number of cyber-surveillance systems were controlled via ML11 of the EU military list, which covers 'Electronic systems or equipment, designed either for surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purposes'.

Certain EU Member States also maintain national controls on items that are not covered by the EU control list. In certain cases, these additional controls cover surveillance technologies. For example, Hungary maintains national controls on 'equipment for crime surveillance and coercion' and 'secret service devices' via its national controls on arms exports.[92]

In many cases, surveillance technologies that are subject to export are captured by control list categories that also include a wide range of non-surveillance technologies. As a result it is not possible to produce an estimate of the value of dual-use related exports of surveillance technologies from EU Member States.

The cyber-surveillance sector

This study defines cyber-surveillance technologies as ICT goods, services and technologies that are specifically designed, in whole or in part, for surveillance purposes. This includes, but is not limited to, the following:

- Mobile telecommunications interception equipment;
- Intrusion software;
- Monitoring centres;
- Lawful Interception systems and data retention systems;
- Biometrics;
- Digital forensics;
- Location tracking devices;
- Probes; and
- Deep Packet Inspection (DPI) systems.

This definition includes several technologies that are used in both cyber-surveillance systems and non-surveillance systems, such as probes and Deep Packet Inspection (DPI) systems. Probes are used to collect data as it passes through a communications

[92] Hungary Trade Licensing Office, 'Report on Arms Export Controls of the Republic of Hungary, 2009', [N/D], <http://www.sipri.org/research/armaments/transfers/transparency/national_reports/Hungary/HUN_2009.pdf>.

network.[93] DPI systems are used to examine the content of data as it passes through a communications network.[94]

Probes and DPI systems are used in a range of cyber-surveillance systems. In addition, probes and DPI systems are also employed when a state bypasses standardized Lawful Interception processes through the use of a 'tap' or a 'black box' (see 7.5 Lawful Interception Systems and data retention systems). Probes and DPI systems have been mentioned as the possible focus for export control restrictions. Indeed, DPI systems are included in the range of goods, services and technologies covered by the EU embargoes on Syria and Iran.[95]

However, probes and DPI systems are also used in a range of non-surveillance technologies and systems. For example, DPI systems are used to ensure that data is being supplied in the right format or is free of viruses as well as for surveillance or censorship purposes.[96] In many cases, particular probes or DPI systems are marketed for both surveillance and non-surveillance purposes. For example, Hewlett Packard manufactures several types of probes and DPI systems that can be used for both surveillance and non-surveillance purposes.[97]

The definition outlined above excludes Internet content filtering and blocking technologies, which have been linked to certain human rights abuses and mentioned as a possible focus for export control restrictions. However, while these technologies are linked with censorship issues, they does not directly relate to surveillance. In addition, these technologies also have a range of non-censorship uses such as ensuring that harmful websites are not accessed through publicly accessible networks.

The definition also excludes communications networks. These are almost always supplied with some level of surveillance functionality built in and are the subject of export controls. However, it is questionable whether it could be claimed that they are specifically designed, in whole or in part, for surveillance purposes. Although they are not covered by this definition of cyber-surveillance technologies, issues relating to the export of communications networks and how they are covered by dual-use export controls are discussed in 7.5 Lawful Interception systems and data retention systems.

[93] Passive probes collect data indiscriminately as it moves through the communications network. Actives probes collect data from specific individuals using their identifiers (e.g. IP address) or based on specific signatures (e.g. specific semantic content). See 'Catalyst 6500 Series Switches Lawful Intercept Configuration Guide' (CISCO, Aug 2007), <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/lawful/intercept/book.pdf>.

[94] Duncan Geere, 'How Deep Packet Inspection Works', *Wired*, 27 Apr. 2012, <http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works>.

[95] Council Decision 2011/782/CFSP of 1 Dec. 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP, Official Journal of the European Union, 2 Dec. 2012; and Council Decision 2012/168/CFSP of 23 March 2012 amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran, *Official Journal of the European Union*, 24 Mar. 2012, p. 85.

[96] Duncan Geere, 'How Deep Packet Inspection Works', *Wired*, 27 Apr. 2012, <http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works>.

[97] 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

The range of companies involved in the production and export of cyber-surveillance technologies is broad. A number of companies, including a large number of SMEs, are exclusively engaged in the production of one or more cyber-surveillance technologies (so-called 'pure players'). Meanwhile, a number of larger defence companies, such as BAE Systems and SAFRAN, provide a range of different cyber-surveillance goods and services as part of a broader spectrum of cyber and non-cyber surveillance and security solutions. Finally, a large number of ICT companies produce technologies like probes and DPI systems, often for both surveillance and non-surveillance end-uses.

Unlike in other sectors—such as nuclear, chemical or defence—there are no EU or national industry associations that represents all of these companies. Rather, certain companies are members of ICT-focussed associations, such as Digital Europe, or IT-focussed associations, such as BitKom, or defence and security associations, such as ASD, while others are not members of any association.

Companies involved in the cyber-surveillance sector cooperate and market each other's technology, especially in the case of big, complex projects, where different skills and technologies are required. Gamma International (UK/Germany) is reported to have worked with Dreamlab (Switzerland) and Elaman (Germany/Switzerland) in the supply of cyber-surveillance technologies to Turkmenistan.[98] Gamma International (UK/Germany) is also reported to utilize zero-day exploits produced by Vupen (France).[99] One company representative noted that in certain cases the company would compete with another company in order to try and win a contract, while in another case it would cooperate with the same company and submit a joint bid.[100]

There is also a significant level of internationalisation in the industry, with cooperation between EU and non-EU based companies. Moreover, many EU-based companies maintain offices outside the EU while many non-EU based companies maintain offices inside the EU. For example, Hacking Team (Italy) have reportedly sold its intrusion software to LEAs in the United States via the US registered company CICOM.[101] Meanwhile, Verint (USA) maintains offices in several EU Member States.[102]

The sector is also characterized by the provision of training and follow-on support. Many of the companies involved not only supply cyber-surveillance technologies but also training and technical support in relation to the use of the systems.[103] Moreover, certain types of cyber-surveillance technologies require almost constant software updates in order to remain undetected and to function effectively (see 7.3 Intrusion software).

[98] Kenneth Page, 'Six Things We Know from the Latest FinFisher Documents', Privacy International, 15 August 2014, <https://www.privacyinternational.org/?q=node/371>.
[99] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015). p. 31.
[100] Industry representative, Interview with the author.
[101] Eric King, 'Hacking Team Spyware Sold to US DEA, and US Army', 15 April 2015, <https://www.privacyinternational.org/?q=node/559>.
[102] See <http://www.verint.com/about/doing-business-with-verint/verint-offices-worldwide/>.
[103] Kenneth Page, 'Six Things We Know from the Latest FinFisher Documents', Privacy International, 15 August 2014, <https://www.privacyinternational.org/?q=node/371>.

Finally, the sector is also characterized by the presence of a wide-range of specialized brokers and suppliers who are not necessarily engaged in the production of cyber-surveillance technologies. For example, TKSL (Germany) resells cyber-security and surveillance products to police and intelligence services but does not actually produce the systems itself.[104]

Cyber-surveillance sector: Data

The size of the cyber-surveillance industry is not clear. In 2011 it was estimated that the global 'mass surveillance' industry was worth $5 billion a year.[105] However, the basis for the figure is unclear and it has not been updated since. A number of other studies have also been produced aimed at mapping particular goods, services and technologies within the cyber-surveillance industry. For example, the global market for biometrics was estimated to be worth $7.59 billion in 2012.[106] Meanwhile, the global market for DPI was estimated to be worth $470 million in 2011.[107] In addition, in 2014 it was estimated that the global market for Lawful Interception would be worth $1.34 billion by 2019.[108] However, these studies are difficult to compare and combine due to uncertainties and/or differences in the methodologies used.

Finally, a number of estimates exist for the size of the cyber-security industry. For example Visiongain has estimated that the value of the global cyber security market reached $75.4 billion in 2015.[109] However, while the contours of the cyber-security industry encompass many aspects of the cyber-surveillance sector they do not capture all parts of it. In addition, the concept of cyber security also encompasses a range of technologies that are not part of the cyber-surveillance sector including 'security management', 'transaction protection', 'trusted platforms', and 'identity and authentication'.[110]

7.1.2 Focus of this study

This study will focus on ICT goods and technologies that are specifically designed, in whole or in part, for surveillance purposes, and which are currently covered by EU Dual-use controls or are the focus of discussion for later expansion of those controls

[104] Catherine Stupp, 'Germany Leaves Brussels behind on Surveillance Tech Export Controls', EurActiv, 10 July 2015, <http://www.euractiv.com/sections/infosociety/germany-leaves-brussels-behind-surveillance-tech-export-controls-316226>.

[105] Vernon Silver, ' Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms', Bloomberg, 22 Dec. 2011, <http://www.bloomberg.com/news/articles/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms>.

[106] 'The Biometrics Market 2012-2022', (Visiongain, 19 Sep. 2012), <https://www.visiongain.com/report_license.aspx?rid=898>.

[107] Rowena Rodrigues, 'The Surveillance Industry in Europe', in *Surveillance, fighting crime and violence* (IRISS, Feb. 2012), p. 72.

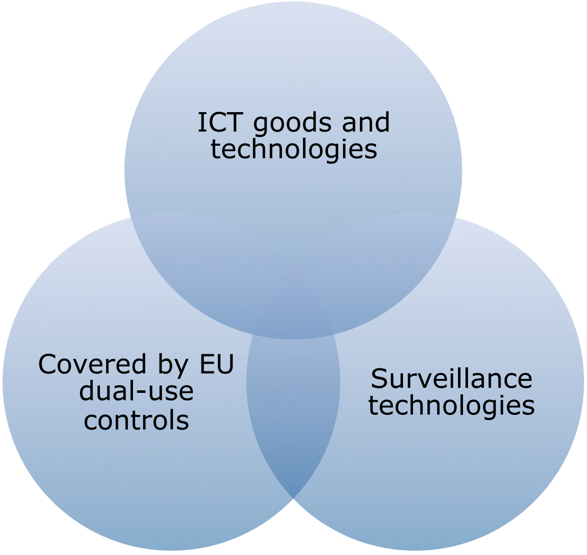
[108] 'Lawful Interception Market worth $1,342.4 Million by 2019', Markets and Markets, [N/D], <http://www.marketsandmarkets.com/PressReleases/lawful-interception.asp>

[109] 'Cyber Security Market 2015-2025: Leading Companies in Network, Data, Endpoint, Application & Cloud Security, Identity Management & Security Operations," *MarketWatch*, 22 June 2015, <http://www.marketwatch.com/story/cyber-security-market-2015-2025-leading-companies-in-network-data-endpoint-application-cloud-security-identity-management-security-operations-2015-06-22>.

[110] 'Assessing Cyber Security Export Risks', (UK Government, 2015).

(See Figure 7.2). In doing so, the report will also focus on technologies that have been of most concern in relation to violations of human rights or that threaten international or EU security.

Figure 7.2. Focus of the study


ICT goods and technologies
Covered by EU dual-use controls
Surveillance technologies

As such, the report will focus upon: (a) mobile telecommunications interception equipment; (b) intrusion software; (c) monitoring centres; (d) Lawful Interception systems and data retention systems; and (e) biometrics.

Each of these technologies vary significantly in a number of areas, including: (a) the extent to which they have non-surveillance applications; (b) whether or not they are currently affected by the EU's dual-use export controls, (c) the range of security and human rights concerns attached to their export and use; (d) how extensively they are used by EU Member State LEAs and intelligence agencies; (e) whether or not there are agreed standards relating to their use; and (f) the number and type of EU and non-EU based companies that are engaged in their production.

All of these differences have implications for the current impact of dual-use controls and the potential impact of the different review options.

As a result, the section adopts a case study approach to focus in more detail on each technology. For each case study, the report provides:

- A description of the item or technology and what it does;
- A description of if and how it is captured by dual-use export controls;

- Examples of human rights concerns linked to its use;[111]
- Examples of security concerns linked to its use;[112]
- Examples of its use and governance of its use in EU Member States;
- Examples of producer companies, both in and outside the EU; and
- An indication of the current/potential export control regulatory burden for both government and industry.

However, the amount of detail contained in each case study varies depending on the level of concern in relation to violations of human rights or international/EU security. For a summary of the case study findings, see Table 7.3

The information presented in these individual case studies is intended to allow for an assessment of the current impact of export controls in the cyber-surveillance sector as well as the potential impact of relevant review options. The conclusions present an overall assessment of the stakeholder perceptions of the impact of current controls in this area and the potential impact of a further expansion in controls as a result of the implementation of relevant review options.

7.2 Mobile telecommunications interception equipment

7.2.1 Description of technology

Mobile telecommunications interception equipment refers to technologies used to track, identify, intercept and record on mobiles phones. One key example of this type of technology is an International Mobile Subscriber Identity (IMSI) Catcher: a device used to identify the subscriber identifier of mobile phones and intercept their traffic 'off the air'.

Working as a fake mobile tower (virtual base transceiver station VBTS), an IMSI Catcher enables so-called 'man in the middle attacks'. Specifically, it logs all the IMSI number of the mobile phones in the nearby area as they attempt to connect to it.[113] More advanced systems are also able to locate targeted devices, intercept calls and text-messages, and block certain services.[114]

[111] This will include documented cases of human rights abuses linked to their use and concerns raised about the human rights implications of their use.
[112] This will include documented cases of threats to international or EU security, and concerns about the security implications of their use.
[113] Danielle Kehl and Robert Morgus, 'The Dictator's Little Helper: How to stop Western companies from exporting surveillance technologies to authoritarian governments', Slate, 31 Mar. 2014, <http://www.slate.com/articles/technology/future_tense/2014/03/export_controls_how_to_stop_western_companies_from_sending_surveillance.html>.
[114] Stephanie K. Pell and Christopher Soghoian, 'Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy', *Harvard Journal of Law & Technology* 28, no. 1 (2014): 1–75.

Table 7.3. Summary of case study findings

	Mobile telecommunications interception equipment	Intrusion software	Monitoring centres	Lawful Interception systems and data retention systems	Biometrics
Covered by Annex 1	Yes	Yes	Partial	Partial	No
Human rights violations	Yes (CR)	Yes (DC)	Yes (DC)	Yes (DC)	Yes (CR)
Security threats	Yes (CR)	Yes (CR)	No	No	No
Use by EU Member States	Yes (NS)	Yes (NS)	Yes (NS)	Yes (SS)	Yes (SS)
Producer companies inside the EU	Yes	Yes	Yes	Yes	Yes
Producer companies outside the EU	Yes	Yes	Yes	Yes	Yes
Regulatory burden (government)	Mixed	Limited	Limited	Mixed	No
Regulatory burden (industry)	Mixed	Mixed	Mixed	Mixed	No

CR = Concerns raised; DC = Documented cases; NS = No agreed standards on use at EU level; and SS = Some agreed standards on use at EU level.

7.2.2 How it is captured by dual-use export controls

Prior to 2012 exports of IMSI Catchers were controlled by certain states on the grounds that they were covered by categories 5A001, 'Telecommunications systems, equipment, components' and/or 5D002, 'Software' in the EU dual-use control list. In 2009, for example, the UK denied an export licence application worth £0.8 million submitted by Datong for the export of IMSI Catchers covered by 5A001 and 5D002 to a country in the Asia Pacific region, believed to be Bangladesh.[115] The licence was denied because of the risk that the goods would be used to commit human rights abuses.

[115] Ryan Gallagher and Rajeev Syal, 'Met Police Using Surveillance System to Monitor Mobile Phones,' *The Guardian*, 30 Oct. 2011, <http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance>; and 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

In 2012 the language in the Wassenaar Arrangement dual-use control list was modified to explicitly cover IMSI Catchers. These updates were implemented at the EU level in December 2014 via 5A001f 'Mobile telecommunications interception or jamming equipment, and monitoring equipment therefor'.

7.2.3 Human rights concerns

The study was unable to find any documented cases of IMSI Catchers supplied by companies based in EU Member States being connected to violations of human rights. However, the use of IMSI Catchers raises concerns regarding potential violations of the following:

- right to privacy;
- freedom of expression;
- freedom of association; and
- freedom from arbitrary arrest and detention.

For example, in France, the French data protection agency (La Commission Nationale de l'Informatique et des Libertés (CNIL)) has warned that the use of IMSI Catchers by LEAs could lead to violations of the right to privacy.[116] In the United States some organisations have argued that use of IMSI Catchers by LEAs could constitute a violation of the fourth amendment to the US Constitution, which outlaws 'unreasonable searches and seizures'.[117]

A number of security services accused of human rights abuses have purchased, or have sought to purchase, IMSI catchers. In 2014 a Bangladeshi security agency that had been criticized in the past for multiple human rights abuses was reported to be seeking to acquire IMSI Catchers.[118]

[116] Pierre Alonso and Amaelle Guiton, 'Imsi-Catchers, Des Valises Aux Grandes Oreilles', 15 Apr. 2015.
[117] Hanni Fakhoury, 'Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About', *Electronic Frontier Foundation*, 22 Oct. 2012, <https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy>; and Valentino Valentino-Devries, 'How Technology Is Testing the Fourth Amendment', *Wall Street Journal*, 21 Sep. 2011, <http://blogs.wsj.com/digits/2011/09/21/how-technology-is-testing-the-fourth-amendment/>.
[118] Edin Omanovic, 'Bangladesh's Brutal Security Service Meets with Swiss Surveillance Company Neosoft', 4 Sep. 2014, <https://www.privacyinternational.org/?q=node/433>.

7.2.4 Security concerns

The study was unable to find any documented cases of IMSI Catchers supplied by companies based in EU Member States being used in ways that pose a threat to EU or EU Member State security. However, in the United States IMSI Catchers have reportedly been used in:

- theft of government secrets; and
- theft of commercial secrets.[119]

Police in the Czech Republic have detected the unauthorized use of IMSI Catchers, although they have not been able to identify who is using them and for what purpose.[120]

7.2.5 Use and governance in EU Member States

IMSI Catchers are widely used by LEAs and intelligence agencies in EU Member States. The Metropolitan Police in the UK reportedly use IMSI Catchers produced by the UK-based company Datong, which is now part of the Seven Technologies Group.[121] However, the Metropolitan Police has neither confirmed nor denied their use.[122] LEAs in the Czech Republic and Germany are also reported to use IMSI Catchers.[123]

There is limited information on how the use of IMSI Catchers is regulated in EU Member States or the number of times they are used. In France, legislation adopted in 2015 allows intelligence agencies to use IMSI Catchers without a warrant in terrorism-related investigations.[124] In Germany, the use of IMSI catchers is regulated by law and is subject to conditions including a proportionality test. [125] In addition, the intelligence

[119] Jeff Stein, 'New Eavesdropping Equipment Sucks All Data Off Your Phone', *Newsweek*, 22 June 2014, <http://www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html>.

[120] Ryan Gallagher, 'Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion', *Slate*, 22 Aug. 2012, <http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications_.html>.

[121] Sam O'Neill, 'Police Sweep up Phone Data with Secret Snooping Device', *The Times (London)*, 1 Nov. 2014, <http://www.thetimes.co.uk/tto/news/uk/crime/article4254706.ece>.

[122] Eric King and Matthew Rice, 'Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist', (Privacy International, 5 Nov. 2014), <https://www.privacyinternational.org/?q=node/454>.

[123] Ryan Gallagher, 'Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion', *Slate*, 22 Aug. 2012, <http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications_.html>.

[124] Martin Untersinger, 'Que sont les IMSI Catchers, ces valises qui espionnent les téléphones portables, *Le Monde,* 10 April 2015; Martin Untersinger, 'L'Assemblée vote définitivement la loi sur le renseignement', *Le Monde,* 26 June 2015; Loi n°2015-912, du 24 juillet 2015 relative au renseignement', JORF n°0171, du 26 juillet 2015,page 12735, texte 2

[125] Eric King and Matthew Rice, 'Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist', (Privacy International, 5 Nov. 2014), <https://www.privacyinternational.org/?q=node/454>.

agencies are required to provide information to a Parliamentary Control Panel on their use of IMSI Catchers every six months.[126]

7.2.6 Producer companies in the EU

A number of companies based in the EU produce IMSI Catchers (See Table 7.4). There is very little public information available about revenues, profit and employment for many of these companies. The information that is available indicates that most of these companies are 'pure players' that specialize in the production of a range of surveillance technologies for LEAs and intelligence agencies.

Table 7.4. EU-based producers of mobile telecommunications interception equipment

Company	Location	Revenue	Profit	Employment
		(2013)	(2013)	(2013)
Aappro	UK	-	-	-
Amesys	France	-	-	-
Cobham PLC	UK	£1 790 m.	-	10 090
Ercom	France	-	-	≈100
Gamma International	Germany / UK	-	<€1 m.	-
GTS Services	France	-	-	-
Nethawk Ojy[a]	Finland	€29 m.	-	370
PKI Electronic	Germany	-	-	-
Rhodes and Schwartz	Germany	€1 750 m.	-	9 800
Seven Tech. Group	UK	-	-	≈100
SSI Group	France	€3 m.	-	4
Syans	France	-	-	-

a. 2009 data

[126] Eric King and Matthew Rice, 'Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist', (Privacy International, 5 Nov. 2014), <https://www.privacyinternational.org/?q=node/454>.

7.2.7 Producer companies outside the EU

A number of companies based outside the EU produce mobile telecommunications interception equipment such as IMSI Catchers. These include: Ability (Israel); Harris Corporation (USA); Neosoft (Switzerland); Nice Systems (Israel / USA); Proximus (Ukraine); Safetech (Brazil); Septier (India); and Verint (USA). A number of these companies maintain offices in the EU.[127]

In recent years there has been a significant expansion in the number of companies that are able to produce mobile telecommunications interception equipment. Devices that in the past would have cost over $100,000 and could only be produced in a small number of states are now available for a few thousand dollars and are produced much more widely.[128] A recent paper argued that a hobbyist would be able to produce the most basic type of IMSI Catcher for only $100.[129] However, such a system would not have the same capabilities as the more advanced IMSI Catchers, which are able to locate targeted devices, intercept calls and text-messages, and block certain services.

7.2.8 Current / potential regulatory burden (Government)

Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, six reported that mobile telecommunications interception equipment was exported from their state. Of the ten EU Member States, three issued a total of 60 export licences for goods covered by category 5A001f with a total value of €25.1 million and denied 1 licence with no value attached. In 2015, three EU Member States issued a total of 27 export licences for goods covered by category 5A001f with a total value of €16.8 million and denied 2 licences with a total value of €0.7 million.[130]

None of these EU Member States reported issuing global licences for the export of mobile telecommunications interception equipment, implying that all EU Member States control these exports through individual licences. The licence denials appear to have been issued due to concerns relating to Criterion 2: Respect for Human Rights and Criterion 3: Internal Situation.

7.2.9 Current / potential regulatory burden (Industry)

There are no clear indications of EU-based companies that manufacture IMSI Catchers seeking to relocate since the 2012 Wassenaar control list modifications. However, in Switzerland, companies have reportedly withdrawn licence applications for the export of IMSI Catchers and other surveillance equipment in response to the negative

[127] See 'About', Verint, [N/D] <http://www.verint.com/about/doing-business-with-verint/verint-offices-worldwide/>.

[128] Stephanie K. Pell and Christopher Soghoian, 'Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy', *Harvard Journal of Law & Technology* 28, no. 1 (2014): 1–75, p.5.

[129] Stephanie K. Pell and Christopher Soghoian, 'Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy', *Harvard Journal of Law & Technology* 28, no. 1 (2014): 1–75, p.5.

[130] Figures for 2015 are as of June 2015.

publicity generated by reports of their connection with human rights abuses.[131] There are also reports that companies are planning to move production and leave Switzerland as a result of the imposition of export controls.[132]

7.3 Intrusion Software

7.3.1 Description of technology

Intrusion software is a type of malware that can both penetrate and take over ICT devices such as computers and mobile phones without detection. This allows content and traffic to be remotely and covertly monitored, extracted and modified and for the activation of microphones and cameras. Intrusion software can be installed using a range of different methods, including phishing emails and fake websites.[133] A range of different types of intrusion software exists, from commercially available systems that are marketed to private end-users (such as MobileSpy, mSpy and StealthGenie) to more sophisticated systems that are marketed exclusively to LEAs and intelligence agencies (IAs).[134]

In order to operate effectively, infusion software needs to be inserted and then operated without the user of the target device being aware of its presence. As a result, the system needs to be able to bypass any anti-virus systems installed on the device. Since these anti-virus systems are constantly updated, the supplier must also constantly update the intrusion software in order to avoid detection.[135]

Although the differences are hazy, intrusion software can be seen as distinct from 'offensive' forms of malware that are designed to disrupt or damage ICT devices or networks or the information they contain. Offensive malware vary significantly in terms of their complexity. Unsophisticated types are readily available either through legal or illegal channels. More sophisticated systems—such as Stuxnet virus which was used to disrupt the Iranian nuclear programme—are highly complex and far more difficult to develop and acquire.[136] It is widely assumed that only states have the

[131] Kenneth Page, 'Swiss Government Forced to Reveal Destinations, Costs of Surveillance Exports', Privacy International, 14 Jan. 2015, <https://www.privacyinternational.org/?q=node/98>.

[132] Henry Habegger, 'Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]', *Schweiz Am Sonntag*, 1 Aug. 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[133] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015).

[134] 'Mobile Spyware Maker mSpy Hacked, Customer Data Leaked', *Krebs on Security*, 15 May 2015, <http://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/>.

[135] UK Department for Business Innovation & Skills, UK National Contact Point for the OECD Guidelines for Multinational Enterprises Privacy International & Gamma International UK Ltd: Final Statement After Examination of Complaint', December 2014), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf>.

[136] Bruce Schneier, 'The Story Behind The Stuxnet Virus', *Forbes*, 10 July 2010, <http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html>.

financial and technical resources to design offensive malware as complex as the Stuxnet virus.

Both intrusion software and offensive malware are often reliant upon 'zero-day' software vulnerabilities and exploits in order to gain access to the device or network that they wish to monitor or disrupt. Definitions vary, but zero-day software vulnerabilities are generally understood to be flaws in a programme that are unknown to the software vendor or users, while zero-day software exploits are programmes that take advantage of those flaws.[137]

For example, reports indicate that Hacking Team (Italy) have used a number of zero-day software exploits to insert their intrusion software on to target devise.[138] However, in many cases Hacking Team's intrusion software is inserted without the use of zero-day software exploits but via social engineering techniques that trick the target into downloading the software onto their device.[139]

7.3.2 How it is captured by dual-use export controls

Prior to 2012 certain EU Member States controlled exports of some types of intrusion software on the grounds that they were covered by category 5A002 on 'cryptography' in the EU's dual-use control list. For example, in 2012 the UK Government began to control exports of intrusion software produced by Gamma International (Germany/UK) because of the level of cryptography the system used for remotely controlling and extracting information from the targeted device.[140] Gamma International also produced a version of the software with a lower level of encryption that was not subject to control.[141]

In 2013 new categories were added to the Wassenaar Arrangement dual-use control list to cover certain types of intrusion software, on the grounds that they 'may be detrimental to international and regional security and stability'.[142] The language was proposed by the UK Government and was aimed at addressing the human rights and national security concerns associated with their use.[143] These updates were

[137] For more information, see Mailyn Fidler, 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis', I/S: *A Journal of Law and Policy for the Information Society*, Forthcoming.
[138] Kim Zetter, 'Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work,' *Wired*, 24 July 2015, <http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/>.
[139] Alastair Stevenson, 'The CEO of Hacking Team Tells How His Surveillance Company Is Recovering from the Hack That Stole All Its Data', *Business Insider*, 24 July 2015, <http://uk.businessinsider.com/interview-with-hacking-team-ceo-david-vincenzetti-2015-7>.
[140] 'British government admits it has already started controlling exports of Gamma International's FinSpy', Privacy International, 9 Sep. 2012, <https://www.privacyinternational.org/news/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma>.
[141] UK Department of Business, Innovation and Skills official, Interview with the author, 28 April 2015.
[142] Wassenaar Arrangement, 'Public Statement 2013. Plenary meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies', 4 Dec. 2013, <http://www.wassenaar.org/publicdocuments/index_PS_PS.html/>.
[143] UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.

implemented at the EU level in December 2014 via categories 4A005, 4D004, 4E001a, and 4E001.c.

The controls do not cover intrusion software per se, but are focused on technology specially designed or modified for the generation, operation or delivery of, or communication with, 'intrusion software'.[144] This was to avoid people becoming unwittingly subject to controls if they left the country with a computer that was infected with intrusion software without their knowledge and to try and ensure that the controls did not apply to companies or individuals working in IT security.[145]

The controls are not designed to control offensive malware systems. Moreover, under the Wassenaar Arrangement's General Software Note (GSN), commercially available intrusion software systems that are marketed to private end-users are not covered by the controls.[146] However, in many states the sale of commercially available intrusion software is regulated under other laws and regulations.

The UK Government has stated that it understands the controls on intrusion software as covering '(c)omplex surveillance tools which enable unauthorized access to computer systems'.[147] Nonetheless, there are concerns that goods, services and research activities in the field of IT security may also be covered (see below). There are also concerns that controls on intrusion software may need to be updated to keep pace with the evolving nature of the technology in this area. For example, the Pegasus system produced by the Israeli company NSO Group is reportedly able to remotely extract information from computers and mobile phones without using the types of software described in the EU dual-use control list.[148]

7.3.3 Human rights concerns

Intrusion software exported from EU Member States has been connected to violations of human rights in at least 9 countries.[149] The human rights abuses committed include violations of:

[144] UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.
[145] UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.
[146] See Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.
[147] 'Assessing Cyber Security Export Risks', (UK Government, 2015).
[148] Barbara Opall-Rome, 'Israeli Smartphone Targeting System Cleared for Export', *Defense News*, Aug. 2013; and Edin Omanovic, Privacy Internationa, Interview with the author, 27 April 2015. Nonetheless, the system does appear to be subject to Israeli export controls.
[149] 'Mapping Hacking Team's 'Untraceable' Spyware', (Citizen Lab, 17 Feb. 2014), <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>; Morgan Marquis-Boire et al., 'You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab', *The Citizen Lab*, accessed 31 May 2015, <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>; and 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia', (Human Rights Watch, March 2014), <http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf>.

- right to privacy;
- freedom of expression;
- freedom of association;
- right to life;
- freedom from arbitrary arrest and detention; and
- freedom from torture inhuman treatment and degrading treatment.

In the majority of cases, two companies supplied the systems involved: Gamma International and Hacking Team. However, most of the allegations are based upon evidence that LEAs or intelligence agencies in states with a poor human rights record are using the systems, rather than any explicit connection between the systems themselves and specific human rights abuses.

Concrete examples mainly relate to violations of the right to privacy and freedom of expression. For example, Citizen Lab have demonstrated how Hacking Team intrusion software was used by the Morocco authorities to monitor the communications of journalists from a citizen media project, and by the UAE authorities to monitor the communications of a human rights activist.[150]

Sarah A. McKune of Citizen Lab noted that the use of spyware against individuals by states that lack effective rule of law amounts to a violation of the right to privacy and, possibly, freedom of expression.[151] However, establishing clear links between the use of such technology and serious, potentially life-threatening abuses of human rights is often hard to achieve. In general, the issue is 'under-researched and not well documented'.[152] Citizen Lab has a number of projects aimed at establishing clearer links between the use of cyber-surveillance technologies and abuses of human rights.[153]

Intrusion software exported from EU Member States been also used by LEAs or intelligence agencies in third countries to monitor the communications of human rights activists based in the EU.[154] For example, in 2014 it was reported that the Bahrain

[150] 'Mapping Hacking Team's 'Untraceable' Spyware', (Citizen Lab, 17 Feb. 2014), <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>.
[151] Sarah A. McKune, Senior Legal Advisor, Citizen Lab, Munk School of Global Affairs, University of Toronto, Interview with the author, 2 July 2015.
[152] Sarah A. McKune, Citizen Lab, Interview with the author, 2 July 2015.
[153] As part of this work, Citizen Lab has been focusing upon the psychological impact of being made the target of cyber-surveillance technologies. Sarah A. McKune, 'Human Rights and Technologies: The Impact of Digital Surveillance and Intrusion Systems on Human Rights in Third Countries" (European Parliament Hearing, 21 Jan. 2015).
[154] Ben Knight, 'FinFisher Spyware Preliminary Investigation Started in Germany', *Deutche Welle*, 20 Feb. 2015, <http://www.dw.de/finfisher-spyware-preliminary-investigation-started-in-germany/a-18270876>; and 'Assessing Cyber Security Export Risks', (UK Government, 2015).

security forces had used Gamma International intrusion software to spy on a number of Bahrain lawyers, activists and politicians, including several based in the UK.[155]

7.3.4 Security concerns

The study was unable to find any documented cases of intrusion software supplied by companies based in EU Member States being used in ways that pose a threat to EU or EU Member State security. In one possible case the Oman security forces are reported to have used intrusion software supplied by Gamma International (Germany/UK) to spy on the British oil company Shell.[156]

There are a range of scenarios in which intrusion software could be used to threaten international or EU security. These include:

- disruption of critical infrastructure;
- theft of military or WMD-related knowledge or technologies;
- theft of government secrets; and
- theft of commercial secrets.

In March 2013, the Director of US National Intelligence James Clapper highlighted the security threats, including the theft of government and commercial secrets, posed by commercially available intrusion software.[157] Offensive malware systems pose a significant array of potential threats to EU or EU Member State security but – as noted – these are not the intended target of the controls on intrusion software.

7.3.5 Use and governance in EU Member States

Different types of intrusion software are widely used by EU Member State LEAs and defence and intelligence agencies, and the market for these types of systems within the EU appears to be expanding.[158] In 2013, it was reported that the German Federal Criminal Police Office had acquired intrusion software produced by Gamma International (Germany/UK).[159] In 2014 it was reported that the Netherlands, Hungary and Italy were using intrusion software produced by Gamma International

[155] Fahad Desmukh, ‘Bahrain Government Hacked Lawyers and Activists with UK Spyware’, *Bahrain Watch*, 7 Aug. 2014, <https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/>.

[156] Alastair Sloan, ’Spy-tech firms Gamma and Trovicor target Shell Oil in Oman’, The Register, 20 May 2015, <http://www.theregister.co.uk/2015/05/20/omani_intel_docs/>.

[157] James R. Clapper, Director of National Intelligence, ‘Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence’ (US Government, 23 Mar. 2013).

[158] ‘The Little Black Book of Electronic Surveillance: 2015’, (Insider Surveillance, Feb. 2015).

[159] Andre Meister, ‘Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware’, *Netzpolitik.org*, 16 Jan 2013, <https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/>.

(Germany/UK).[160] In 2015, it was reported that different LEAs in a number of EU Member States—including Italy, Spain, Cyprus, Poland, the Czech Republic and Hungary—were using intrusion software produced by Hacking Team (Italy).[161]

Some government and industry experts argue that LEAs and intelligence agencies are unable to rely upon traditional Lawful Interception processes in order to access the communications of target individuals. In particular, this is due to: (a) the rapid expansion in the range of communication protocols; (b) the growing use of 'over-the-top' messaging services; (c) the growing use of 'end-to-end' encryption; (d) the growing use of the 'dark net' or 'dark web'; and (e) the provision of communication services by companies based outside the territory of the LEA or intelligence agency.[162] As a result, government agencies are becoming increasingly reliant on different types of 'device level' compromise, such as intrusion software.[163] However, others argue that intrusion software is not necessary and that traditional methods of Lawful Interception are sufficient to meet the needs of LEAs or intelligence agencies.[164]

There is a lack of agreed international and regional standards regarding if, when and how intrusion software should be used by LEAs and intelligence agencies, and the mechanisms through which the process should be governed. For example, the use of such systems is not covered by the various technical standards on Lawful Interception (See 7.5 Lawful Interception management systems and data retention systems). A number of EU Member States are drafting laws that cover these issue but the standards laid down vary significantly. There is also a lack of information on the number of times LEAs and intelligence agencies in EU Member States use intrusion software. One exception is the Netherlands, where the Intelligence Oversight Committee publishes information on the government's use of a range of surveillance technologies, including intrusion software.[165]

7.3.6 Producer companies in the EU

A number of companies based in the EU produce intrusion software for LEAs and intelligence agencies (see Table 7.5).[166] There are also a number of companies, such as Vupen (France), that are focused specifically on the development of zero-day

[160] Chris Duckett, 'WikiLeaks Names NSW Police as FinFisher Malware Customer', *ZDNet*, 15 Sep. 2014, <http://www.zdnet.com/article/wikileaks-names-nsw-police-as-finfisher-malware-customer/>.

[161] Alastair Sloan, 'Spy-Tech Firms Gamma and Trovicor Target Shell Oil in Oman', 20 May 2015, <http://www.theregister.co.uk/2015/05/20/omani_intel_docs/>.

[162] See Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, 'Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology', 9 Apr. 2015.

[163] David Anderson Q.C., 'A Question of Trust: Report of the Investigatory Powers Review'. (note 13).

[164] Carly Nyst, Privacy International, Interview with the author, 27 April 2015.

[165] Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), <http://www.ctivd.nl/over-ctivd/inhoud/taken-en-bevoegdheden>.

[166] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015); and Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

software exploits which can be used to insert its intrusion software on the target devise (see above).

There is very little public information available about many of these companies. The information that is available indicates that most of these companies are 'pure players' that specialize in the production of a range of surveillance technologies for LEAs. In addition, with the exception of Chemring Technology Solutions, they are mostly SMEs.[167]

There is limited information on the value of the global or European market for intrusion software. Hacking Team (Italy) has stated that its products cost 'hundreds of thousands' of US dollars and are customized for each client.[168]

Table 7.5 EU-based manufacturers of intrusion software

Company	Location	Revenue (2013)	Profit (2013)	Employment (2013)
Chemring Tech. Solutions	UK	£472 m.	£57 m.	>3500
Elaman	Germany/ Switzerland	-	<€1 m.	-
Gamma International	Germany/UK	-	<€1 m.	-
GR Sistemi	Italy	-	-	-
Hacking Team	Italy	€9 m.	€2 m.	<50
iPS	Italy	$24 m	-	69
RCS Lab	Italy	-	-	-

7.3.7 Producer companies outside the EU

A number of companies based outside the EU produce and/or export intrusion software.[169] These include: AGLAYA (India); Clear-Trail Technologies (India); Harris

[167] Chemring Technology Solutions' work in the field of surveillance technologies forms only one part of its work in sensors and electronics, which accounted for 45 per cent of its revenues in 2013. See <http://www.chemring.co.uk/~/media/Files/C/Chemring-V2/PDFs/introduction-to-chemring-for-customers-oct2014.pdf>.

[168] 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia', (Human Rights Watch, Mar. 2014), <http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf>.

Corporation (USA); NICE Systems (Israel/USA); NSO Group (Israel); Oxygen Software (Russia); SS8 (USA); and Stratign FZCO (UAE).

The development and testing of intrusion software is a complex process that involves large teams of people. Nonetheless, the production and use of intrusion software appears to be a growing area of activity with a number of new providers emerging in recent years in Asia and the Middle East.[170] A number of larger states, including the United States, are reported to produce their own intrusion software, without the assistance of commercial vendors.[171]

7.3.8 Current / potential regulatory burden (Government)

Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, one reported that items covered by the controls on intrusion software were exported from their country. The same state reported that it had issued one export licence for intrusion software in 2015. EU Member States also noted that it was too early to assess the impact of these controls, since they were only adopted at the EU level in December 2014.[172]

Some EU Member States have engaged in efforts to make industry aware of their responsibilities under the new controls and, in particular, to address concerns raised by companies working in the field of IT security. The UK has responded to questions from IT researchers regarding whether their activities are subject to control.[173] The UK has also published a guidance note on how the controls on 'intrusion software' will be implemented and other Member States have stated that they intend to do the same.[174]

7.3.9 Current / potential regulatory burden (Industry)

Companies based in the EU that produce intrusion software maintain different standards in relation to their internal compliance programme (ICP) and have responded in different ways to the expansion of export controls in this area.

Since 2013, Hacking Team (Italy) have taken steps to develop and implement an ICP based around 'know your customer' principles and the inclusion of contract language specifying how its products will be used.[175] In certain cases, Hacking Team (Italy) has halted software updates—which effectively prevent the customer from using the

[169] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>; and 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015).

[170] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015).

[171] 'Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397' (UN General Assembly, 23 Sep. 2014).

[172] Kees-Jan Steenhoek, Acting head of the export control department, The Netherlands Ministry of Foreign Affairs, Interview with the author, 17 April 2015.

[173] Thetekwizz, 'Final Year Dissertation Paper Release: An Evaluation of the Effectiveness of EMET 5.1', *tekwizz123's Blog*, 1 July 2015, <http://tekwizz123.blogspot.com.au/2015/07/final-year-dissertation-paper-release.html>.

[174] UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.

[175] 'Customer Policy', Hacking Team, 2013, <http://hackingteam.it/index.php/customer-policy>.

product—when these standards were not being applied.[176] Hacking Team also monitors NGO and press reports about the alleged misuse of its products.[177]

After the introduction of the new controls on intrusion software Hacking Team stated that it was in full compliance and would be applying for export licences from the Italian authorities.[178] Hacking Team (Italy) also suspended certain aspects of its ICP, including a process whereby a review board vets potential customers, on the grounds that the introduction of the new controls made them unnecessary.[179] Hacking Team (Italy) acknowledges that its ICP and the new controls on intrusion software bring associated costs.[180] However, the company notes that there are legitimate concerns associated with the use of its products that need to be addressed.[181] In addition, certain customers, particularly those in Western Europe, will be more likely to purchase their products if the company acts in a responsible manner.[182]

Gamma International (Germany/UK) has been less public about the standards it applies when assessing potential customers and less willing to engage with and respond to criticisms of their business practices. In 2014 the UK National Contact Point (NCP) for the OECD Guidelines on Multilateral Enterprises found that Gamma International's business practices were inconsistent with certain aspects of the Guidelines.[183] During the investigation, Gamma International (Germany/UK) informed the UK NCP about the 'development of a code of conduct relevant to human rights obligations under the Guidelines'.[184] However, information about this policy is not publicly available.

In April 2012 Gamma International (Germany/UK) halted exports of Finfisher intrusion software from the UK.[185] In 2014, Gamma International (Germany/UK) transferred the FinFisher intrusion software part of its business to Germany and Switzerland. Reports indicate that the UK's attempts to control exports of intrusion software may have played a role in this decision.[186] Gamma International (Germany/UK) is a subsidiary of

[176] 'Response from Hacking Team Re: Update on Sale and Use of Hacking Team Solutions in Ethiopia', *Human Rights Watch*, 7 Mar. 2015, <https://www.hrw.org/news/2015/03/07/response-hacking-team-re-update-sale-and-use-hacking-team-solutions-ethiopia>.
[177] 'Customer Policy', Hacking Team, 2013, <http://hackingteam.it/index.php/customer-policy>.
[178] 'HackingTeam Complies With Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/Intelligence Gathering Tools', *Hacking Team*, 25 Feb. 2015, <http://www.hackingteam.it/index.php/about-us>.
[179] Representative, Hacking Team, Interview with the author, 24 June 2015.
[180] Ibid.
[181] Ibid.
[182] Ibid.
[183] UK Department for Business Innovation & Skills, UK National Contact Point for the OECD Guildelines for Multinational Enterprises Privacy International & Gamma International UK Ltd: Final Statement After Examination of Complaint', December 2014), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf>.
[184] Ibid.
[185] Ibid.
[186] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb. 2015), p. 29.

Gamma Group. Gamma Group maintains technical and sales offices in a number of non-Wassenaar Arrangement states, including Lebanon, Singapore and the UAE.[187] There is a possibility that Gamma Group has moved its work on FinFisher intrusion software to these offices.[188]

The amount of regulatory burden created for companies through the implementation of controls on intrusion software will depend on how the controls are implemented at the national level. This includes whether the controls are applied through the use of individual, global or general licences, how the licences are assessed, and what additional restrictions companies are required to implement via any EUCs or contracts associated with the export. Italy is reported to be controlling exports of intrusion Hacking Team (Italy) software through the use of general licences.[189] Germany has reportedly required Gamma International (Germany/UK) to include language in any EUCs connected to exports of FinFisher intrusion software stating that the products will not be used to infect any device located in, or associated with, Germany.[190]

There have been concerns raised that the controls on intrusion software might have impacts in the field of IT security, particularly on the work of companies providing software and training on 'penetration testing', the work of academics and researchers active in the field of IT security, and the processes by which individuals or organisations make ICT companies aware of software vulnerabilities and exploits.

A number of articles have argued that the controls on intrusion software, if properly applied, should not have a negative impact on IT.[191] However, concerns persist and were reignited in May 2015 when the US Bureau of Industry and Security (BIS) published language on its proposed implementation of the 2013 Wassenaar Arrangement control list additions.[192] The proposed language included a number of

[187] Edin Omanovic, 'Surveillance Companies Ditch Switzerland, but Further Action Needed', 5 Mar. 2014, <https://www.privacyinternational.org/?q=node/377>.

[188] Ibid.; and Henry Habegger, 'Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]', *Schweiz Am Sonntag*, 1 Aug. 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[189] Cora Currier and Morgan Marquis-Boire, 'A Detailed Look at Hacking Team's Emails About Its Repressive Clients', *The Intercept*, 7 July 2015, <http://firstlook.org/theintercept/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/>.

[190] Kenneth Page, 'Six Things We Know from the Latest FinFisher Documents', Privacy International, 15 August 2014, <https://www.privacyinternational.org/?q=node/371>.

[191] See Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[192] Joe Uchill, 'Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses', *Christian Science Monitor*, 26 June 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses>; and Dennis Fisher, 'Coalition of Security Companies Forms to Oppose Wassenaar Rules', *Threat Post*, n.d., <https://threatpost.com/coalition-of-security-companies-forms-to-oppose-wassenaar-rules/113794>.

phrases that alarmed academics and individuals working in IT security.[193] In particular the proposed language:

- Indicated that penetration testing software and vulnerability disclosures would be covered by the controls;
- Indicated that a policy of 'presumptive denial' would apply to exports of these items;
- Indicated that exceptions under the "General Software" and "General Technology" notes would not apply to the controls; and
- Indicated that US controls on 'deemed exports' would apply to the controls.

Academics and researchers working in the field of IT security are engaged in teaching and researching issues on how to build secure IT systems. This involves understanding how to develop and use vulnerabilities and exploits. The EU has supported two networks of academics and researchers working on IT security: the Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS) and SysSec.[194] SysSec has 85 associate members worldwide.[195]

The process by which individuals or organizations make ICT companies aware of software vulnerabilities and exploits is managed through 'vulnerability coordination' or 'vulnerability disclosure'. There are around a thousand individuals worldwide who are capable of finding and exploiting vulnerabilities in the latest versions of modern software and operating systems.[196] There are thousands more who are capable of finding less sophisticated vulnerabilities, such as web application vulnerabilities.[197] Both types of vulnerabilities can be potentially devastating to organizations or individuals if they are exploited.[198]

An emerging market for the acquisition of vulnerability information, also known as 'bug bounties', has emerged in the last 20 years and expanded significantly since 2013.[199] Bug bounties are offered and paid directly by ICT companies, via vulnerability broker competitions (such as the annual Pwn2Own competition), and through the work of companies that manage or facilitate bug bounty programmes (such as HackerOne, BugCrowd, and Synack). Bug bounties are incentives to encourage and direct vulnerability disclosure and are a subset of the general activity of informing ICT companies about potential security issues.[200]

[193] For example, see 'Google, the Wassenaar Arrangement, and vulnerability research', Google Online Security Blog, 20 July 2015, <http://googleonlinesecurity.blogspot.se/2015/07/google-wassenaar-arrangement-and.html>.
[194] See <http://www.nessos-project.eu> and <http://www.syssec-project.eu>.
[195] See <http://www.syssec-project.eu/community/members/#members_map_nav>.
[196] Katie Moussouris, Chief Policy Officer, HackerOne, Interview with the author, 21 May 2015.
[197] Ibid.
[198] Ibid.
[199] Ibid.
[200] Ibid.

The concerns raised by companies, academics, researchers and individuals working in IT security include the following:

- Language in the Wassenaar Arrangement control list category, particularly 'the modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions', describes a software exploit and thereby makes them subject to control.[201]

- Research on software security bugs or vulnerabilities can involve collaboration between researchers in different countries and can result in the identification of new exploit techniques. Sharing information about these new exploit techniques between the researchers would be subject to control.[202]

- Because research on software exploits lies within the field of applied computer science, exchanges between IT security researchers that are cooperating in this area would not be covered by the Wassenaar Arrangement's exemption for 'basic scientific research'.[203]

- Because knowledge of a software exploit can only be sold if it has not yet been disclosed, transfers of a software exploit from one state to another would not covered by the Wassenaar Arrangement's exemption for software that is 'in the public domain'.[204]

Most of the larger companies working on IT security believe that that their products will not be covered by the new controls on intrusion software. However, a number of SMEs working in this area have expressed concerns that their products may be captured. Rapid7, a US-based IT-security company with offices in the EU, has stated that it believes that exports of its penetration testing software, Metasploit, are covered by the controls on intrusion software.[205] Certain versions of Metasploit are already subject to export controls because of the level of encryption employed. However, according to Rapid7, the introduction of new controls, even if applied via general licences, would lead to increased compliance costs.[206]

One EU-based SME that provides training on IT security and penetration testing has halted activities in non-Wassenaar Arrangement countries due to concerns about violating the controls.[207] A company representative stated that their national licensing

[201] 'Problematic Wassenaar Definitions', F-Secure, 9 June 2015, <https://www.f-secure.com/weblog/archives/00002816.html>.
[202] Katie Moussouris, Chief Policy Officer, HackerOne, Interview with the author, 21 May 2015.
[203] Stefano Zanero, Associate Professor, Politecnico di Milano University Interview with the author, 8 May 2015.
[204] Katie Moussouris, Chief Policy Officer, HackerOne, Interview with the author, 21 May 2015.
[205] Jen Ellis, 'Response to the US Proposal for Implementing the Wassenaar Arrangement Export Controls for Intrusion Software', (Rapid 7 Community, 12 June 2015), <https://community.rapid7.com/community/infosec/blog/2015/06/12/response-to-the-us-proposal-for-implementing-the-wassenaar-arrangement-export-controls-for-intrusion-software>.
[206] Ibid.
[207] IT security company representative, Interview with the author.

authority had been asked to clarify this issue but has not yet responded.[208] The company representative noted that the types of EU-based SMEs doing IT security usually have no more than 10-15 employees and the focus of their business constantly changes. As such, they face significant challenges when trying to comply with export controls.[209]

Significant concerns have been raised about the impact of the controls on intrusion software on 'vulnerability coordination' or 'vulnerability disclosure'. The organisers of the 2015 Pwn2own contest issued a statement warning participants that any software or technologies they bring may be subject to national export controls.[210] A number of individuals who had attended previous events did not attend the 2015 competition, though it is unclear if this was because of concerns relating to controls on 'intrusion software'. In September 2015 it was reported that Hewlett Packard was withdrawing sponsorship from the 2016 Pwn2own contest because of concerns about the difficulties of complying with the export controls on intrusion software.[211]

The guidance note produced by the UK Government aimed to alleviate the concerns of the IT security research community. The note underlined the exemptions that apply under the Wassenaar Arrangement and the intended focus of the controls. However, it also noted that certain types of penetration testing software were covered as well as certain types of bug reports and malware samples.[212]

A number of experts have noted that the EU and EU Member States could do more to clarify the intended scope of the controls on intrusion software and specify that work in the field of IT Security is not covered. The community involved 'has little access to legal support for parsing complex export control regulations' and that 'lack of clarity has already threatened to impose a chilling effect'.[213]

7.4 Monitoring Centres

7.4.1 Brief description of the technology

Monitoring centres (also known as Law Enforcement Monitoring Facilities) are systems operated by LEAs and intelligence agencies which pool, store and, in some cases, analyse data from different surveillance sources to reveal patterns, correlations and other information.[214] In certain cases, monitoring centres allow for the analysis of data

[208] Ibid.
[209] Ibid.
[210] '2015 Pwn2own Contest Rules', [N/D], <http://zerodayinitiative.com/Pwn2Own2015Rules.html>.
[211] Dan Goodin, 'Pwn2Own Loses HP as Its Sponsor amid New Cyberweapon Restrictions', *Ars Technica*, 2 Sep. 2015, <http://arstechnica.co.uk/tech-policy/2015/09/pwn2own-loses-hp-as-its-sponsor-amid-new-cyberweapon-restrictions/>.
[212] UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.
[213] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.
[214] Privacy International, 'Monitoring Centres', [N/D], <https://www.privacyinternational.org/?q=node/75>; and Edin Omanovic and Matthew Rice,

in a way that enables the identification of people and groups of people of interest and the monitoring their behaviours. Monitoring centres vary in capability and size but they commonly depend on the following capabilities: data collection; data retention; data processing; and data interface.

Data collection. Monitoring centres differ in terms of the type of information they collect and the sources they utilize. Many monitoring centres are primarily focused on collecting communications data. The communications data is either collected by the communications operator and provided to the monitoring centre via processes of Lawful Interception or the government requests or transfers the data directly from the communications network to the monitoring centre through the use of 'taps' or a 'black box' (for more information, see 7.5 Lawful Interception systems and data retention systems).

In some cases communications data collected by a monitoring centre will be augmented with information from other intelligence sources. These can include audio and video surveillance systems (e.g. laser acoustic systems, CCTVs); location monitoring devices (e.g. GPS trackers, smart chips); Internet monitoring tools (e.g. web-scraping software, social media scanners); or 'device level' compromise (e.g. intrusion software).

Data retention. Monitoring centres also differ in terms of the amount of information they are able to retain. Monitoring centres with higher data retention capacities have greater surveillance capabilities.[215] Intercepted data are usually stored and indexed in Databases Management Systems (DBMS) or Data Warehouses (DW). DBMSs are typically used for *transactional data*, i.e. data that is frequently updated in order to provide a current snapshot of information. Long-term retention of data is managed through DWs.[216] DWs are used for the storage of all raw data. They are typically never updated and they form the basis for Data Marts (DMs) that extract derived data from the primitive data stored in the DW. Monitoring centres usually consult datasets through a single, unified data access that federates DBMS, DW and DM.

Data processing. Monitoring centres also differ in terms of their ability to process and analyse the information they receive. Monitoring centres typically rely on the following techniques: decryption, data mining, image recognition, semantic analysis, relationship mapping and profiling. Decryption is the process by which encrypted data is decoded to reveal its content. Data mining the procedure 'by which large databases

'Monitoring Centers: Force Multiplier From the Surveillance Industry', Privacy International, 29 Apr. 2014, <https://www.privacyinternational.org/?q=node/439>.

[215] Storage capabilities have increased exponentially in recent years. According to Privacy International, the surveillance company VASTech provided Gaddafi's Libya with a system that could capture 30 to 40 millions minutes of landline and mobile conversation a month and archive them for years. See. Privacy International, 'Monitoring Centres', [N/D], <https://www.privacyinternational.org/?q=node/75>.

[216] Coroama, V., *et al.* 'Emerging smart surveillance technologies', in Friedenwald, M. and Bellanova, R., *Smart Surveillance – State of the Art*, SAPRIENT Project, Delivrable 1.1, 2012. p. 30.

are mined by means of algorithms for patterns of correlations between data'.[217] Image recognition and semantic analysis are two specific methods to identify data of interest in larger datasets. Relationship mapping is the process of mapping the relationship between individual based on data related to individuals (names, emails and phone numbers).[218]

Data interface is the process by which the monitoring centre presents the processed information in an intelligible format. Providers of monitoring centres usually provide user-friendly interfaces that will help operators to understand the data and make best use of it.

7.4.2 How it is captured by dual-use export controls

Prior to 2012, monitoring centres were not covered by either the Wassenaar Arrangement or the EU dual-use control lists. However some EU Member States have controlled exports of certain monitoring centres using Article 8 of the Dual-use Regulation, which allows for the control of non-listed items for reasons of public security or because of human rights considerations.

In 2012, Italy used Article 8 to impose controls on the export of 'public LAN database centralised monitoring systems' to Syria.[219] The controls were imposed following reports in 2011 that the Italian company Area SpA had begun to install a monitoring centre in Syria and were aimed at making future sales of such systems subject to export controls.[220] In 2015, Germany used Article 8 to impose controls on the export of a broad range of monitoring centres (see below).

In 2013 a new category covering 'IP Network Surveillance' was added to the Wassenaar Arrangement dual-use control list to cover certain types of network surveillance monitoring centres. The language was proposed by the French Government and was specifically designed to control exports of a monitoring centre that the French company Amesys had sold to Libya.[221] France implemented the control

[217] Hildebrandt, M., 'Defining profiling: A New Type of Knowledge', in Mireille Hildrebrand and Serge Gutwirth, (eds.), *Profiling the European Citizens: Cross-Disciplinary Perspectives,* (Springer, New York, 2008), pp. 17.46.

[218] Clark, R., 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance', *Journal of Law and Information Science,* Vol. 4, No2, 1993, pp. 403-419; and Coroama, V., *et al* 'Emerging Smart Surveillance technologies', in Friedenwald, M. and Bellanova, R.,*Smart Surveillance – State of the Art*, SAPRIENT Project, Delivrable 1.1, 2012, p. 30.

[219] 'Information note — Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Information on measures adopted by Member States in conformity with Articles 5, 6, 8, 9, 10, 17 and 22', Official Journal of the European Union, 19 Sep. 2012, C283, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.283.01.0004.01.ENG>.

[220] Tim Maurer, Edin Omanovic, and Ben Wagner, 'Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age', (New America Foundation, Digitale Gestellschaft, Open Technology and Privacy International, Mar. 2014). In November 2011 Area SpA announced that they would not complete the installation of the monitoring centre in Syria. Silver, V., 'Italian firm said to exit Syrian monitoring project', Bloomberg, 28 Nov. 2011, <http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html>.

[221] Edin Omanovic, 'Export Controls in the Digital Age: The EU Export Control Policy Review and Surveillance Technology', *World ECR*, Mar. 2015.

almost immediately after it was approved at the Wassenaar Arrangement. [222] This update was implemented at the EU level in December 2014 via category 5A001j.

Category 5A001j applies to monitoring centres which operate on 'carrier class IP Networks' and which perform: (a) analysis at the application layer; (b) extraction of selected metadata and application content; (c) indexing of extracted data; (d) execution of searches on the basis of 'hard selectors';[223] and (e) 'mapping of the relational network of an individual or groups of people'. Systems and equipment developed for marketing purposes, network quality of service or quality of experience are excluded from the control.

Category 5A001j only applies to monitoring centres that operate on IP networks and that are designed to map relationship networks of an individual or group of individuals.[224] The control does not apply to systems that are focused on other types of communication networks (such as a mobile or fixed-line telephone networks) and which have limited data processing capacities. However, the controls appear to apply regardless of whether the monitoring centre is acquiring information via Lawful Interception processes or drawing it directly from the communications network.

It has been argued that 5A001j may be framed too narrowly and does not cover a range of monitoring centres that might be of potential concern on the basis of human rights or security concerns.[225] Concerns have also been raised about the ability of exporters to circumvent the controls by sourcing the elements of a monitoring centre from different vendors and assembling it in the recipient country.[226] The use of different vendors to design and build a monitoring centre that meets the particular requirements of an end-user is increasingly common.[227] Moreover, the components used often have a range of non-surveillance applications and are not subject to export controls.

In July 2015, Germany adopted a new control list category, 5A902, covering 'Law Enforcement Monitoring Facilities' (also know as 'monitoring centres') and 'retention systems' for 'Intercept Related Information' supplied to end-users based outside the customs territory of the EU. (For more information on the control of 'retention

[222] Privacy International, 'Privacy International BIS submission', [N/D], <https://www.privacyinternational.org/sites/default/files/Privacy%20International%20BIS%20submission.pdf>.

[223] 'Hard data' is defined as 'data or set of data related to an individual (family name, given name, email, street address, phone number or group affiliation)'.

[224] For a full description, see Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[225] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[226] Adam Weber, Elena Hushbeck, Emily Rosenblum, Jay Johnson, Joe Petersen and Pete Heine, 'IP network communications surveillance systems: deciphering Wassenaar Arrangement controls', World ECR, Apr. 2015.

[227] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

systems' see 7.5 Lawful Interception systems and data retention systems).[228] The controls apply both to supplies of complete systems and technical assistance, meaning that services provided for already installed systems would potentially be controlled. Citing Article 8 of the Dual-use Regulation, Germany stated that these additions to its export controls were intended to prevent the use of this technology for 'internal repression' and the suppression of human rights, and that it would promote their wider adoption at both the EU and Wassenaar Arrangement level.[229]

The controls under 5A902 on 'monitoring centres' apply to centres that are compliant with ETSI or 'equivalent' standards along with 'specially designed components'. The controls do not apply to systems and devices that are specifically designed for: (a) billing; (b) data collection functions within the network; (c) quality of service of the network; (d) user satisfaction; and (e) operation at telecommunications companies (services providers).

7.4.3 Human rights concerns

Monitoring centres exported from EU Member States have been connected to violations of human rights by LEAs or intelligence agencies in a number of different states. The human rights abuses committed include violations of:

- right to privacy;
- freedom of expression;
- freedom of association;
- right to life;
- freedom from arbitrary arrest and detention; and
- freedom from torture, inhuman treatment and degrading treatment.

During the Arab Spring, monitoring centres supplied by EU-based companies were used to identify and track dissidents in at least four states, including Iran, Libya, Syria and Bahrain.[230] The most well documented cases involved Amesys in Libya and Trovicor in Bahrain.

Amesys' Eagle system was used by the Libyan intelligence service to monitor both phone, email and chat conversations of government opponents in Libya and abroad on

[228] BMWI, 'Anlage AL zur Außenwirtschaftverordnung [Annex AL to the German Foreign Trade Regulations]', July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/A/anlage-al-zur-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.
[229] BMWI, 'Gabriel: Export von Überwachungstechnik Wird Starker Kontrolliert [Gabriel: Export of Surveillance Technology Under Strong Controls]', 8 July 2015, <http://www.bmwi.de/DE/Presse/pressemitteilungen,did=719188.html>; and Catherine Stupp, 'Germany Leaves Brussels behind on Surveillance Tech Export Controls', EurActiv, 10 July 2015, <http://www.euractiv.com/sections/infosociety/germany-leaves-brussels-behind-surveillance-tech-export-controls-316226>.
[230] 'Amesys Lawsuit (re Libya)', Business & Human Rights Resource Centre, accessed 2 Aug. 2015, <http://business-humanrights.org/en/amesys-lawsuit-re-libya-0>.

a 'massive scale'.[231] Opponents of Gaddafi's regime experienced multiple forms of harassment by the authorities, including arbitrary arrest and detention as well as torture. In certain cases, victims were shown transcripts of emails and text messages while being tortured.[232] Amesys's Eagle System was also reportedly used by the Libyan intelligence services to spy on political opponents based in London and Helsinki.[233]

Amesys is currently the subject of a court case in France where it is accused of complicity with human rights abuses in Libya. The case followed the filing of a criminal complaint in 2011 by two human rights organisations—International Federation for Human Rights (FIDH) and la Ligue des droits de l'Homme (LDH)—acting for five Libyan citizens.

Trovicor, while it was still a part of Nokia Siemens Networks (NSN), installed and maintained monitoring centres in Bahrain that were used by the authorities to monitor democratic activists. According to media reports, almost two-dozen political prisoners were beaten and subsequently interrogated while being shown transcripts of emails and text messages.[234]

7.4.4 Security concerns

The study was unable to find any documented cases of monitoring centres supplied by companies based in EU Member States being used in ways that pose a threat to EU or EU Member State security.

7.4.5 Use and governance in EU Member States

Monitoring centres are widely used by LEAs and intelligence agencies in EU Member States, including systems covered by the controls on 'IP Network Surveillance'. For example, Amesys' Eagle system is reportedly used by the French intelligence agencies.[235]

[231] Aikins M., 'Jamming Tripoli, Inside Moammar Gadhafi's Secret Surveillance Network', 18 May 2012, <http://www.wired.com/2012/05/ff_libya/all/>.
[232] 'The Amesys Case: The Victims Anxious to See Tangible Progress', (FIDH, 11 Feb. 2015), <https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf>.
[233] Ross, A., 'Was Gaddafi 'cyber spying' on opponents in the UK', Bureau of investigative journalism, 30 Nov. 2011, <www.thebureauinvestigates.com/2011/11/30/was-gaddafi-using-french-technology-to-spy-on-opponents-in-the-uk/>.
[234] Silver, V. And Elgin, B., 'Torture in Bahrain becomes routine with help of Nokia Siemens', Bloomberg, 23 Aug. 2011, <http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html>; Silver, V., 'EU may probe Bahrain spy gear abuses', Bloomberg, 24 Aug. 2011; and Trevor, T. 'SpyTech Companies and Their Authoritarian Customers: Part II Trovicor and Area SpA', EFF, 12 Feb. 2012, <https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa>.
[235] 'Amesys: le changement, ce n'est pas maintenant', Reflets.info, 16 June 2012, <https://reflets.info/amesys-le-changement-ce-nest-pas-maintenant/>.

7.4.6 Producer companies in the EU

A significant number of companies in the EU produce monitoring centres, including systems captured by the controls on 'IP Network Surveillance' (see Tables 7.6 and 7.7).[236]

The information available indicates that most of these companies are 'pure players' that specialize in the production of a range of surveillance technologies for LEAs. While most of the companies producing monitoring centres in the EU are SMEs there are also a number of larger defence companies, including BAE Systems and Thales, which produce monitoring centres as part of a wider portfolio of defence and security solutions.

[236] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, March 13, 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

Table 7.6. EU-based manufacturers of monitoring centres covered by controls on 'IP Network Surveillance'

Company	Location	Revenue (2013)	Profit (2013)	Employment (2013)
Amec [a]	France	€3 m.	€1 m.	13
Area	Italy	-	-	>100
ATIS	Germany	€18 m.	€2 m.	106
BAE Systems	UK	$28 000 m.	$275 m.	84 600
Expert Systems [b]	Italy	€11 m.	€1 m.	-
Group 2000	The Netherlands	-	-	55
Nexa Technologies	France	€5 m.	€1 m.	<49
Trovicor	Germany	€20 m.	€2 m.	170
Amec	France	€3 m.	€1 m.	13

a. 2011 data
b. 2012 data

Table 7.7. EU-based manufacturers of other types of monitoring centres

Company	Location	Revenue (2013)	Profit (2013)	Employment (2013)
Gamma International	Germany / UK	-	<€1 m.	-
iPS	Italy	$24 m.	-	200
NETI	Hungary	HUF1 m.	<HUF1 m.	-
Qosmos	France	€19 m.	€3 m.	100
RCS Lab	Italy	-	-	-

7.4.7 Producer companies outside the EU

A significant number of companies based outside the EU produce monitoring centres. Examples of companies that produce monitoring centres covered by the controls on IP Network Surveillance include: Clear trail (India); Defentek (USA); GlimmerGlass (USA); Narus/Boeing (USA); Nice Systems (Israel/USA); SS8 (USA); VASTech (South Africa); Verint (USA); and ZTE Corp (China).[237] Companies that produce other types of monitoring centres that would potentially be captured by expanded controls in this area include: Kommlabs (India); Septier (Israel); and SSI Pacific (Australia).[238]

The level of international competition in the market for monitoring centres appears to be increasing, with a number of component vendors, such as SS8, and defence companies, such as Thales and BAE Systems, entering the market. A number of companies based in the non-Wassenaar Arrangement states, including Clear trail (India) and ZTE Corp (China), are also expanding their presence in the global market.

7.4.8 Current /potential regulatory burden (Government)

Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, two reported that items covered by the controls on IP network surveillance were exported from their country. However, no EU Member States reported that they had received any applications for export licences for these items. EU Member States noted that it was too early to assess the impact of these controls, since they were only adopted at the EU level in December 2014.[239]

Depending on how they are drafted and implemented, the introduction of expanded controls on monitoring centres could create an increased regulatory burden for governments.

7.4.9 Current / potential regulatory burden (Industry)

EU based companies have reacted in different ways to the introduction of controls on 'IP Network Surveillance'. Amesys have taken steps to move their business outside the EU, although it is unclear if this was a direct result of the implementation of controls on IP Network Surveillance since the decision to move pre-dates their introduction. In 2012, Bull—the parent company of Amesys—sold the Eagle system business in 2012 to Nexa Technologies, a French based company owned by the Plath Group based in Germany. Nexa Technologies then divided the Eagle system business in two parts. The DPI activity for private companies stayed within the company in France while the surveillance capability for LEAs and intelligence agencies (re-branded Cerebo) was transferred to a new company called Advanced Middle East Systems (AMESys), based

[237] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, March 13, 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.
[238] Ibid.
[239] Kees-Jan Steenhoek, Acting head of the export control department, The Netherlands Ministry of Foreign Affairs, Interview with the author, 17 April 2015.

in the UAE.[240] Cerebo is officially marketed by AMESys from the UAE but royalties on sales are paid to Nexa Technologies.[241]

Other companies affected by the controls have not moved. Indeed, a representative from one EU-based company that produces systems covered by controls on 'IP Network Surveillance' stated that they were not opposed to the new measures.[242] They noted that being subject to export controls always has advantages. In particular, it creates clarity, awareness, and the conditions for additional political and economic support should a contract need to be cancelled if the export license is revoked due to a change in geopolitical conditions or a misuse by the end-user of the supplied system.[243]

However, the company representative also noted that they would appreciate clearer information from relevant EU bodies and their national licensing authority about which destinations and end-users should be viewed as suitable customers.[244] This would help the company to better focus its investments in long and complicated sales cycle activities. The issue is particularly important since the company needs to find customers outside Europe to maintain its current levels of R&D spending and to face the strong competition from non EU-based companies that are leading in the European market.[245]

The introduction of expanded controls on monitoring centres could potentially create an increased regulatory burden for companies. However, this would depend on how they are phrased and implemented by the relevant national licensing authority. Germany has assessed that its expanded controls on monitoring centres will have a limited effect on the German economy. This is in spite of the fact that Germany is one of the EU Member States with the most companies active in this area.[246] Germany argues that the controls only affect a small group of companies—most of which are already subject to export controls—and will provide create clarity regarding their responsibilities in this area.[247]

[240] Paquette E., 'Les Mercenaires de la cyber-guerre', L'express*,* 22 Nov. 2014.
[241] 'Mais que se passe-t-il chez Bull et Nexa technologies?', 14 Oct. 2014, Reflet Info, <https://reflets.info/mais-que-se-passe-t-il-chez-bull-et-nexa-technologies/>.
[242] Industry representative, interview with the author.
[243] Ibid.
[244] Ibid.
[245] Ibid.
[246] Catherine Stupp, 'Germany Leaves Brussels behind on Surveillance Tech Export Controls', EurActiv, 10 July 2015, <http://www.euractiv.com/sections/infosociety/germany-leaves-brussels-behind-surveillance-tech-export-controls-316226>.
[247] BMWI, 'Verordnung der Bundesregierung Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung [Regulation of the Federal Government Fourth Regulation amending the Foreign Trade Regulations]', 17 July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

7.5 Lawful Interception systems and data retention systems

7.5.1 Description of technology

Lawful Interception (LI) is the process whereby a network operator is required by a judicial or administrative order to provide communications data for one or more of its users to a Law Enforcement Monitoring Facility (also know as a 'monitoring centre') by a LEA or intelligence agency.[248] A network operator is a company that manages a communications network, such as Vodaphone or TeliaSonera. 'Communications data' can be: (a) 'meta data', information about the use of a network or the calls that a subscriber has made; (b) 'content data', what is said in a phone call or the content of text message; or (c) 'location data', information about the movements of a subscriber to a mobile phone network.[249] Data retention refers to the storage of 'meta data' by the network operator.

Most states have laws in place that require network operators to comply with LI requests.[250] Most states also require network operators to store certain types of communications data on all subscribers for potential later use. Technical standards have been developed regarding the type and format of information provided under LI requests and stored via data retention in order to facilitate the work of LEAs and intelligence agencies and to help network operators minimize costs.[251] These technical standards do not stipulate the mechanisms that should govern the use of these powers, the government agencies that should be able to utilize them, or the way they should be employed in practice.

However, certain technical standards on LI do include provisions that can help to prevent human rights abuses, particularly the right to privacy. For example, ETSI's technical standards on LI state that 'Law Enforcement Network systems' should never be integrated 'directly into the public network architecture'.[252] In addition, Germany's technical standards on LI state that the 'mediation function' of the LI system used by

[248] See 'Lawful Interception: A Mounting Challenge for Service Providers and Governments', (Frost & Sullivan, 2011); and Vodaphone, 'Law Enforcement Disclosure Report', Feb. 2015, <http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html>.

[249] Access providers and service providers may also be required to provide communications data to a monitoring centre, but this is handled via a process known as 'government requests'. An 'access provider' is a company that provides access to a communications network but does not necessarily manage the network itself, such as Trustive or Boingo. A 'service provider' is a company which provides some type of 'over the top' communication service, such as Gmail or Skype.

[250] 'Lawful Interception: A Mounting Challenge for Service Providers and Governments', (Frost & Sullivan, 2011).

[251] These include international standards drawn up by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP), as well as national standards, such as the standards in Germany's 'Technical Guideline for implementation of legal measures for monitoring telecommunications and to information requests for traffic data (TR TKÜV)]', the American National Standards Institute (ANSI) standards developed in the US, and Russia's System of Operative Investigative Measures (SORM) standards..

[252] 'Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture (ETSI TR 101 943 V2.2.1)', (ETSI, Nov. 2006), <http://www.etsi.org/deliver/etsi_tr/101900_101999/101943/02.02.01_60/tr_101943v020201p.pdf>.

the network operator should have certain limitations.[253] In contrast, SORM technical standards on LI do not contain such safeguards and are seen as being more prone to facilitating human rights abuses.[254]

LI is often characterized as a form of 'targeted surveillance', in which individuals or groups of individuals are the focus of attention and where processes are conducted in accordance with some kind of prior judicial review. Targeted surveillance is, in turn, frequently contrasted with 'mass surveillance', in which the communications of an entire population or group are collected or monitored. This can be achieved by placing 'taps' on fibre-optic cables that pass communications data from communications network directly to the monitoring centre.[255] In other cases, states require a network operator to pass all communications data directly to the monitoring centre via a 'black box'.[256] These practices effectively bypass technical standards on how LI requests should be submitted and fulfilled. There are no international standards regarding the type or format of the information that can be collected using these practices.

Mass surveillance has been widely criticized as representing a direct violation of the right to privacy under article 17 of the International Covenant on Civil and Political Rights and as being more prone to the facilitation of other forms of human rights abuses than targeted surveillance.[257] However, the use of targeted surveillance can also involve a direct violation of the right to privacy and facilitate more serious human rights abuses. Moreover, the distinction between 'targeted surveillance' and 'mass surveillance' is not always clear. First, there is no agreed definition of what the two terms mean. Second, depending on the amount of information collected and how it is used, 'taps' and 'back boxes' can be employed to conduct 'targeted surveillance'. Third, depending on the powers available to LEAs and intelligence agencies, LI requests can be used in ways that resemble 'mass surveillance'.

In recent years, communications operators have sought to create greater transparency and accountability with regards to the way LI processes and government

[253] German Government, 'Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten (TR TKÜV) [Technical Guideline for implementation of legal measures for monitoring telecommunications and to information requests for traffic data (TR TKÜV)]', Aug. 2012.
[254] See 'Private Interests: Monitoring Central Asia' (Privacy International, Nov. 2014), <https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf>.
[255] 'Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397' (UN General Assembly, 23 Sep. 2014).
[256] Vodaphone, 'Law Enforcement Disclosure Report', Feb. 2015, <http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html>; and Eva Galperin, 'Swedish Telcom Giant Teliasonera Caught Helping Authoritarian Regimes Spy on Their Citizens,' Electronic Frontier Foundation, 18 May 2012, <https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its>.
[257] See 'Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397' (UN General Assembly, 23 Sep. 2014); and Lucy Purdon, 'Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study – Ericsson' (IHRB, 16 Nov. 2014), <http://www.ihrb.org/publications/reports/human-rights-challenges-for-telecommunications-vendors.html>.

requests are governed and operated, and to push governments to develop more standardized processes in this area. For example, a number of communication operators provide information on LI requests and government requests received from the governments of the countries in which they operate, as well as details of how they responded.[258] In addition, via bodies like the Global Network Initiative (GNI) and the Telecommunications Industry Dialogue, communication operators have sought to define agreed policies outlining what communications data they will share with governments and the circumstances in which they will do so.[259] Finally, a number of governments, particularly in the EU, have begun to publish more detailed information on their use of LI powers, including the number of requests for communications data that they have issued to communication operators.[260]

Depending on the type of communications data requested and the relevant national laws in place, a network operator will need to have systems in place that are able to perform one or more of the following functions in order to fulfil LI requests:

a) *A 'mediation function'* to receive requests from LEAs and intelligence agencies and provide responses.[261] This will involve converting the intercepted communications data in to the appropriate format required by the monitoring centre; and

b) *A 'data collection function'* to access relevant information as it passes through the communications network.[262] Usually this is performed through the data collection functions that are integrated in to the core elements of the communications network. Depending on the type of communications data requested, this may also involve the use of probes and DPI systems.

[258] For example, see 'Government Requests Report' [Facebook, N/D], accessed 2 Sep. 2015, <https://govtrequests.facebook.com>; 'Law Enforcement Disclosure Report'; 'TeliaSonera Transparency Report January 2015', (TeliaSonera, Jan. 2015), <http://www.teliasonera.com/en/sustainability/transparency-report-new/>; 'CREDO Transparency Report - Q2 2015' (CREDO, 24 July 2015), <http://www.credomobile.com/transparency>; and 'Transparency at Telstra', [N/D], <https://www.telstra.com.au/privacy/transparency>.

[259] The GNI seeks to provide guidance 'to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally', particularly freedom of expression and the right to privacy, <http://globalnetworkinitiative.org/principles/index.php>. The Telecommunications Industry Dialogue 'is a group of telecommunications operators and vendors who jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights', <http://www.telecomindustrydialogue.org/about/>.

[260] 'TeliaSonera Transparency Report January 2015', (TeliaSonera, Jan. 2015), <http://www.teliasonera.com/en/sustainability/transparency-report-new/>.

[261] 'Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture (ETSI TR 101 943 V2.2.1)' (ETSI, Nov. 2006), <http://www.etsi.org/deliver/etsi_tr/101900_101999/101943/02.02.01_60/tr_101943v020201p.pdf>.

[262] Ibid.

In addition, depending on the relevant national laws in place, a network operator may also need to have systems in place are able to perform a 'data retention function' in order to fulfil data retention requirements.[263]

A range of different companies produces LI systems and/or data retention systems that perform one or more of these functions. In certain cases, the network manufacturer may supply the system. For example, Ericsson (Sweden) has a 'Lawful Interception Solution' that it integrates with its communications networks.[264] Ericsson's 'Lawful Interception Solution' provides a 'mediation function' and a 'data collection function'.[265] In other cases, a separate company may supply the system. Utimaco (Germany) produces a 'Lawful Interception Management System' and a 'Data Retention Suite' that, together, provide a 'mediation function', a 'data collection function' and a 'data retention function'.[266] Utimaco's systems can be used in connection with a range of different communications networks.

LI systems can be managed either by the network operator, by the supplier company, or by a specialized third-party service provider. When rolling out a network for an operator, the vendor usually hands over the management and running of the network to the operator. The vendor can however also manage the network on behalf of the operator, by providing so called Managed Services which can include handling requests for LI that are passed from the operator.[267] Utimaco has arrangements with a number of companies who can manage its LI systems on behalf of the network operator.[268] However, legally speaking it is always the network operator that fulfils the LI request and provides communications data to the monitoring centre.[269]

There are several advantages associated with using LI systems.[270] First, LI systems are able to handle LI requests relating to multiple communication services and protocols via a single user interface. The range of communication services and protocols that might make use of a particular communications network has expanded dramatically in recent years. For example, an IP Network may carry *inter alia* e-mail,

[263] 'Lawful Interception (LI); Retained Data Handling; Handover Interface for the Request and Delivery of Retained Data (ETSI TS 102 657 V1.4.1)' (ETSI, Dec. 2009), <http://www.etsi.org/deliver/etsi_ts/102600_102699/102657/01.04.01_60/ts_102657v010401p.pdf>.
[264] Ericcson, 'Ericsson Lawful Interception Solution', [N/D], <http://www.ericsson.com/us/ourportfolio/telecom-operators/lawful-interception-solution>-
[265] Ericsson representative, Communication with the author, 10 Sep. 2015.
[266] See Utimaco, 'Intercept Communications — Lawfully', [N/D], <https://lims.utimaco.com/products/lawful-interception-management-system/>.
[267] Lucy Purdon, 'Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study – Ericsson' (IHRB, 16 Nov. 2014), <http://www.ihrb.org/publications/reports/human-rights-challenges-for-telecommunications-vendors.html>.
[268] Utimaco, 'Utimaco LIMS Lawful Interception of Telecommunication Services', Feb. 2011, <https://www.documentcloud.org/documents/409336-198-201106-iss-utimaco-lims.html>.
[269] Lucy Purdon, 'Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study – Ericsson' (IHRB, 16 Nov. 2014), <http://www.ihrb.org/publications/reports/human-rights-challenges-for-telecommunications-vendors.html>.
[270] See Utimaco, 'Utimaco LIMS Lawful Interception of Telecommunication Services', Feb. 2011, <https://www.documentcloud.org/documents/409336-198-201106-iss-utimaco-lims.html>.

webmail, internet access and instant messaging traffic, all of which can be the potential subject of an LI request. Second, LI systems make access to communications data accessible via only a single user interface and encrypting all relevant information. This makes it easier for the network operator to comply with technical standards in LI which demand that LI requests are processed 'blind' without any knowledge of its content and purpose. It also makes it harder for unauthorized personnel or outside parties to gain access to communications data. Third, LI-systems will often have in-built elements that can help to prevent human rights abuses (see below).

In most cases, the end-user for an LI system will be a privately run network operator. However, in situations where a state seeks to bypass standardized LI processes through the use of 'taps' or a 'black box' the state authority involved may employ some form of LI system. For example, in 2013, Pakistan's Inter-Services Intelligence (ISI) issued a Request for Proposals (RFP) for the development of an IP Monitoring System that would use 'taps' to access the main fibre optic cables entering Pakistan.[271] The requested solution should include an 'LI system' able to log all interception-related activities and protect sensitive data during transmission.

7.5.2 How it is captured by dual-use export controls

Exports of many types of LI systems are subject to export controls due to the level of encryption they use, meaning that they are covered by category 5A002 on 'cryptography' in the EU dual-use control list. For example, Utimaco's 'Lawful Interception Management System' uses 'encryption of internal and external data traffic' and 'encrypted storage of all sensitive data records'.[272] Most types of communication networks are also subject to export controls due to the level of encryption they use. Hence, communications networks are covered by export controls, regardless of whether or not they are being supplied together with an LI system.

In July 2015, Germany adopted a new control list category, 5A902, covering 'Law Enforcement Monitoring Facilities' (also know as 'monitoring centres') and 'retention systems' for 'Intercept Related Information' supplied to end-users based outside the customs territory of the EU (For more information on the controls on 'monitoring centres' see 7.4 Monitoring Centres).[273] The controls apply both to supplies of complete systems and technical assistance, meaning that services provided for already installed systems would potentially be controlled. Citing Article 8 of the Dual-use Regulation, Germany stated that these additions to its export controls were intended to prevent the use of this technology for 'internal repression' and the suppression of

[271] 'Tipping the Scales: Security & Surveillance in Pakistan', Privacy International, July 2015, <https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf>.
[272] Utimaco, 'Utimaco LIMS Lawful Interception of Telecommunication Services', Feb. 2011, <https://www.documentcloud.org/documents/409336-198-201106-iss-utimaco-lims.html>.
[273] BMWI, 'Anlage AL zur Außenwirtschaftverordnung [Annex AL to the German Foreign Trade Regulations]', July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/A/anlage-al-zur-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

human rights and that it would promote their wider adoption at both the EU and Wassenaar Arrangement level.[274]

The controls on 'retention systems' for 'Intercept Related Information' apply to systems or devices that are compliant with ETSI or 'equivalent' standards along with 'specially designed components'.[275] Hence, the controls cover 'data retention systems' with a 'data retention function' but not LI systems with a 'data collection' or 'data mediation' function. In addition, the controls do not apply to systems or devices that are specifically designed for: (a) billing; (b) data collection functions within the network; (c) quality of service of the network; (d) user satisfaction; and (e) operation at telecommunications companies (services providers).[276] Exemption (e) implies that systems supplied to a network operator would not be covered by the controls.

7.5.3 Human rights concerns

LI systems and data retention systems exported from EU Member States have been connected to violations of human rights in a number of non-EU states. The human rights abuses committed include violations of:

- right to privacy;
- freedom of expression;
- freedom of association;
- right to life;
- freedom from arbitrary arrest and detention; and
- freedom from torture inhuman treatment and degrading treatment.

However, most of the allegations are based upon evidence that network operators in states with a poor human rights record are using the systems, rather than any explicit connection between the systems themselves and specific human rights abuses. EU-based companies have also been criticized for supplying LI systems to network operators in states that apply SORM LI standards, which are viewed as being more prone to facilitating human rights abuses. For example, Ericsson has been criticized for supplying SORM-compliant LI mediation systems to network operators in

[274] BMWI, 'Gabriel: Export von Überwachungstechnik Wird Starker Kontrolliert [Gabriel: Export of Surveillance Technology Under Strong Controls]', 8 July 2015, <http://www.bmwi.de/DE/Presse/pressemitteilungen,did=719188.html>; and Catherine Stupp, 'Germany Leaves Brussels behind on Surveillance Tech Export Controls," Text, *EurActiv*, (July 10, 2015), <http://www.euractiv.com/sections/infosociety/germany-leaves-brussels-behind-surveillance-tech-export-controls-316226>.

[275] BMWI, 'Gabriel: Export von Überwachungstechnik wird stärker kontrolliert [Gabriel: Export of Surveillance Technology Under Stronger Controls]', 8 July 2015, <http://www.bmwi.de/DE/Presse/pressemitteilungen,did=719188.html>.

[276] Ibid.

Kazakhstan.[277] In these cases Ericsson works with a third party to ensure their systems are accessible to law enforcement.[278]

EU-based network operators have been criticized for allowing the LEAs or intelligence agencies in the states where they operate to install black boxes in their communication networks. For example, in 2012 TeliaSonera was criticized for allowing Belarus, Uzbekistan, Azerbaijan, Tajikistan, Georgia and Kazakhstan to install black boxes in their communications networks.[279] In Georgia, lawyers alleged that the use of a black box violated Georgia's national laws on surveillance powers.[280] TeliaSonera responded by issuing a 'freedom of expression policy', which states that it 'advocates that governments should not have direct access to a company's networks and systems'.[281]

If a network operator does not have an LI system or data retention system in place this does not prevent violations of human rights from taking place. Communications data can still be intercepted and stored even if an LI system or data retention system is not installed, though the process may be more costly and complicated. All network operators will collect and store communications data to ensure that their systems are working correctly as for billing and marketing purposes. In certain cases, states have demanded that this information is handed over without utilizing standardised LI processes. Moreover, LI system often have in-built elements that can help to prevent human rights abuses. For example, Ericsson's 'Lawful Interception Solution' is designed to limit the number of people that can be intercepted simultaneously.[282] These restrictions will typically exist regardless of whether the LI system is being used by a network operator or an LEA or intelligence agency.[283]

7.5.4 Security concerns

The study was unable to find any documented cases of LI data retention and mediation systems supplied by companies based in EU Member States being used in ways that pose a threat to EU or EU Member State security.

[277] 'Private Interests: Monitoring Central Asia', Privacy International, Nov. 2014, <https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf>, p. 59.
[278] Ibid.
[279] Eva Galperin, 'Swedish Telcom Giant Teliasonera Caught Helping Authoritarian Regimes Spy on Their Citizens,' Electronic Frontier Foundation, 18 May 2012, <https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its>.
[280] Ibid.
[281] 'TeliaSonera Group Policy on Freedom of Expression in Telecommunications', TeliaSonera, 5 Dec. 2013, <http://www.teliasonera.com/Documents/Public%20policy%20documents/TeliaSonera_Group_Policy_on_Freedom_of_Expression_in_Telecommunications.pdf>.
[282] Lucy Purdon, 'Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study – Ericsson' (IHRB, 16 Nov. 2014), <http://www.ihrb.org/publications/reports/human-rights-challenges-for-telecommunications-vendors.html>.
[283] Ibid.

7.5.5 Use and governance in EU Member States

Different types of LI systems and data retention systems are widely used by network operators in EU Member States. The EU has established standards that network operators should be required to fulfil in the field of Lawful Interception under EU Member States' national legislation.[284] However, national practices in this area vary significantly among EU Member States.[285] Moreover, in many cases laws and regulations are broad and opaque and 'frequently lag the development and use of communications technology.'[286]

Since 2006, EU legislation has required EU Member States to ensure that network operators retain certain types of 'meta data' for between 6 and 24 months.[287] However, in April 2014 the EU Court of Justice declared the EU Data Retention Directive to be invalid due to its failure to comply with the principle of proportionality.[288] National standards in this area also differ significantly.

7.5.6 Producer companies in the EU

A significant number of companies in the EU produce LI systems and/or data retention systems (see Table 7.8).[289] The information available indicates that these companies are a mix of 'pure players' that specialize in the production of a range of surveillance technologies for LEAs, larger defence companies, including BAE Systems and Thales, and large telecommunications companies such as Ericsson and Alcatel-Lucent.

The EU is also home to 3 of the world's 5 largest manufacturers of communication networks: Ericsson, Nokia and Alcatel-Lucent. Nokia (Finland) does not produce its own LI systems but partners with Utimaco (Germany) when selling its communication networks. Dual-use related exports of telecommunications infrastructure were worth up to €2.8 billion in 2014 (See Table 7.2).

[284] European Council, 'Council Resolution of 17 January 1995 on the lawful interception of telecommunications', Official Journal of the European Union C329, 11 Mar. 1996, p. 1-6.
[285] Vodafone, 'Law Enforcement Disclosure Report', Feb. 2015, <http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html>.
[286] Ibid.
[287] European Council, 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', Official Journal of the European Union, 13 April 2006, L 105, pp. 54-63.
[288] David Anderson Q.C., 'A Question of Trust: Report of the Investigatory Powers Review" (Her Majesty's Stationery Office, June 2015), p. 110.
[289] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb 2015).

Table 7.8. EU-based manufacturers of LI systems and/or data retention systems

Company	Location	Revenue (2013)	Profit (2013)	Employment (2013)
Aculab	UK	£3 m.	-	185
Alcatel-Lucent	France	€14 436 m.	€ 1 294 m.	62 311
ATIS	Germany			
BAE Systems	UK	$28 000 m.	$275 m.	84 600
CCT Cetratech	Sweden	-	-	-
Chemring Tech. Solutions	UK	£472 m.	£57 m.	>3 500
ComsTrac	UK	-	<€1 m.	-
DigiVox	The Netherlands	-	-	-
Elaman	Germany/ Switzerland	-	<€1 m.	-
Ericsson	Sweden	SEK227 400 m.	SEK17 800 m.	114 340
Group 2000	The Netherlands	-	-	55
GTEN	Czech Republic	-	-	-
INNOVA	Italy	-	-	140
INVEA-TECH	Czech Republic	$3 m.	-	-
iPS	Italy	$24 m.	-	200
NETI	Hungary	HUF1 m.	<HUF1 m.	-
NSF Telecom	Finland	-	-	-
Pine Lawful Interception	The Netherlands	-	-	-

Company	Location	Revenue (2013)	Profit (2013)	Employment (2013)
SIEMENS Convergence Creators, GMbH	Austria	-	-	-
Syborg	Germany	-	<€1 m.	60
Telesoft	UK	-	-	100
Thales	France	€14 000 m.	€1 600 m.	66 000
Utimaco	Germany	-	-	-
Westminster International	UK	-	-	-

7.5.7 Producer companies outside the EU

A significant number of companies based outside the EU produce LI systems and/or data retention systems.[290] These include CRYPTOM-M (Ukraine); Altron (Ukraine) AQSAQAM Americas (Australia/USA); Bridgewater (Canada); ClearTrail (India); Communigate (USA); Dreamlab (Switzerland); Emulex (USA); Everis (USA); Fastech (India); Incognito (Canada); Intelleq Networks (USA); IP Fabrics (USA); MFI-Soft (Russia); NetOptics (USA); NetQuest (USA); NICE Systems (Israel/USA); ONPATH Technologies (USA); Packet Forensics (USA); PALADION (India); Pen-Link (USA); Protei (Russia) Septier (Israel); SS8 (USA) SSI Pacific (Australia/New Zealand/Singapore); SUNTECH (Brazil); TraceSpan (Israel); Verint (USA); VOCAL (USA); and VoIP-PAL (USA). A number of companies based outside the EU produce communications networks. These include ZTE Corp (China) and Huawei (China).

One industry representative noted that the question of foreign availability is very relevant for LI systems and communication networks, since much of the technology involved is the subject of internationally agreed technical standards and there are a range of highly capable non-European manufacturers.[291] As a result, it is relatively easy for these companies to move into a market that European companies exit. [292] For example, since 2010, Ericsson and Nokia have reduced sales of communications

[290] 'The Little Black Book of Electronic Surveillance: 2015', (Insider Surveillance, Feb 2015).
[291] Industry representative, interview with the author.
[292] Ibid.

networks to Iran, while Huawei (China) and ZTE Corp (China) have increased their presence significantly.[293]

7.5.8 Current /potential regulatory burden (Government)

Existing controls on the export of LI systems and network infrastructure via category 5A002 on 'cryptography' appear to be enforced through the use of all types of licences available in the Dual-use Regulation: general, global and individual licences.

Depending on how they are drafted and implemented, the introduction of expanded controls on monitoring centres could create an increased regulatory burden for governments.

7.5.9 Current /potential regulatory burden (Industry)

Two of the companies that provided responses to the SIPRI/Ecorys questionnaire identified themselves as suppliers of 'Lawful Intercept data retention and mediation'. Both companies stated that the type of licence that they most often used in the last 5 years was a general licence.

A number of companies that produce different types of LI systems have ICPs in place. Ericsson's Sales Compliance Board brings together different departments to assess the human rights issues associated with a particular sale.[294] The Board can approve or reject deals or make them subject to conditional approval.[295] Ericsson has also conducted a series of in-depth human rights impact assessments on particular markets. To date, impact assessments have been carried out for Iran, Myanmar and Sudan.[296]

Depending on how they are drafted and implemented, the introduction of expanded controls on monitoring centres could create an increased regulatory burden for industry.

Germany has assessed that its expanded controls on 'data retention' systems will have a limited effect on the German economy. This is in spite of the fact that Germany is one of the EU Member States with the most companies active in this area.[297] Germany argues that the controls only affect a small group of companies—most of which are

[293] Steve Stecklow, 'Special Report: Chinese Firm Helps Iran Spy on Citizens', *Reuters*, 22 Mar. 2012, <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322>.
[294] Lucy Purdon, 'Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study – Ericsson' (IHRB, 16 Nov. 2014), <http://www.ihrb.org/publications/reports/human-rights-challenges-for-telecommunications-vendors.html>.
[295] Ibid.
[296] Ericsson representative, Interview with the author, 4 May 2015.
[297] Catherine Stupp, 'Germany Leaves Brussels behind on Surveillance Tech Export Controls', EurActiv, 10 July 2015, <http://www.euractiv.com/sections/infosociety/germany-leaves-brussels-behind-surveillance-tech-export-controls-316226>.

already subject to export controls—and will provide greater clarity regarding their responsibilities in this area.[298]

One industry representative noted that introducing expanded controls on LI systems, particularly systems that that have a 'mediation function' would potentially impact exports of communications networks. The majority of communications networks include an LI system with a 'mediation function' installed by either the network manufacturer or another company.[299] If EU Member States were to apply standards relating to human rights or human security when assessing applications for these licences, it would place EU-based suppliers at a competitive disadvantage.[300]

7.6 Biometrics

7.6.1 Brief description of the technology

Biometrics is an automated technique for recognising 'individuals based on their biological and behavioural characteristic'.[301] Biometric systems include a large spectrum of technologies, in which an individual's unique identifiable attributes are used for authentication or identification purposes. Biometric systems can be sorted in to four categories based on the type of attribute used: visual; auditory; chemical; olfactory; or behavioural (see Table 7.9).

Biometric systems employ different recognition techniques depending on the particular features that are analysed. However, they commonly employ the following steps: (a) scanning; (b) digitalizing; and (c) matching. *Scanning* is the process by which the system identifies a pattern as it scans and isolates a specific set of physical or behavioural features. *Digitalizing* is the phase through which these features are converted into a digital template using an algorithm.[302] *Matching* is the process by which the digital template is checked against one or more databases (e.g. flight records, record of convicted criminals) or samples (e.g. a biometric ID-card or a biometric passport). This is done via the use of a pre-defined algorithm, which produces a score indicating the closeness of the match. Depending on the sensitivity of the systems, false negative (i.e. rejection of authorized individuals) and false positive (i.e. false identification of individuals) may occur.[303]

[298] BMWI, 'Verordnung der Bundesregierung Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung [Regulation of the Federal Government Fourth Regulation amending the Foreign Trade Regulations]', 17 July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.
[299] Industry representative, interview with the author.
[300] Ibid.
[301] Definition of the International Standardisation Organisation (ISO).
[302] Zureck, E. And Hindle, K.,'Governance, Security and Technology: The Case of Biometrics', *Studies in Political Economy,* Vol. 73, Spring/Summer 2004, pp.113-137.
[303] Coroama, V., *et al.* 'Emerging smart surveillance technologies', in Friedenwald, M. and Bellanova, R.,*Smart Surveillance – State of the Art*, SAPRIENT Project, Delivrable 1.1.p.35.

Table 7.9. Typology of biometric solutions

Type	Sub-type	Description
Visual recognition	Ear	Analysis of the shape of the ear
	Eye – Iris	Analysis of the feature found in the iris
	Eye – Retina	Analysis of the veins in the back of the eye
	Face	Analysis of the facial features or patterns
	Fingerprint	Analysis of the ridges and valleys found on the surface tips of a human finger
	Hand	Analysis of the geometric features of the hand, e.g. lengths, width
	Vein	Analysis of the vein patterns in the human finger or palm
Auditory recognition	Voice[304]	Identification and verification based on voice matching
Chemical recognition	DNA	Analysis of segments from DNA
Olfactory recognition	Odour	Analysis of individuals' odours
Behavioural recognition	Signature	Analysis of handwriting style
	Typing	Analysis of typing patterns
	Gait	Analysis of walking style or gait

Source: Biometrics institute

[304] Voice recognition should not be confused with speech recognition. Speech recognition is about *what is being said.* Voice recognition is about *who says it.* Voice recognition is sometime classified as a sub-type of behavioural recognition.

Biometric systems are primarily used for *authentication* purposes: to verify the identity of individuals seeking to access restricted things or items (e.g. phones, computers or databases), services (e.g. healthcare, bank accounts or public transport) or areas (e.g. planes or buildings). In that case, the individual's biometric pattern is checked against the ones contained in a record or a sample. Biometric systems can also be used for *identification* purposes: to identify 'unknown' people in the context of a criminal investigation and/or for intelligence purposes.

However the underlying technology used in *authentication* and *identification* systems is fundamentally the same. The main distinction is with the databases used for matching digital templates and the conditions under which scanning occurs. Hence, *authentication* systems will compare templates against a database of authorised individuals and scanning will occur in a controlled environment. However, *identification* systems will compare templates against one or more databases of known individuals and scanning will occur in an uncontrolled environment.

The global biometrics industry is growing significantly, driven by demand for both authentication and identification systems. According to the Biometric Research Group, the global market for biometric systems was worth around $7 billion in 2012 and is expected to be worth $15 billion in 2015.[305] Fingerprint based systems accounted for $5 billion of the market in 2012 and are expected to account for $10 billion in 2015, while face, iris, vein and voice recognition-based systems accounted for $2 billion of the market in 2010 and are expected to account for $5 billion in 2015.

In a broad sense, all biometric systems can be considered 'cyber surveillance' technologies, in that they rely on digital computing to capture biometric attributes and computer databases to store, manage, identify or verify biometric templates. However, in a narrow sense, only systems that focus on attributes that can be verified using cyber-related tools and which are used for *identification* purposes can be considered cyber-surveillance technologies. This would include systems that focus on verifying face, voice, gait or typing recognition via communications data.

However, even this narrower range of biometric systems includes both surveillance and non-surveillance technologies. For example, facial recognition systems for the *identification* of 'unknown' people are widely used in non-surveillance commercial products, including social media and picture management programmes.[306]

7.6.2 How it is captured by export control

Biometric systems are not covered by either the Wassenaar Arrangement or the EU dual-use control lists. Discussions about adding certain biometric systems to the Wassenaar Arrangement dual-use control lists have taken place in recent years but it is unclear which systems have been proposed for inclusion or the current state of these discussions.

[305] Biometric Research Group's website: <http://www.biometricupdate.com/research>.
[306] Robert, J., 'Who owns your face, Weak laws give power to Facebook', *Fortune,* 17 June 2015, <http://fortune.com/2015/06/17/facebook-moments-privacy-facial-recognition/>.

In the United States, certain biometric systems are subject to export controls as part of US restrictions on transfers of 'crime control and detection items' covered by Section 6(n) of the Export Administration Act of 1979, as amended (EAA).[307] US restrictions on crime control and detection items were introduced to support US foreign and human rights policy.[308] The United States denies all licences for the export of crime control and detection items to any state where the government 'engages in a consistent pattern of violations of internationally recognized human rights'.[309] All other licence applications are assessed on a case-by-case basis.[310]

US controls on biometric systems cover voice recognition systems (ECCN 3A980) and fingerprint recognition systems (ECCN 3A981).[311] The controls cover equipment, components and associated software, including fingerprint matching algorithms and voice analysis programmes. The controls apply to all destinations, except Australia, Japan, New Zealand and members of the North Atlantic Treaty Organization (NATO). EU-based companies wishing to re-export these technologies may also be subject to restrictions due to US re-export controls.

Iris recognition and facial recognition systems are not covered by US export controls, despite the fact they may also be misused to track and single out political or religious dissidents.[312] Discussions on adding them to the control list were initiated in 2008 when the United States sought public comment on how the crime control regulations should be changed.[313] The comments collected suggested that these systems should be included, but also that control should be reduced on items with wide commercial use (such as fingerprint powder). The United States published some revisions to the crime control regulations in 2009 but these did not include additional controls on facial and iris recognition systems.[314]

[307] Tim Maurer, 'Exporting the Right to Privacy', *Slate*, 15 May 2014, <http://www.slate.com/articles/technology/future_tense/2014/05/wassenaar_arrangement_u_s_export_control_reform_keeping_surveillance_tech.html>.

[308] They are intended 'to deter the development of a consistent pattern of human rights abuses, distance the United States from such abuses and avoid contributing to civil disorder in a country or region'. 2015 Report on Foreign Policy Based Export Controls, <https://www.bis.doc.gov/index.../1182-bis-2015-foreign-policy-report>.

[309]Ibid.

[310]Ibid.

[311] Kline, R., 'The rules of exporting biometrics outside the U.S.', *Secureidnews.com*, 29 July 2008, <http://www.secureidnews.com/news-item/the-rules-on-exporting-biometrics-outside-the-us/>*;* and BIS, 'Commerce Control List, Supplment no1 to Part 774 Category 3 – Electronics', last modified 13 July 2015, <http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

[312] Kline, R., 'The rules of exporting biometrics outside the U.S.', *Secureidnews.com*, 29 July 2008, <http://www.secureidnews.com/news-item/the-rules-on-exporting-biometrics-outside-the-us/>.

[313]Ibid; and 2010 Report on Foreign Policy Based Export Controls, <https://www.bis.doc.gov/index.php/forms-documents/doc_view/651-bis-foreign-policy-report-2010>.

[314] 2010 Report on Foreign Policy Based Export Controls, <https://www.bis.doc.gov/index.php/forms-documents/doc_view/651-bis-foreign-policy-report-2010>.

7.6.3 Human rights concerns

The study was unable to find any documented cases of biometric systems exported from an EU Member State being directly connected to violations of human rights.

However, the use of biometric systems raises concerns regarding potential violations of the following:

- Right to privacy;
- Freedom of association;
- Freedom from arbitrary arrest and detention; and
- Freedom for torture, inhuman treatment and degrading treatment.

Concerns are mainly focused on biometric systems that are designed for *identification*, rather than *authentication,* and primarily relate to potential violations of the right to privacy and its underlying principles, particularly the right to anonymity and the right to secrecy over personal information.[315] For example, people who desire to remain anonymous in a particular situation could be denied their privacy by biometric recognition. In addition, biometric systems can reveal sensitive medical information that could be the basis for systemic discrimination against segments of the population.

Concerns have also been raised about the use of certain biometric systems in connection with more serious human right abuses. In particular, voice and facial recognition systems could be used by authoritarian regimes to identify political opponents. These concerns are reinforced by the fact that biometric recognition methods are not equally mature and therefore not equally reliable. Facial recognition is reportedly not very effective in 'uncontrolled environments' such as crowds, and may lead to false identification.[316] Innocent people could consequently be arrested or abusively monitored by law enforcement or intelligence agencies.

There are currently no international standards on how personal information collected via biometrics technologies can be used and shared.[317] In the EU, citizens are protected since 1995 by the directive 95/45/EC on personal data protection. However, this directive does not apply to travellers and migrants who enter the EU. The latter

[315] Prabhakar, S; Pankanti, S., Jain, A.K., 'Biometric recognition: security and privacy concerns', *Security and Privacy*, IEEE, Vol.1, N°2, pp.33-42; and Campisi, P., 'Security and Privacy in Biomerics:Toward an Holitics Approach', *in* Campisi, P. (ed.), *Security and Privacy in Biometrics,* Springer: London, 2013, pp.6-7.

[316] Coroama, V., *et al.* 'Emerging smart surveillance technologies', in Friedenwald, M. and Bellanova, R.,*Smart Surveillance – State of the Art*, SAPRIENT Project, Delivrable 1.1.p.38; and Kreiss, R, 'the effectivness of surveillance in preventing and detecting crime and terrorism', in Trilateral Reserach and Consulting, *Surveillance, Fighting crime and violence,* IRISS project, Delivrable 1.1. 2012 pp. 182-183.

[317] Ceyhan, A., 'Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitude', *Cultures et Conflits,* n°64, 2006, p.33-47; and Rules, J., 'Needs for surveillance and the movement to protect privacy', in K.Ball, and D. Lyon, *Routledge Handbook of Surveillance Studies,* (London : Routledge, 2012).

have no legal guarantees on how their personal biometric data is handled by border agencies in the EU.

7.6.4 Security concerns

The study was unable to find any documented cases of biometric systems supplied by companies based in EU Member States being used in ways that pose a threat to EU or EU Member State security.

There is a range of scenarios in which biometric systems could be used to threaten international or EU security. These include:

- theft of government secrets; and
- theft of commercial secrets.

However, concerns are mainly focused on biometric systems that are designed for *authentication* rather than *identification,* and particularly the theft of biometric records and their use in gaining access to restricted items or areas.[318] Despite these concerns, the Biometrics Institute has stated that it is almost impossible to use stolen biometric records in this way.[319]

7.6.5 Use and governance in EU Member States

Biometrics systems are widely used by EU Member States, EU-based companies and the EU itself for both authentication and identification purposes.

EU Member States use iris, fingerprint and facial recognition-based systems for authentication purposes, such as border controls, while public authorities and private companies use them for protecting sensitive sites and properties.[320] EU Member States use fingerprint and DNA-based systems for identification purposes, such as identifying suspects in criminal investigations and tracking undocumented migrants.[321]

[318] For example, in 2006, a contract worker at the Israeli Welfare Ministry reportedly stole and re-sold Israel's primary biometric dataset, which contained personal information on 9 million Israelis. The stolen records were later connected to cases of identity theft and fraud. Ungerleider, N., 'The dark side of biometrics: 9 million Israelis hacked hit the web', *Fast Company,* 24 Oct. 2011, <http://www.fastcompany.com/1790444/dark-side-biometrics-9-million-israelis-hacked-info-hits-web>.

[319] Biometric Institute, FAQ 6 Is Theft of a biometric possible', <http://www.biometricsinstitute.org/pages/faq-6.html>.

[320] Goldstein, J *et al.,* 'Large scale biometrics deployment in Europe: Identifying challenge and threats', JRC Scientific and Technical Report, Office for Official Publication of the European Communities, Luxembourg, 2008, p.16, <http://www.a-sit.at/pdfs/biometrics_report.pdf>.

[321] For example, the EURODAC database allows EU Member States to compare fingerprint records against those taken in other EU Member States when assessing asylum applications or conducting serious crime or terrorism-related investigations. 'Identification of applicants (EURODAC)', European Commission, 23 June 2015, <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm>.

The use of voice recognition, facial recognition and behavioural-based systems in EU Member States for either authentication or identification purposes is poorly documented, most likely because they remain comparatively niche technologies.[322]

Through its research programmes the EU has funded and is funding a number of projects aimed at expanding capabilities in these areas. For example, HUMABIO (funded by FP6) focused on developing behavioural-based systems for authentication purposes.[323] BIO-DISTANCE (funded by FP7) focused on developing facial and iris recognition based systems for use 'on the move' and at distance.[324] ADABTS (funded by FP7) focused on developing behavioural-based systems for identifying threatening behaviour in crowded spaces. Finally, StillnoFace (funded by Horizon 2020) is focused on recognising individuals in pictures without relying on facial recognition.[325]

EU funding for biometric systems has aroused concern on the basis that due attention has not been paid to their potential ethical implications.[326] The EU has produced guidelines aimed at helping applicants assess the ethical implications of their projects and to help EU officials avoid funding projects with potentially negative implications.[327] The scenarios that the guidelines aim to avoid include funding 'the development of social, behavioural or genetic profiling technologies that could be misapplied for stigmatisation, discrimination, harassment or intimidation'. [328]

7.6.6 Producer companies in the EU

A significant number of EU-based companies produce different types of biometric systems, a number of which are market leaders. For example, Morpho (France) produces most types of biometric systems and claims to be the global leader in at least two sub-sectors: ID documentation (that includes biometrics) and automated fingerprint, iris and facial recognition-based systems.

Most EU-based companies that are active in this sector produce biometric systems for authentication purposes. These include: Delaney (UK); Easy Secure (Netherlands); Fingerprint Card (Sweden); Human Recognition Systems (UK); I.evo (UK); and Simply

[322] Goldstein, J *et al.*, 'Large scale biometrics deployment in Europe: Identifying challenge and threats', JRC Scientific and Technical Report, Office for Official Publication of the European Communities, Luxembourg, 2008, pp.17 <http://www.a-sit.at/pdfs/biometrics_report.pdf>.
[323] European Commission Community Research and Development Information Service, HUMABIO, <http://cordis.europa.eu/project/rcn/78373_en.html>.
[324] European Commission Community Research and Development Information Service, Bio-DISTANCE, <http://cordis.europa.eu/result/rcn/146958_en.html>.
[325] European Commission Community Research and Development Information Service, StillNoFace, <http://cordis.europa.eu/project/rcn/195218_en.html>.
[326] Muller, B., *Security, Risk and the Biometric State*, (New-York, Routledge, 2010), p. 150.
[327] European Commission, Research and Innovation Particpant Portal, Disaster Resilience: Safeguarding and Securing Society, Including Adapting to Climate Change, 'Explanatory note on potential misuse of research', <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-drs-2015.html#tab2>, Accessed 4 Aug. 2015.
[328] European Commission, Research and Innovation Particpant Portal, Disaster Resilience: Safeguarding and Securing Society, Including Adapting to Climate Change, 'Explanatory note on potential misuse of research', <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-drs-2015.html#tab2>, Accessed 4 Aug. 2015.

Biometrics (UK). However, several companies produce biometric systems for both authentication and verification purposes. These include: Cognitec (Germany); and Vision-box (Portugal).

A number of companies produce different types of biometric systems as part of a wider suite of surveillance or security technologies. These include Ganetec (Spain); Phonexia (Czech Republic); Global Security (UK); Elaman (Germany); and BAE Systems (UK). Only a small number of these companies report their revenues, profit and number of employees, indicating that they are SMEs (See Table 7.10). However, there are also a number of larger defence companies, including BAE Systems and Morpho, that are active in the sector.

Table 7.10. EU-based manufacturers of biometric systems

Company	Location	Type	Revenue (2013)	Profit (2013)	Employment (2013)
A.i. Solve	UK	Voice / Facial	-	-	-
Acustek	Ireland	Voice	-	-	-
Adatis Gmbh	Germany	Misc.	-	-	-
Agnito	Spain	Voice	-	-	32
Allevate	UK	Facial	-	<£1 m.	-
Artec Technologies AG	Germany	Face	€2 m.	-	-
Aurora	UK	Facial	-	-	-
BAE Systems	UK	Misc.	$28 000 m.	$275 m.	84 600
Behaviometrics AB	Sweden	Typing	SEK4 m.	SEK3 m.	8
Cognitec	Germany	Facial	-	<€1 m.	60
Delarney Secure	UK	Misc.	-	-	-
Digital barriers [a]	UK	Facial	£19 m.	£15 m.	150
Easy Secure International	The Netherlands	Finger / Face	-	-	-

Company	Location	Type	Revenue (2013)	Profit (2013)	Employment (2013)
Elaman	Germany / Switzerland	Voice	-	<€1 m.	-
Face Phi	Spain	Facial	-	-	18
Facebanx	UK	Facial	-	<£1 m.	15
Fingerprint Cards	Sweden	Fingers	SEK34 m.	SEK15 m.	-
Gamma Group	Germany / UK	Facial	-	<$1 m.	-
Ganetec	Spain	Facial	-	-	20
Gewnkey Solutions BV [b]	The Netherlands	Misc.	-	-	10
Global Security	UK	Finger	-	-	-
GR Sistemi	Italy	Facial / Voice	-	-	>100
Herta Security	Spain	Facial	-	-	-
Human Recognition system	UK	Misc.	-	-	
i-Evo	UK	Finger.	-	-	20
Morpho (SAFRAN)	France	Misc.	€1 500 m.	.	8 600
Net-X Solutions	UK	Facial	-	<£1 m.	-
Neurotechnology	Lithuania	Facial	-	-	-
Next Biometrics Group	Norway	Finger	NOK38 m.	NOK39 m.	20
Phonexia	Czech Rep.	Voice	-	-	-
Probaye	France	Typing	€1 m.	<€1 m.	22
Sail Labs Tech.	Austria	Voice / Typing	-	-	20

Company	Location	Type	Revenue (2013)	Profit (2013)	Employment (2013)
Secure Info. Management	Germany	Voice	-	<€1 m.	-
Semlex Group	Belgium	Misc.	-	-	-
Simply Biometrics	UK	Misc.	-	-	-
Spikenet Technology	France	Facial	<€1 m.	<€1 m.	17
TM3 Software (Keytrac)	Germany	Typing	-	<€1 m.	-
TraceTag International	UK	DNA	-	-	-
Unamic	Spain	Facial	-	-	-
Vicorp	UK	Voice	-	-	-
Vision-Box	Portugal	Misc	-	-	-
Vocapia	France	Speech	-	-	<9

a. 2014 data
b. 2012 data

7.6.7 Producer companies outside the EU

A significant number of companies based outside the EU produce biometric systems. Of these companies, the two largest are 3M (US) and NEC (US), although neither company has biometrics as a core business.[329] Many of the remaining companies are 'pure players', producing biometric systems for both authentication and identification purposes. These include Aware Inc. (USA); M2SYS LLC (USA) Animetrics Inc (USA); Cross March Technologies (USA); Suprema Inc. (USA); TBS (Switzerland); Iritech (USA); HID (USA); and Verisis (Turkey).

A number of companies produce different types of biometric systems as part of a wider suite of surveillance or security technologies. These include: Defentek (USA); Kommlabs (India); and Nice Systems (Israel/USA). For example, Nice Systems'

[329] 3M acquired the UK biometrics provider Cogent in 2010. It now sells a wide spectrum of biometrics products and services including to the military and law enforcement agencies (mobile identification tools, scanners and document readers). NEC's biometric offering is also very wide; it includes mobile fingerprint scanners, software for biometric identification, face recognition, databases and mobile ID verification devices.

produce Track Horizon Insight, an intelligence platform for mass interception and analysis that includes voice-based recognition systems.[330]

7.6.8 Current / potential regulatory burden (Government and Industry)

Depending on how they are drafted and implemented, the introduction of controls on biometric systems could make a significant range of non-surveillance biometric systems subject to export controls. This would be particularly true of controls that focused only on the technical specifications of the system rather than its intended end-use. This, in turn, could create an increased regulatory burden for both governments and industry.

The US regularly assesses the economic impact of its restrictions on transfers of 'crime control and detection items' and has concluded that the effect has been minimal. In fiscal year 2014, the Department of Commerce approved 4,552 export licence applications for 'crime control and detection items', worth over $1.1 billion. 136 applications were denied, worth over $124 million. [331]

However some US providers of biometrics solutions argue that US export controls have had an impact on their business and particularly their ability to access the Chinese market. In response to a US request for public comments on these controls Cross Match Technologies (USA) also questioned the relevance of denying licences for biometric technologies to China given the lack of a clear connection 'between human rights abuses in China and the use of biometric technology for crime control'.[332]

7.7 Impact of the implementation of export controls on cyber-surveillance technologies

Given the variety of technologies involved, it is clearly problematic to try and draw clear conclusions about the economic, social (including security) and environmental impacts associated with the implementation of export controls on cyber-surveillance technologies. In addition, as many stakeholders noted, several of these controls—particularly those on intrusion software and IP Networks—were only introduced at the EU level in 2014, so it is somewhat premature to make a detailed assessment of their impact.

Nonetheless, the following sub-section presents some broad conclusions based on the findings of the case studies and consultations with stakeholders via the interviews and questionnaires.

7.7.1 Economic impact

As with all areas of the 'dual-use industry', the regulatory burden for companies associated with export controls on cyber-surveillance technologies differs significantly

[330] NiceTrack Horizon insight, brochure available at: <https://www.documentcloud.org/documents/815869-996-nice-systems-brochure-nicetrack-horizon.html>.

[331] US State Department, '2015 Report on Foreign Policy Based Export Controls', <https://www.bis.doc.gov/index.../1182-bis-2015-foreign-policy-report>.

[332] Ibid.

from company to company. Stakeholders noted that larger companies with longstanding experience in export controls face fewer difficulties with compliance. In contrast, SMEs may face problems, particularly if they have less experience with export controls, are producing cyber-surveillance technologies that are closely associated with human rights and/or security concerns, and are engaged in supplying markets in less stable parts of the world.

The regulatory burden for companies also varies depending on the manner in which the controls on cyber-surveillance technologies are enforced by the state's licensing authority. This will include whether the licensing authority is enforcing the controls via an individual or general licences, whether they are more or less likely to approve a particular sale, and whether they are in a position to give a clear and binding advance indication of which markets and customers are acceptable.

Interestingly, the economic impact of export controls in this area can be less to do with risks of having licences denied and more to do with the sensitivities associated with supply items that are subject to export controls. One industry representative noted that the most serious problem that companies face in terms of compliance costs do not relate to the time and effort involved in preparing licence applications, but rather the 'friction' generated by the application of export controls.[333] In particular the process of requiring customers to sign and comply with EUCs can have a chilling effect on the search for new business.[334]

A number of stakeholders pointed to reports that companies were leaving the EU in response to the recent expansion of controls on cyber-surveillance technologies. However, this study was only able to identify two relatively clear cases where this has happened. One UK Government official noted that although there were rumours circulating about companies leaving Europe to escape new export controls on surveillance technologies, there was no evidence that any had actually done so.[335] In addition, many of the products involved were already subject to export controls due to the level of cryptography they contained, and so the introduction of new controls would not lead to a significant additional regulatory burden.[336] Sarah A. McKune of Citizen Lab noted that the arguments about relocation should not be overstated.[337] Many companies would face costs associated with moving outside the EU that would prevent them from moving.

As discussed, concerns have been raised about the unintended side effects of this particular set of controls on intrusion software (see 7.3 Intrusion Software). To date, the concrete economic impact upon companies, researchers and academics working in IT security that believe they are subject to these controls is hard to quantify. None of the officials interviewed said they had received any licence applications from companies, researchers and academics working in IT security and several noted that

[333] Industry representative, Interview with the author.
[334] Ibid.
[335] UK Department of Business, Innovation and Skills official, Interview with the author, 28 Apr. 2015.
[336] Ibid.
[337] Sarah A. McKune, Citizen Lab, Interview with the author, 2 July 2015.

they did not view their activities and transactions as being covered by the controls on intrusion software. However, if companies, researchers and academics working in IT security do end up being covered by the controls—or even if a misconception takes hold that they are covered—it could have long-term economic and even security implications.

As with all areas of the 'dual-use industry', the regulatory burden for licensing authorities associated with the implementation of controls on cyber-surveillance technologies differ significantly between Member States. Among the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, resources spent processing licences for the export of cyber-surveillance technologies during 2014-15 in FTE ranged from 0 in 2 EU Member States to 6 in 2 EU Member States.

The level of regulatory burden will depend on the number of affected companies located in the EU Member State and the number of licence applications received, both of which vary significantly, as they do in many areas of dual-use export controls. Of the ten EU Member States that responded to the questionnaire, 6 indicated that 0-10 companies producing cyber-surveillance technologies were based in their territory and 1 indicated that there were 11-25. The rest stated that they did not know. 6 EU Member States indicated that exports of cyber-surveillance technologies accounted for 0-5 per cent of total dual-use exports and 1 stated that they represented more than 5 per cent. The rest stated that they did not know. Two EU member states said that they received no licence applications for the export of cyber-surveillance technologies during 2014-2015 while one said that it had received more than 50.

The amount of regulatory burden generated by the implementation of controls on cyber-surveillance technologies will also depend upon the systems that states have for assessing applications and how much time they take to implement. In Germany, licences for the export of surveillance technologies are, in principle, assessed at an inter-ministerial clearing-house.[338]

Of the ten EU Member States that responded to the questionnaire, 6 noted that the enforcement of controls on cyber-surveillance technologies presented particular challenges. Challenges highlighted by EU Member States included the identification of relevant items by customs; distinguishing between mainstream equipment with legitimate purposes and the subset of items that pose a threat; ensuing that a company respects any conditions attached to an export licence; identifying companies that supply non-tangible technologies or training; and obtaining information about the end-user.

The need to carry out industry outreach, often to companies that did not previously have any experience with export controls was also highlighted as a regulatory burden attached to the implementation of these controls. Of the ten EU Member States that responded to the questionnaire, 9 have carried out company visits in connection with the implementation of controls cyber-surveillance technologies and 4 have held industry workshops. One EU Member State official noted that industry outreach had

[338] Germany government official, Interview with the author, 17 April 2015

been a difficult process when it came to the implementation of new controls on cyber-surveillance technologies.[339] Although there is a national association representing the 'surveillance sector' it had refused to meet with the representative of the export licensing authority.[340]

7.7.2 Social impact (including human rights and security)

The human rights and security benefits of imposing controls on exports of cyber-surveillance technologies are naturally hard to quantify. As demonstrated, there are clear cases where cyber-surveillance technologies supplied by EU-based companies have been directly implicated in serious violations of human rights. In addition, there are a wide range of human rights and security concerns associated with the export and use of all of these systems.

Available information indicates that human rights concerns are more central than security concerns when states are deciding whether to approve licences for the export of cyber-surveillance technologies. Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, 6 indicated that 'Criterion 2: Respect for Human Rights' was among the criteria that most frequently results in denials of licences for the export of cyber-surveillance technologies. Only one indicated that 'Criterion 5: National Security of Member States and Allies' was among these criteria.[341]

About half of the respondents to the SIPRI/Ecorys company survey that identified themselves as suppliers of cyber-surveillance technologies indicated that they are aware that exports of these technologies from the EU and from third countries may pose a threat in terms of security or pose a risk of human rights violations.

A number of stakeholders pointed to the high level of 'replaceability' that exists with regards to many types of cyber-surveillance technologies and the implications this have for the amount of amount of impact that EU Member States controls on cyber-surveillance technologies is likely to have. EU-based companies appear to have a strong lead in certain parts of the cyber-surveillance sector – particularly the production of high-performance intrusion software - but this may not be the case for long. Moreover, in other areas, such as monitoring centres, the range of supplier companies based outside both the EU and the Wassenaar Arrangement appears to be expanding. Other stakeholders played down the level of competition in the sector. Sarah A. McKune of Citizen Lab noted that repressive regimes continue to use cyber-surveillance technologies produced by EU-based companies. This highlights both Europe's technological advantages in this area and the potential for EU-based controls to have a positive impact.[342]

[339] EU Member State official, interview with the author.

[340] Ibid.

[341] Three EU member states indicated that 'Criterion 1: Respect for International Obligations' was among these criteria, 2 indicated that 'Criterion 7: Risk of Diversion' or re-export was among the criteria, one indicated that 'Criterion 3: Internal Situation' was among these criteria.

[342] Sarah A. McKune, Citizen Lab, Interview with the author, 2 July 2015.

Other stakeholders noted the potential negative implications upon security that could be associated with implementation of controls in this area. One industry representative noted that if cyber-surveillance companies leave Europe it could mean that EU Member States would lose the ability to cooperate with the intelligence agencies of states in other parts of the world, particularly in Africa and the Middle East.[343] These channels provide both a means of sharing intelligence but also influencing and improving the standards of the intelligence agencies in those states.[344]

Other stakeholders noted that the issue of human rights and security impacts should not just be thought of in terms of measureable outcomes but also in terms of alignment with EU values. As the recent European Parliament resolution noted, the application of stronger controls in this area is also about ensuring 'coherence between the EU's external actions and its internal policies related to ICTs.'[345]

7.7.3 Environmental impact

The study was unable to identify any environmental impacts associated with imposing controls on exports of cyber-surveillance technologies.

7.8 Implications of the review options for the 'cyber-surveillance sector'

Review option 4 covers the modernization of existing controls, including adding a new dimension for controlling exports of cyber-surveillance technologies. This could potentially involve any of the following:

- Applying criteria relating to human rights and international/EU security to exports of cyber-surveillance technologies;
- Introducing EU-wide industry self-regulation for producers of cyber-surveillance technologies;
- Introducing further multilaterally agreed list-based controls of cyber-surveillance technologies at the WA level;
- Introducing an EU definition or autonomous control list for cyber-surveillance technologies (via a technical or descriptive list); and
- Introducing an EU cyber-surveillance catch-all mechanism (via a dedicated catch-all for cyber-surveillance technologies or application of general catch-all).

[343] Industry representative, Interview with the author.

[344] Ibid.

[345] European Parliament, 'European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries (2014/2232(INI))', 8 Sep. 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0288&language=EN&ring=A8-2015-0178>.

This section presents a broader discussion about the different ways in which these review options could be implemented as well as stakeholder views on their potential impact based on the findings of the case studies and consultations via the interviews and questionnaires.

7.8.1 Applying criteria relating to human rights and international/EU security to exports of cyber-surveillance technologies

There are a range of human rights and security concerns associated with the export and use of cyber-surveillance technologies. Many of these concerns are reflected in EU policy documents while others are not.

Human rights concerns

The use of cyber-surveillance technologies has direct implications for:

- the right to privacy.

In particular, the use of most types of cyber-surveillance in states that lack effective laws and regulations governing their use will almost always represent a violation of the right to privacy. The use of cyber-surveillance technologies has also been directly or indirectly linked to abuses of other human rights by LEAs or intelligence agencies, including:

- freedom of expression;
- freedom of association;
- right to life;
- freedom from arbitrary arrest and detention; and
- freedom from torture and inhuman or degrading treatment.

These rights are enshrined in a number of international and regional instruments, including the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights.[346] Certain of these rights are considered inviolable while others may be suspended in certain restricted circumstances.

The right to privacy, freedom of expression and freedom of association may be restricted for certain legitimate reasons, including the protection of people's rights and national security, although only if the prescriptions are 'prescribed by law, legitimate, necessary and proportionate'.[347]

The right to life and to freedom from arbitrary arrest and detention 'must be protected from arbitrary or unlawful deprivation or interference by the State' and any restriction

[346] The Universal Declaration of Human Rights (UN), accessed 7 June 2015, <http://www.un.org/en/documents/udhr/>; and International Covenant on Civil and Political Rights (UN, n.d.), <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.
[347] 'Assessing Cyber Security Export Risks' (UK Government, 2015).

must be 'according to clear rules and processes set down in the law'.[348] The right to freedom from torture and inhuman or degrading treatment can never be limited or restricted.[349]

Relevant EU policies

There are multiple commitments under EU law to uphold—and avoid violations of—these rights. For example, the Charter of Fundamental Rights of the European Union enshrines, inter alia, the rights to privacy, freedom of expression and the protection of personal data.[350] Commitments have also been made to use EU policy instruments, including trade restrictions, to prevent abuses of the right to privacy, freedom of expression, or freedom of association, particularly in cyber-space.[351]

The EU has also made specific policy commitments to restrict exports of cyber-surveillance technologies that might be used in human rights violations. For example, the 2012, 'EU Strategic Framework and Action Plan on Human Rights and Democracy' stated that the EU would '(i)nclude human rights violations as one of the reasons following which non-listed items may be subject to export restrictions by Member States'.[352]

In 2014, these policies were further developed when the Council of the European Union adopted the 'EU Human Rights Guidelines on Freedom of Expression Online and Offline', which stated that the 'EU will promote action at the international level to prevent the sale of surveillance or censorship technology to authoritarian regimes'.[353]

Many of the human rights concerns associated with the export and use of cyber-surveillance technologies are already addressed in Council Common Position 2008/944/CFSP and the associated User's Guide, which provides guidance on its implementation.[354] In particular, Criterion 2 of Council Common Position 2008/944/CFSP requires Member States to deny an export licence if 'there is a clear risk that the military technology or equipment to be exported might be used for internal repression'. In addition, the User's Guide notes that

[348] Ibid.
[349] Ibid.
[350] 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.
[351] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, 'ICT for Democracy: Supporting a Global Current of Change', 8 Dec. 2011.
[352] 'EU Strategic Framework and Action Plan on Human Rights and Democracy', (Council of the European Union, 25 June 2012).
[353] 'EU Human Rights Guidelines on Freedom of Expression Online and Offline', (Council of the European Union, 12 May 2014).
[354] 'User's Guide to Council Common Position 2008/944/CFSP Defining Common Rules Governing the Control of Exports of Military Technology and Equipment', (Council of the European Union, 29 April 2009), <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209241%202009%20INIT>.

'communications/surveillance equipment can have a strong role in facilitating repression'.[355]

However, there are also limitations in terms of how the different human rights concerns associated with the export or use of cyber-surveillance technologies are addressed. For example in the guidance contained in the User's Guide on how to interpret criterion 2:

- The section on 'end-user' makes no mention of deliveries to private companies and emphasises that transfers to 'police or security forces' are the primary focus of concern and attention;[356]
- The section 'recipient country's attitude' make no direct mention of the legal and regulatory frameworks with regards to Lawful Interception, access to information or freedom of expression;[357] and
- The section on the recipient state's human rights standards make no direct mention of the legal and regulatory frameworks with regards to Lawful Interception, access to information or freedom of expression.[358]

Security concerns

The export and use of cyber-surveillance technologies have also raised concerns regarding potential violations of international or EU security. While documented cases of such violations are difficult to find, a number of potential threats have been highlighted, including:

- disruption or destruction of critical infrastructure;
- theft of military or WMD-related knowledge or technologies;
- theft of government secrets; and
- theft of commercial secrets.

Unlike for human rights, there are no international or regional standards that categorise and rank the different security risks associated with the export and use of cyber-surveillance technologies.[359]

Relevant EU policies

The EU Cyber-Security Strategy makes reference to the threats posed by cyber-attacks and cyber-crime and the need to improve coordination in the field of resilience

[355] Council of the European Union, User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, Brussels, 29 April 2009.
[356] Ibid.
[357] Ibid.
[358] Ibid.
[359] Ibid.

and response.[360] However, there is no specific discussion of the security issues concerned with the export of cyber-surveillance technologies.

Certain security concerns associated with the export and use of cyber-surveillance technologies are addressed in Council Common Position 2008/944/CFSP and the associated User's Guide.[361] In particular, Criterion 5 Council Common Position 2008/944/CFSP requires Member States to take into account 'the potential effect of the military technology or equipment to be exported on their defence and security interests as well as those of Member State and those of friendly and allied countries'.[362]

However, there are also limitations in terms of how the security concerns associated with the export of use of cyber-surveillance technologies are addressed. For example in the guidance contained in the User's Guide on how to interpret criterion 5:

- The section on 'nature of the equipment' emphasises that transfers of military goods are the primary focus of concern and attention;[363] and
- The text on 'National security' makes no reference to the risks associated with offensive cyber systems and/or attacks on critical infrastructure.[364]

Finally, the link between the EU Dual-use Regulation and the EU Common Position and the commitment to apply the criteria of the EU Common Position to all exports of dual-use goods is not entirely clear. Article 12 of the EU Dual-use Regulation requires Member States to take into account 'all relevant considerations' when assessing export and brokering licences for dual-use goods. These include: obligations under relevant export control regimes; EU, OSCE and UN sanctions; and 'considerations of national foreign and security policy, including those covered by Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment'.[365]

However, Article 6 of the EU Common Position states that exports of dual-use goods should be subject to assessment under the EU Common Position criteria, but only 'where there are serious grounds for believing that the end-user of such goods and technology will be the armed forces or internal security forces or similar entities in the

[360] 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (European Commission, 7 Feb. 2013).
[361] 'User's Guide to Council Common Position 2008/944/CFSP Defining Common Rules Governing the Control of Exports of Military Technology and Equipment', (Council of the European Union, 29 April 2009), <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209241%202009%20INIT>.
[362] 'Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335'.
[363] Council of the European Union, User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, Brussels, 29 April 2009.
[364] Ibid.
[365] 'Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items', (Official Journal of the European Union, 29 May, 2009).

recipient country.'[366] In many cases, the end-user for cyber-surveillance technologies is not 'the armed forces or internal security forces' but a privately run network operator.

Human security approach

One way to fill these gaps would be to apply a 'human security' approach to export controls for dual-use goods. According to the European Commission, this would potentially involve 'a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations'.[367]

The United Nations Development Programme (UNDP) coined the term 'human security' in 1994.[368] It was an attempt to broaden the notion of security, which was seen to be excessively focused on state security, to include a range of other components, including 'economic security, food security, health security, environmental security, personal security, community security and political security'.[369] The concept has reoriented and broadened numerous policy debates away from traditional notions of state security.[370] However, it is not legally binding and does not have a universally agreed definition.[371]

Certain industry associations have raised concerns about a shift to a 'human security' approach in export controls for dual-use goods. The AeroSpace and Defence Industries Association of Europe (ASD) has noted that '(t)he concept of "human security" would appear to take the Regulation in an entirely new direction with the possibility of unilaterally adding items to the control list that are not accepted internationally'.[372] Other industry representatives have argued that the adoption of any EU-specific human rights or human security standards with regards the export of cyber-surveillance technologies might place EU-based companies at a competitive disadvantage.

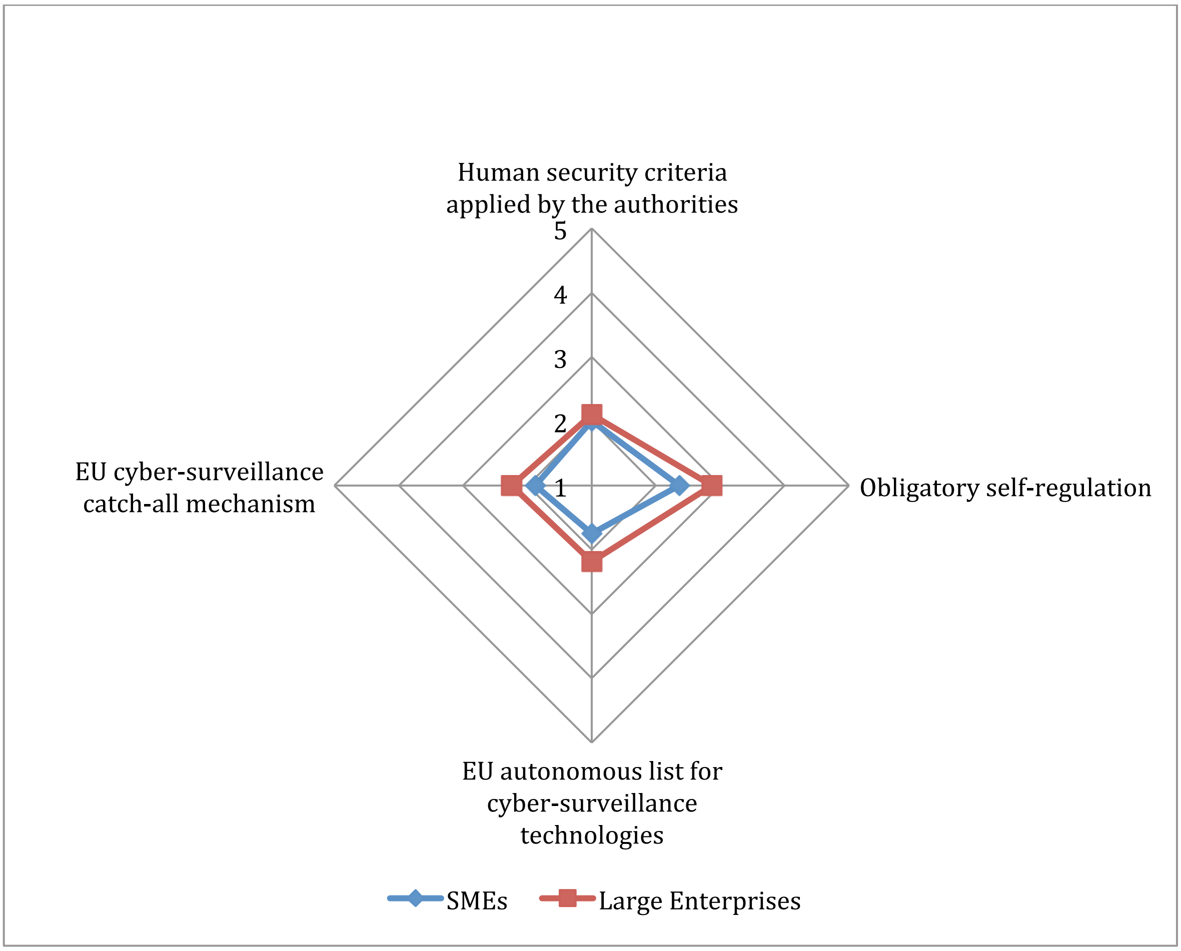
On average, respondents to the SIPRI/Ecorys company survey that identified themselves as suppliers of cyber-surveillance technologies indicated that the application of human security criteria to exports of cyber-surveillance technologies would have a negative impact on their exports, their compliance costs, their

[366] 'Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335', (Council of the European Union, 8 Dec. 2008).
[367] 'The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World', (European Commission, 24 Apr. 2014).
[368] UNDP, *Human Development Report 1994* (Oxford University Press, 1994), <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf>.
[369] Ibid.
[370] Carly Nyst, Privacy International, Correspondence with the author, 27 May 2015.
[371] Ibid. A recent report noted that '(h)uman security is a flexible approach and can be tailored to different contexts and topics, according to the specific context.' Oscar A. Gomez and Des Gasper, 'Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams', (UNDP, n.d.), <http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf>.
[372] 'ASD Position Paper on the Review of the Dual-Use Export Control System of the European Union', (ASD, 22 Oct. 2014).

investment and production, and the EU-wide level playing field (see Figure 7.3). The potential impact on compliance costs was thought to be particularly strong.

Some NGOs are also wary about the potential shift from a human rights to a human security based approach. The Coalition Against Unlawful Surveillance (CAUSE) have noted that '(t)here is a risk that adopting this intangible, and not legally binding concept may have unintended consequences'.[373] The concept of human rights is much better defined under international law and there is already a wide-ranging body of well-respected opinion by UN special rapporteurs as well as jurisprudence from international courts that have applied aspects of human rights law to the digital and surveillance spheres.[374]

Figure 7.3. Industry views on the impact of potential actions regarding export controls and cyber-surveillance technologies*



*1=very negative impact; 3=neutral; 5=very positive impact

Total respondents=18

[373] 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.
[374] Carly Nyst, Privacy International, Correspondence with the author, 27 May 2015.

Source: SIPRI/Ecorys company survey

Stakeholders also pointed to risks associated with expanding the range of human rights and security considerations that states take into account when assessing dual-use exports. In particular, such an expansion may generate calls for further additions to the range of items that are subject to control. For example, a wide range of goods and technologies raise concerns related to the right to privacy, freedom of expression, or freedom of association beyond cyber-surveillance technologies. These include Internet content filtering and blocking systems.

While many stakeholders questioned the application of a human security approach to the export of cyber-surveillance technologies, several emphasised the need for the EU to develop clearer guidelines on how licences for the export of these technologies should be assessed. Such guidelines would in turn, need to be based upon clearer standards relating to when and how cyber-surveillance technologies should be used by states. The EU has agreed standards in some of these areas, such as the use of Lawful Interception systems, but not others, such as the use of intrusion software and IMSI Catchers.

This would involve the EU developing: technical standards concerning the technical capabilities that cyber-surveillance technologies should have; legislative standards concerning the legal frameworks states should have in place for governing their; and practical standards concerning how these technologies are used in practice. As one industry representative noted, rather than banning exports, the EU should seek to host responsible suppliers of cyber-surveillance technologies that meet the legitimate needs of LEAs and intelligence agencies while supplying systems that are less open to abuse and providing training on responsible practices.[375]

In developing these standards, there is significant scope to share national guidelines and practices with regards to assessing exports of cyber-surveillance technologies.

For example, the UK Government has produced the ‘Overseas Security and Justice Assistance Guidance’.[376] The guidance applies to all government departments and focus on identifying and mitigating human rights risks associated with the provision of ‘physical, financial or information assistance to security and justice authorities overseas’. The UK Government has also developed OSJA guidance for cyber-related assistance but these are not publicly available.[377] In addition, when assessing any export licence applications the UK can request additional information from the applicant, including more detail about how an item might be used.[378] For example, for systems relating to Lawful Interception, this could include asking about how many

[375] Industry representative, Interview with the author.
[376] ‘Overseas Security and Justice Assistance Guidance’, (UK Government, 28 Feb. 2014), <https://www.gov.uk/government/publications/overseas-security-and-justice-assistance-osja-guidance>.
[377] UK Department of Business, Innovation and Skills official, Interview with the author, 28 April 2015.
[378] Ibid.

'hard selectors' a system is capable of using, which may help in assessing its utility in mass surveillance.[379]

7.8.2 Introducing EU-wide industry self-regulation for producers of cyber-surveillance technologies

The development of some form of industry self-regulation for producers of cyber-surveillance technologies has been proposed by a number of different commentators and experts. For example, in May 2012 the European Parliament adopted a non-legislative resolution calling on the European Commission to 'produce guidelines for EU companies to act in a manner consistent with the Union's fundamental principles in such situations'.[380]

On average, the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies indicated that introducing obligatory EU-wide self-regulation for producers of cyber-surveillance technologies would have a neutral impact on administrative costs, the EU-wide level playing field, and preventing transfers that might threaten international or EU security (see Figure 7.4). However, it would have a positive impact on preventing transfers that might result in human rights violations.

On average, respondents to the SIPRI/Ecorys company survey that identified themselves as suppliers of cyber-surveillance technologies indicated that the adoption of obligatory EU-wide self-regulation for producers of cyber-surveillance technologies would have a negative impact on their exports, their compliance costs, their investment and production, and the EU-wide level playing field (see Figure 7.3). However, the potential impact was viewed as being less negative than that associated with other review options in this area.

Stakeholders highlighted a number of points arguing in favour of introducing EU-wide self-regulation for producers of cyber-surveillance technologies.

First, sales of cyber-surveillance technologies often involve close cooperation between buyer and seller and continual processes of post-delivery support and maintenance.[381] This creates the possibility for exporting companies to have an understanding of how their systems will be used before export and how they are used after export, as well as the potential ability to deactivate them if agreed standards in human rights are not being implemented.[382]

[379] Ibid.

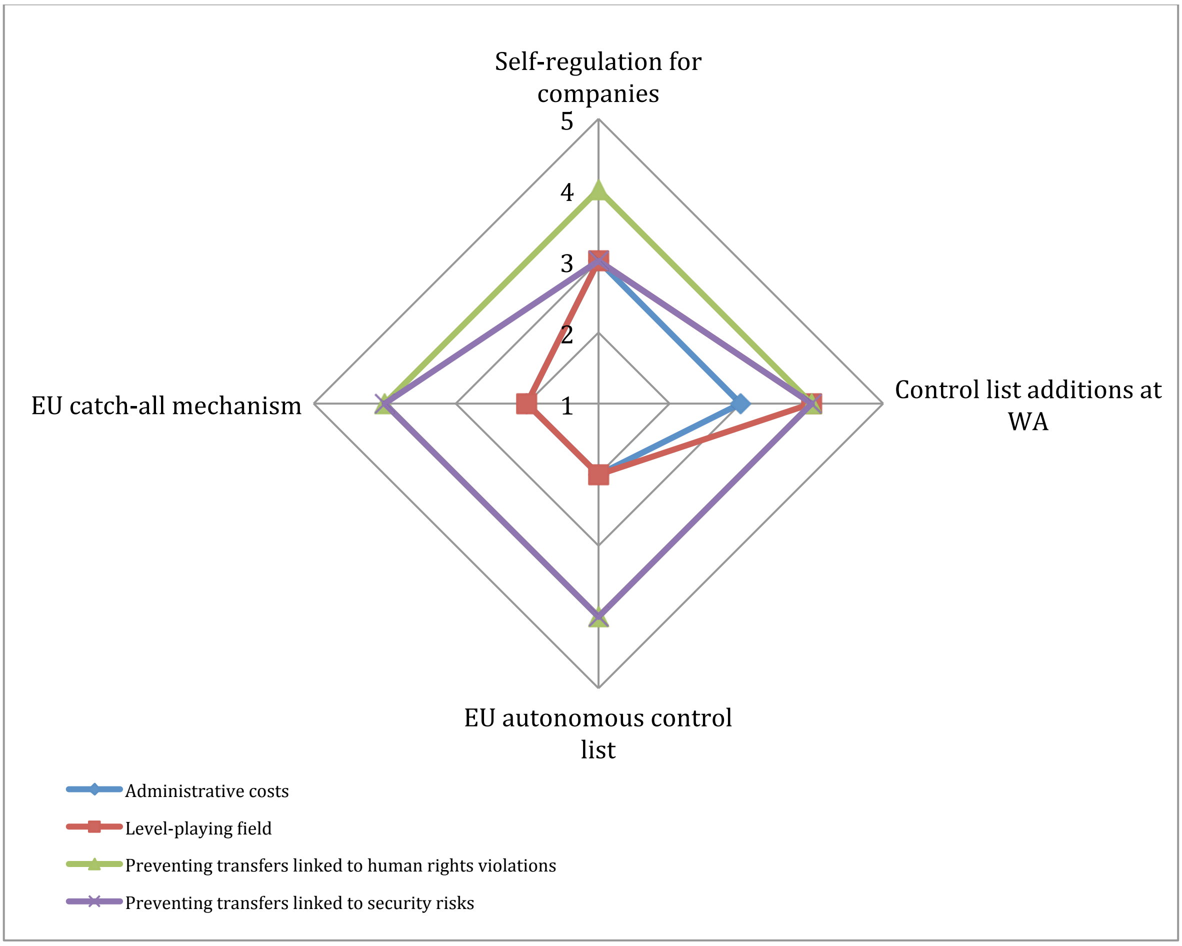
[380] European Parliament, 'Trade for change: the EU Trade and Investment Strategy for the Southern Mediterranean following the Arab Spring revolutions (2011/2113(INI))', Resolution, 10 May 2012, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0201+0+DOC+XML+V0//EN>.

[381] Cindy Cohn and Jillian York, ''Know Your Customer' Standards for Sales of Surveillance Equipment', (Electronic Frontier Foundation, 24 Oct. 2011), <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

[382] Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', (Access, 13 Mar. 2015), <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

Second, there is a range of good practice guidelines drafted by international organisations, governments and NGOs that could be utilised when developing standards for industry self-regulation. Examples include the 'Guiding Principles on Business and Human Rights' produced by the UN;[383] the 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' produced by the European Commission;[384] the '"Know Your Customer" Standards for Sales of Surveillance Equipment' produced by the Electronic Frontiers Foundation;[385] the

Figure 7.4. EU Member State's views on the impact of potential actions regarding export controls and cyber-surveillance technologies*



*1=very negative impact; 3=neutral; 5=very positive impact

Total respondents=10

Source: Questionnaire about controls on cyber-surveillance technologies

[383] 'Guiding Principles on Business and Human Rights', (UN Human Rights Council, June 2011), <http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf>.
[384] 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', (European Commission, June 2013).
[385] Cindy Cohn and Jillian York, ''Know Your Customer' Standards for Sales of Surveillance Equipment', (Electronic Frontier Foundation, 24 Oct. 2011),

guidelines for 'Assessing Cyber Security Export Risks' produced by Tech UK;[386] and the OECD Guidelines for Multinational Enterprises.[387] Several ICT companies have also developed their own due diligence policies. For example, Ericsson and Nokia have standards and practices for vetting potential sales opportunities that go beyond export control obligations and include a range of human rights concerns.[388]

Third, cyber-surveillance technologies involve the use of a wider range of technologies that have both surveillance and non-surveillance uses and which will always be hard to make subject to export controls. Sarah A. McKune of Citizen Lab noted that a range of technologies, such as Deep Packet Inspection (DPI), could be used for both quality of service and surveillance purposes, thereby underlining that export controls will never be a sufficient mechanism for tackling the problems raised by these technologies.[389] One key element of a more comprehensive approach is greater transparency from the companies involved, including the release of more information about the content of contracts with customers.[390]

However, stakeholders also noted a number of points that highlight the potential difficulties associated with introducing EU-wide self-regulation for producers of cyber-surveillance technologies. First, the range of companies involved in the production and export of cyber-surveillance technologies is wide. Unlike in other sectors—such as nuclear, chemical or defence—there are no EU or national industry associations that represents all of these companies and which could act as a coordinator for the development of standards for self-regulation.

Second, there are no agreed regional or international standards for the use of many cyber-surveillance technologies, which makes it difficult for companies to develop and implement ICPs. Since 2013 Hacking Team has taken steps to develop and implement an ICP (see 7.3 Intrusion software). However, following the theft and release of Hacking Team's internal emails, the content of their ICP was criticised on the grounds that it did not appear to be preventing the company from doing business with governments with 'controversial human rights records.'[391]

Third, while larger companies producing network infrastructure have developed and implemented ICPs, many SMEs have not. In many cases, these companies will be less willing and/or able to develop and implement due diligence policies due to the potential costs involved. Among respondents to the SIPRI/Ecorys company survey, SMEs thought that they would be negatively impacted by the introduction of obligatory

<https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

[386] 'Assessing Cyber Security Export Risks', (UK Government, 2015).

[387] OECD, OECD Guidelines for Multinational Enterprises, <http://www.oecd.org/corporate/mne/>.

[388] 'Nokia Human Rights Policy', (Nokia, 25 Feb. 2015), <http://company.nokia.com/sites/default/files/download/nokia_human_rights_policy_1.pdf>; and 'ICT and Human Rights: An Eco-System Approach', (Ericsson, 2012).

[389] Sarah A. McKune, Citizen Lab, Interview with the author, 2 July 2015.

[390] Ibid.

[391] James Lee, 'Hacking Team Leak Highlights the Need to Implement Human Rights Due Diligence', Tech UK, 14 July 2015, <https://www.techuk.org/insights/news/item/5123-hacking-team-leak>.

EU-wide self-regulation for producers of cyber-surveillance technologies, while larger enterprises thought the impact would be neutral (see Figure 7.3).

7.8.3 Introducing further multilaterally agreed list-based controls of cyber-surveillance technologies at WA level

Of the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies, three indicated that additional cyber-surveillance technologies should be made subject to export control restrictions. The suggested additions included 'Lawful Interception Systems', 'Data Retention Systems', and 'Covert mass surveillance'. The Coalition Against Unlawful Surveillance Exports (CAUSE) has highlighted a number of surveillance technologies that are not currently subject to explicit export licensing restrictions. These are 'Lawful Interception Solutions & Inter-connectors', 'Monitoring Centres & Voice Identification', 'Probes and Fibre Taps', and 'Location Monitoring'.[392]

7.8.4 Introducing an EU definition or autonomous control list for cyber-surveillance technologies (via a technical or descriptive list)

In general, government officials and industry stakeholders viewed agreeing control list additions via the Wassenaar Arrangement as preferable to making additions at the EU level.

On average, the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies indicated that adopting additional controls at the EU level would have a negative on impact on administrative costs while doing so at the Wassenaar Arrangement level would have neutral impact (see Figure 7.4). Meanwhile, adopting additional controls at the EU level would have a negative impact on the EU-wide level playing field while doing so at the Wassenaar Arrangement would have positive impact (see Figure 7.4). Member States indicated that introducing controls at the EU or Wassenaar Arrangement level would have a similar and positive impact on preventing transfers that might result in human rights violations and preventing transfers that might threaten international or EU security.

On average, respondents to the SIPRI/Ecorys company survey that identified themselves as suppliers of cyber-surveillance technologies indicated that the adoption of an EU autonomous list for cyber-surveillance technologies would have a negative impact would have a negative impact on their exports, their compliance costs, their investment and production, and the EU-wide level playing field (see Figure 7.3).

The limitations associated with this approach included:

- It may create the impression that the EU is adding items to its control list that have not been agreed via the different multilateral control regimes. This may make third countries less willing to adopt the EU control list, which may reduce the EU's ability to develop and promote its standards in export controls.

[392] 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

- It may place EU-based companies at a competitive disadvantage. This would be particularly true if the items involved were the subject of international standards, such as those agreed at ETSI, since this would increase the possibility of non-EU based companies being able to produce similar items.

However, it was also noted that the Wassenaar Arrangement's focus on dual-use goods that may be involved in the production or use of WMD or conventional arms might place limits on the type of cyber-surveillance technologies that can be added to its control list. Several stakeholders noted that non-EU Wassenaar Arrangement participants may oppose further additions of cyber-surveillance technologies to the Wassenaar dual-use control list. It was also noted that while the Wassenaar Arrangement can be an effective forum for deciding which cyber-surveillance technologies should be subject to export controls, it will not be possible to use it to agree related export criteria for human rights and/or human security.

7.8.5 Introducing an EU cyber-surveillance catch-all mechanism (via a dedicated catch-all or application of a general catch-all)

A proposal for a dedicated catch-all mechanism for exports of cyber-surveillance technologies was made by the European Parliament in October 2012 in its list of proposed amendments to the European Commission proposal to amend the 2009 Dual-use Regulation. Specifically, the European Parliament proposed the inclusion of a requirement for authorization of exports of unlisted dual-use items if the exporter has been informed by either its national authorities or the Commission that the items may be used in connection with violations of human rights, democratic principles or freedom of speech through the use of 'interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use'.[393]

On average, the ten EU Member States that responded to a questionnaire about controls on cyber-surveillance technologies indicated that the adoption of an EU catch-all clause for cyber-surveillance technologies would have a negative impact on administrative costs and the EU-wide level playing field, but a positive impact on preventing transfers that might result in human rights violation or security threats (see Figure 7.4).

On average, respondents to the SIPRI/Ecorys company survey that identified themselves as suppliers of cyber-surveillance technologies indicated that the adoption of an EU catch-all clause for cyber-surveillance technologies would have a negative impact on their exports, their compliance costs, their investment and production, and the EU-wide level playing field (see Figure 7.3).

EU Member States have experience with implementing catch-all mechanisms for items with a WMD end-use and for items with a conventional military use in connection with listed items in an embargoed destination. However, some government officials noted

[393] European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) no. 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (COM(2011)0704 – C7-0395/2011 – 2011/0310(COD)), 23 Oct. 2012.

that a cyber-surveillance catch-all mechanism would be different in nature from the WMD and embargo catch-all mechanisms. First, a significant body of knowledge has built up among exporters and regulators with regards to the items and issues covered by the WMD and embargo catch-all mechanisms. Second, exporters and regulators are dealing with a limited range of technologies and destinations. These conditions might not apply for a cyber-surveillance catch-all mechanism.

Stakeholders also noted that if there was a lack of specificity in both the technology and end-users covered by a cyber-surveillance catch-all mechanism it might make it hard to implement. This could potentially be overcome by focusing its application on a specific list of destinations, such as states subject to an EU arms embargo.

Finally, stakeholders also noted that under article 8 of the Dual-Use regulation, EU Member States are already about 'prohibit or impose an authorisation requirement the export of dual-use items not listed in Annex I for reasons of public security or human rights considerations.'[394] In effect, this article already allows EU member states to impose controls on un-listed cyber-surveillance technologies because of human rights concerns associated with their use.

The arguments raised by stakeholders in favour of a dedicated catch-all mechanism for exports of cyber-surveillance technologies include:

- It has the potential to capture exports that are of concern because of human rights or security implications, but which are not covered by a list based control mechanism.
- It has the potential to keep pace with developments in cyber-surveillance technologies more effectively than an exclusively list-based control mechanism.
- Since cyber-surveillance technologies usually market their products as being for specific end-uses and end-users, it should be possible to identify items that should be covered.[395]

The arguments raised by stakeholders against a dedicated catch-all mechanism for exports of cyber-surveillance technologies include:

- It may create uncertainty amongst industry about whether its products are covered, leading to increased compliance costs and lost revenue.

[394] 'Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items', (Official Journal of the European Union, 29 May, 2009).

[395] As a recent report noted, '(w)hile this approach suffers from enforcement difficulties, it is nevertheless still an effective means by virtue of the fact that the vast majority of surveillance technology manufacturers explicitly and exclusively sell their products to government endusers for the purposes of surveillance.' Privacy International, 'Privacy International BIS submission', [N/D], <https://www.privacyinternational.org/sites/default/files/Privacy%20International%20BIS%20submission.pdf>.

- It may lead to speculative export licence applications from companies that are unsure if their products are covered, stretching the resources of licensing authorities.

- More so than with a list-based approach, there may be differences in how it is applied among EU Member States, leading to a reduced level playing field for companies.

8. Sector case studies

As indicated in the methodology chapter, three sectors were selected for further research. These case studies provide more details on the performance of the sector, present the results of the survey for that specific sector, complemented by further explanations and additions from the in-depth interviews with business associations and companies. The following case studies have been conducted as part of this work: the machines tools sector, the chemicals sector and the aerospace sector.

8.1 Machine tools sector

8.1.1 Sector profile and importance of dual-use[396]

The machine tools industry is a key sector of modern manufacturing. Machine tools enable the production of other industrial equipment and machinery. The industry is concentrated on customised and small-scale production of high-precision machines that produce a large variety of goods from bicycles to planes, watches to computers. Part of this sector is represented by metalworking machine tools that include a wide variety of machines powered to manufacture products or parts (usually metallic but not only). Their distinctive characteristic is that they work a large variety of materials, metal in particular, to produce a required shape. There are three most common technologies: cutting machines, drilling and milling machines, and forming machines.

The machine tools sector is a SME-dominated industry and is characterized by high value machines that can cost between €100,000 to €10 million.

Based on data provided by CECIMO, the European Association of Machine Tools Industries, global production of machine tools is estimated at €58.8 billion in 2014. Big machine tool producers are China (€12.9 billion), Japan (€9.7 billion), South Korea (€4.2 billion), the United States (€3.7 billion) and Taiwan (€3.5 billion). Europe is a global leader in this key technology sector: European machine tools production increased to €19.8 (€22.9)[397] billion in 2014 from €19.7 (€22.7) billion in 2013. In addition, the EU is a leading innovator, as European SME's bring about 90% of all innovations to market. European machine tools builders therefore achieve the highest unit prices in the world.

For 2014, European machine tool exports recorded €15.7 (€18.3) billion of which 58%, €9.1 billion, were shipped outside the EU. The European machine tools industry employed about 135,000 (150,000) people in 2013 and creates approximately an additional 600,000 jobs via its supply chain.[398] The 10 dual-use products most

[396] The machine tools industry is part of the sector 'HS 84 *Nuclear reactors, boilers, machinery and mechanical appliances*', the largest sector in terms of value of extra-EU dual-use related exports (see Chapter 4). The survey results presented in this case study refer to the companies exporting dual-use products classified with the HS code 84. It should be noted that the information provided by CECIMO and the companies interviewed refers exclusively to the metalworking machine tools industry.
[397] The data in brackets is for all CECIMO members including non-EU Switzerland and Turkey, otherwise the data cover only CECIMO EU-members.
[398] Data and information provided by CECIMO.

commonly exported by CECIMO members[399] accounted for more than €7 billion in 2013, with a positive trend from 2009 (COMTRADE data).[400]

The metalworking machine tools industry, and in particular the cutting machine tools sector, is significantly affected by dual-use export controls. Among the types of technologies presented above, the cutting machine tools especially fall under the dual-use category. Of the forming machine tools, only certain hot-isostatic, isostatic presses and some very advanced forming technologies are controlled. Given that the European machine tools industry increasingly focuses on top-end and high-precision machines, nearly all European producers face export controls. Although no official figures are available, CECIMO estimates that more than 80% of the European cutting machine tools are classified as dual-use. It should be emphasized that this estimate cannot be extended to other types of machines. Even the in-depth interviews showed that the share of dual-use exports differs widely by company as this depends on the specific types of machines exported. More specifically, based on the information provided by the companies consulted, the share of dual-use products can vary from 15% of the turnover (e.g. machines for the aerospace industry) to almost 100% in the case of an industrial group producing machines for the world's largest industries.

8.1.2 Dual-use export controls - compliance issues

The types of licences

Concerning the types of licences used to export dual-use machines, companies mostly apply for individual licences as their orders are characterised by a high level of customisation and/or are not regular over time. More specifically, 48% of the companies exporting HS-84 products and all the metalworking machine tools companies interviewed, use individual licences to export dual-use items. Global licences are used only by a minority of the companies located in countries where the licensing authorities issue this type of licence. EU general licences are used by 14% of the companies exporting HS-84 products.

With regard to spare parts, most of them are not controlled but if a key component is listed, usually the whole machine requires a licence. The in-depth interviews showed that spare parts represent a minor issue when exporting, as typically companies export the whole machine and most spare parts are not classified as dual-use items.

The organization and process to obtain a licence

According to the survey results of companies exporting dual-use products classified as HS 84, 58% of these companies have a formalized internal compliance programme (ICP) and 41% an informal system. In the companies consulted and operating in the metalworking machine tools industry, the process associated with obtaining and

[399] The 10 dual-use products most commonly exported by CECIMO members are 845710, 845811, 845610, 846021, 845891, 845961, 845630, 846390, 846140 and 845730.
[400] This data comes from the COMTRADE database, not from CECIMO directly. Given the differences in data collection methods, the COMTRADE trade data cannot be directly be compared with CECIMO trade data. Production and employment data are not presented due to their limitations already presented in detail in Chapter 4

managing of licences is usually done within the company but without a formal ICP in place. However, even if not formally recognised, most of the companies have a standardised and consolidated system for checking if a licence is required and screening of all aspects of dual-use exports. More specifically, both in the SMEs and large companies consulted, the licensing procedure involves both technical experts and administrative functions. The former provide specific information on the machines as requested by the authorities, while the latter are in charge of preparing the documentation and applying for the licences. Depending on the size of the company, the sales department can also be involved in this process, notably for collecting information of the end-use of the machine.

According to the metalworking machine tool companies consulted, the procedures for obtaining a licence are not considered to be complex and preparing a licence application takes an average of 4-5 hours. The company survey reveals different results in this regard: on average companies consider the procedures to be complex and the administrative burden related to dual-use export compliance to be heavy and time-consuming.

Almost all of the companies interviewed and 50% of the companies exporting HS84 products that responded to the online survey, apply for licences electronically and significantly benefit from it compared to the previous system. In requesting the licence, the most time-consuming part of the process is collecting information on both the machines and the customers. Besides the general report or presentation on the customer, the most important document is the end-user certificate that contains all technical details of the machine and its final use. Collecting information from customers located in countries such as China, Russia and Brazil can be very time consuming, as usually customers have to follow a long bureaucratic procedure in order to provide the requested information. This part of the procedure is therefore very unpredictable in terms of timing; the length of this phase depends on the type of machines exported and on the type of customer (e.g. if the purchasing company is an intermediary that distributes to end-user companies, the documentation should include a description of both the intermediary and the final user). This information gathering could take weeks or even months and entirely depends on the completeness of the information provided by the customers. However, when the company has reliable and stable customers and the dual-use products exported do not vary significantly, the entire procedure could be considered as routine and easy to complete.

With regard to compliance issues, CECIMO underlined the need of its company members, mostly SMEs, to consult experts within the national member associations on export controls. As system complexity and variability require a constant commitment to compliance with regulatory obligations, the limited structure and availability of resources cause some problems to small machine tools builders. In this regard, in many cases national associations support companies through:

- providing information and training, and monitoring developments in international regimes;

- acting as intermediaries with local authorities;

- setting up management systems including dual-use compliance, in relation to the granting of licences; and

- checking compliance with the technical parameters of regulations.

According to CECIMO, companies try to manage the licensing internally with the support of the authorities: one of the reasons for the in-house handling is the interest to keep the know-how inside the company. The in-depth interviews confirmed that the application process is done internally.

8.1.3 Economic, social and environmental implications of dual-use export controls

The compliance costs

Compliance costs vary considerably across companies depending on the share of dual-use sales. CECIMO estimates that per company they can reach annual fixed costs of about €100,000 and about €10,000 per single licence application. One company consulted estimated that the total costs of the export control process constitute more than 1% of the total turnover.

More specifically, the costs for dual-use export controls comprise two main categories: staff costs and other costs, for example for third parties and for the ICP (software and databases). Regarding the first category, CECIMO estimates that export oriented member companies need 1 full-time employee (FTE) per 40 million of sales. More generally, almost 70% of the companies that responded to the survey declared that they have between 0.5 and 10 FTE employees in charge of dealing with the export control process and that related costs range from €1,200 to €4 million per year. The metalworking machine tool companies interviewed, both SMEs and large ones, have from 0.5 to 2 FTE employees responsible for obtaining and managing the licences.

Other costs are mainly related to training for technical staff, activities that monitor the evolution of the regulation and costs for ICPs. The companies that responded to the survey declared that costs for third parties (e.g. outsourcing and training) range from €2,500 to €100,000 per year and costs for ICPs, such as software and databases, range from €5,000 to €300,000 per year. However, for most of the companies consulted these are not applicable or constitute only a minor part of the total costs.

Finally, for the majority of the companies (80% of the survey respondents) the costs related to the services provided by brokers/freight forwarders/transporting companies have not changed since 2009 when they became subject to some dual-use trade controls, with the introduction of limited transit and brokering controls in the EU Dual-use Regulation.

The impact of export controls on competition and sales

According to CECIMO, the key elements for global competitiveness in the machine tools industry are high and durable quality, precision, productivity of machines, level of customization, training offered to customers and aftersales services. Another important driver of competition that emerged during the consultation is the price. European companies mostly compete with producers in other developed countries, like Japan, Taiwan and South Korea, mainly for high-end machines, while the main competitors for low-end machines are China, India, Brazil, Turkey and Russia. Most of the competitor countries are also the most important export-destination countries for EU producers.

According to CECIMO, distortions of competition are related to the fact that international export controls or sanctions are not uniformly applied. Some competitors are not members of (all) the international export control regimes (e.g. China), while some competitors from export controlling countries interpret the international obligations more loosely. In addition, some important competitors fail to join international sanctions that cover dual-use items (e.g. against Russia).

According to some companies interviewed, the EU sanctions against Russia show that national and regional sanctions have a substantial economic impact: countries not having similar sanctions as the EU, like Japan, Korea, Taiwan and China, have been able to significantly increase their market share on the Russian market. Russian customers are now exploring options of e.g. Chinese suppliers to substitute for European machines. Given that existing ties may now be lost, the sanctions do not only affect current exports but may also affect future exports to Russia.

In addition, CECIMO and one of the companies interviewed reported that especially smaller companies avoid doing business in certain markets, which they consider to be difficult to risky for obtaining a license. This limits the company's trade opportunities.

The dual-use machine tools from countries outside of the export control regimes (like Wassenaar and NSG) have reached the quality levels comparable to that of European producers. Therefore, the needed levels of technology are widely and easily available beyond global export control systems. This situation generates an uneven playing field for the European machine tools companies. In that sense, current definitions of dual-use machine tools in Annex I are considered to be outdated by some interviewees. They argued that, compared to 30 years ago, contemporary machines have higher performance values and therefore the precision threshold for controls should be higher.

During the consultations with companies, it emerged that there is also unfair intra-European competition. This is mainly related to the fact that there are differences among Member States in obtaining licences. One specific example was provided where a licence for the same dual-use product exported to the same extra-EU country was issued by the licensing authority in one country but could not be obtained in another Member State. Finally, based on information reported by companies, some Member

States have more efficient processes than others for obtaining licences, and it was claimed that some EU Member States applied less stringent criteria.

The in-depth interviews also brought to light some other aspects related to the obtaining of licences that can impact on competition and companies' sales. Despite the fact that the procedure to prepare a licence application can be considered rather straightforward, the licensing process is not generally considered to be predictable. For example, there are significant variations between EU Member States in terms of the time required to obtain an export licence. The interviews showed that at least one EU licensing authority has a monthly meeting to analyse the applications and to decide whether to issue the licences. Consequently, in case the licensing authorities have follow up questions on the application, the decision on the licence is taken the following month. Due to this uncertainty on the timing and the subsequent approval, the companies consulted stated that the production of customised products does not start until the licence is obtained. This is also due to the fact that the banks usually do not accept negotiating credit lines without the approved licence.

In another EU Member State companies can inform the licensing authority in order to obtain a pre-agreement. However, the stakeholders interviewed apply for the licence only once the contract with the customer is signed. This insecurity of whether and when a company will receive an export licence can lead to the cancellation of sales: some of the companies consulted indicated to have lost between 1% and 20% of deals for this reason. Another company stressed that this insecurity generates mainly economic costs linked to the waiting time and orders being placed on hold.

According to both the survey results and the in-depth consultation, in the machine tools sector, cases of licence denials are very rare, also due to the experience of the companies and the fact that many companies check the likeliness of obtaining a licence beforehand.

Finally, once the licence is issued, some companies experienced delays at customs when seeking to export dual-use items. Sometimes they are required to provide additional information regarding the dual-use products and the customers. Also, in some cases machines that are not classified as dual-use are stopped at customs (e.g. machines exported to Russia and Turkey) and companies are required to send an additional declaration proving that the machines are not listed.

The impact of the export controls on research and innovation

For the majority of the companies in this sector, export controls do not affect the capacity to innovate or the investment on R&D activities. Rather, companies consulted have their own internal research centre and develop their technology in house. Few companies collaborate with academia or research centres. In addition to this, CECIMO stressed that the export controls process is not an issue as the research network is mainly located in the EU.

The impact of production, trade and final use of dual-use items on the society and the environment

Concerning the impact of production, trade and final use of dual-use items on the society and the environment, no specific issues were raised during the consultation. The social impact of dual-use machine tools is similar to ordinary machine tools, but generally dual-use machine tools have a higher safety level and therefore contribute to socially responsible industry.

Concerning environmental aspects, CECIMO reported that the Ecodesign Directive covers machine tools. The Directive offers a possibility to develop an alternative to the regulatory measures in the form of a voluntary agreement. Taking into account the complexity of machine tools, CECIMO established a self-regulatory measure to meet the eco-design requirements. Dual-use technologies are state of the art and high-precision machines, and for this reason increase energy and production efficiency of manufacturing. One manufacturer pointed out that the increased environmental standards in the automobile industry created a requirement for more sophisticated machines. As a consequence, more machines have a dual-use potential and are therefore subject to export controls even though their sophistication is intended for a civilian use.

8.1.4 Some comments on the review options

Low value shipments/spare parts

According to CECIMO, EUGEAs for spare parts of licensable machines that have been exported would help companies to control costs and meet deadlines while ensuring the traceability of the destination and end-use. 65% of the companies exporting HS 84 products affirmed that they would benefit from an EUGEA on low value shipments, with a positive impact mainly on exports and on the level playing field.

ICP requirements

Generally, there was no particular preference in terms of legal requirements vs guidelines: the main point conveyed is that both solutions should be easy to translate into practice without adding more costs. For this reason, the EU wide legal ICP requirements should not require specific complicated procedures, IT systems or dedicated staff, as this would represent an administrative burden and cost for companies, especially for SMEs. Moreover, they should be applied uniformly among Member States to guarantee a level playing field for European companies.

8.2 Chemical sector

8.2.1 Sector profile and importance of dual-use

According to the European Chemical Industry Council (Cefic), world turnover of the chemical industry was valued at €3,156 billion in 2013.[401] Global sales grew by 2.4% from €3,084 billion in 2012. This trend was largely driven by China, where chemical sales grew from €918 billion in 2012 to €1,047 billion in 2013.

The EU chemical industry ranks second in total sales, just ahead of the United States. When including both the EU and non-EU countries in Europe,[402] total sales reached €630 billion in 2013, or 20% of world chemical sales in value terms. The total value of EU sales (€527 billion in 2013) has been continuously growing, but overall world chemical sales have outpaced that rate of growth. The EU contribution to world chemical sales between 2003 and 2013 dropped by 14.5%, from 31.2% in 2003 to 16.7% in 2013. Germany is the largest chemical producer in Europe, followed by France, Italy and the Netherlands. These four countries together accounted for 62.6% of EU chemical sales in 2013, valued at €329.7 billion. The share rises to nearly 83.6%, or €440.7 billion, when including Spain, Belgium and the United Kingdom.

The European chemical industry is an exporting industry, with exports accounting for over 80% of total sales. Exports to countries outside the EU, totalling €139 billion, account for one-quarter of its production. The EU was the leading exporter of chemicals in the world, accounting for 42.5% of global chemical exports, with Asia (incl. China and Japan) and NAFTA countries as main competitors. In terms of the value of exports, the most important destination countries (among non-EU countries) for the export of dual-use items (or products that contain dual-use items) during the last five years were the USA, Russia, China and India, according to the survey participants, which is in line with aggregate figures presented by Cefic.

Concerning the importance of dual-use exports, the majority of the companies participating in our survey declared that less than 10% of their turnover is generated by dual-use exports to non-EU countries.

In 2013 chemical companies in the EU employed a total staff of about 1.2 million, but the sector generates a greater number of indirect jobs that is estimated to be up to three times higher according to Cefic.

8.2.2 Dual-use export controls - compliance issues

The types of licences

Based on the survey results, the type of licence that is used most often (by 52% of the chemical companies that responded to the survey) is the individual licence. 21% most often use an EU general licence and 12% a national general licence. On average

[401] This section is based on data and information presented in the Cefic report 'The European Chemical Industry – Facts and Figures 2014'. In the analysis of the survey results, the chemical industry includes companies that export dual-use products classified as HS28, HS29, HS30, HS32, HS38 and HS39.
[402] The Cefic statistics also include Switzerland, Norway, Turkey, Russia and Ukraine.

the efficiency of the export control process under the latter two types of licences are considered higher than the process to obtain the individual one.

One company interviewed provided an explanation for the different results in this regard: it uses a global licence as it permits sending products up to a certain quantity instead of a single licence for every export, even if the procedure to obtain a global licence at first glance appears less time-efficient. In fact, it takes on average three months to receive the approval for a global licence, as opposed to the average time of two months for an individual one.

The organization and process to obtain a licence

Almost all companies that responded to the survey (94%) have an ICP and in more than half of the cases this is a formal programme. Consequently, the obtaining and managing of licences for dual-use items is usually done internally and with dedicated persons.

The interviews showed that in large companies this process is standardized, while in SMEs it is often more informal. More generally, according to the chemical companies consulted and as confirmed by the survey results, the administrative burden is considered heavy and time-consuming, which is mainly due to additional information often requested by the authorities. On average these companies obtain a licence in 3-4 months. The length of the procedure seems influenced by the limited staff capacity of the licensing authorities, according to some interviewees.

60% of the companies that responded to the survey can apply for licences electronically and of these, 60% significantly benefit from it. According to some companies interviewed, the introduction of the electronic procedure did not have a relevant impact on the procedure efficiency in their companies. A company stated that it could not apply for licences electronically, but would benefit if they were able to do so. In this specific case, the most time-consuming part of the application is to obtain the documents, as they need the original copy sent through postal mail and sometimes there are issues related to commercial confidentiality of the information requested from the customers. Another interviewee considered the electronic system very slow and experienced cases where the electronic application was interrupted and the authorities did not receive the information.

With respect to the global licence, one company indicated that in at least one EU Member State it cannot be extended or renewed, but once it has expired companies have to restart the procedure from the beginning.

8.2.3 Economic, social and environmental implications of dual-use export controls

The compliance costs

Compliance costs vary considerably from one company to another as they depend strongly on sales figures, product portfolio and size of the export business. The most important compliance costs are staff costs: according to the survey results, 80% of companies have between 0.1 and 12 FTE employees, while the remaining 20% have between 120 and 900 FTE employees in charge of dealing with the export control process. The related costs range from €10,000 to €1 million per year. Most of the costs of complying with dual-use export controls are related to the administrative burden associated with two phases of the licensing procedure: first, classifying dual-use items and/or checking if a licence is required; and second, obtaining licences for dual-use items. During the in-depth interviews, a large enterprise mentioned also the costs related to the screening system that is used by an external provider to check every business relation, blacklists and also credit worthiness.

71% of the chemical companies that responded to the survey declared that they face other costs related to compliance with dual-use export controls that are mainly related to ICPs (such as software and databases) and costs for third parties (including training and outsourcing). The former range from €5,000 to €100,000 and the latter from €4,000 to €50,000. Large companies interviewed reported costs for internal training, provided through on-line tools and face-to-face meetings.

The impact of export controls on competition and sales

Chemical companies are operating in a very competitive world market, above all concerning dual-use controlled chemical substances. Important competitor countries are India, China and the United States.

According to one national association, key elements for international competitiveness are predictable product availability, price, quality and delivery times. In particular, the export control process and the possibility of obtaining the licence directly influence delivery times.

According to this national association, the current dual-use export controls affect competition in the chemical sector in two ways. First, smaller companies are often not in a position to export dual-use chemicals, because of their lack of knowledge about export control procedures. Secondly, the internationally agreed control regimes are not implemented uniformly and there are different approaches to implementation by the authorities in third (non-EU) countries. This implies a lack of a level playing field, both between companies of different size and between countries.

Dual-use export controls were also indicated to have an impact on customs export procedures. It was noted that in many cases there is no clear alignment of export requirements and customs requirements for the same export. This might also cause frictions and delays in companies’ export processes.

According to the survey results, companies lose contracts (according to 70% of the respondents) or money (68% of the respondents) due to the length of time required to obtain licences for dual-use items. It should be noted that in the interviews companies indicated that the loss of a contract only happened in a few cases. The majority of the companies, 85% of the respondents, did not experience cases where they received a denial for a licence application and another EU or non-EU exporter fulfilled the deal through an identical export. The companies consulted through interviews confirmed this situation.

Concerning transport providers, chemical companies declared that since 2009 administrative requirements have increased, apparently with no added value for the control process. Since then, some transport companies have decided not to carry dual-use products. According to the companies interviewed, since 2009 transporters have required more information and specifics on the dual-use products, but this seems to have had a minor impact on companies.[403] One multinational company reported that transporters often raise their prices when they have to transport dual-use items. According to a national association, most of the forwarders have almost completely cancelled transportation into Syria and Iran However, this seems directly related to the respective sanctions, rather than the 2009 changes to the Dual-use Regulation. Another issue raised by one interviewee is that since 2009 liability lies only with the sender of a good ('Letter of indemnity') even if it is the forwarder who has the real power to influence the transport and delivery of the product, according to one interview.

The impact of the export controls on research and innovation

The export controls are considered to heavily impact on cooperation with research partners. Being a sector where innovation is considered a key driver for competitiveness, company-internal research and development, close cooperation with science/academia institutions and driving forward of innovation by acquisitions play an important role in the innovative capacity of a company.

Half of the companies stated that they work with research partners and according to 44% of that 50%, export controls are currently affecting this cooperation, mainly regarding technology transfer and exchange of samples. 40% of companies that collaborate with research partners affirm that export controls affect the innovative capacity of their companies. One company reported that goods and contents thereof require extensive checking against export control requirements during their design phase. This leads to limited possibilities and a higher degree of complexity regarding technical design and execution in certain respects. Also the intra-company technology transfers are affected, which creates difficulties in exchanging knowledge. One of the associations also indicated that currently the EU Dual-use Regulation negatively affects technology transfer for innovation projects with universities, as well as for inter-company projects (e.g. common databases and common drives to exchange knowledge).

The impact of production, trade and final use of dual-use items on the society and the environment

Most interviewees, as well as the survey results, indicated that companies, especially the big chemical ones, generally have implemented compliance management systems and 'responsible care' management systems. These systems handle several topics: from export control to corruption; from plant, process and occupational safety to

[403] Also, as explained previously, changes may be due to EU and international sanctions, for example.

environment, health and safety; and from work and social standards to human rights. All companies have environmental, health and safety units dealing with the evaluation of safe use of chemicals that includes all environmental issues, such as environmental behaviour, air pollution, waste, etc.

8.2.4 Some comments on the review options

Review issue 'Private Sector Partnership'

In view of supporting and facilitating the dual-use export procedures, the companies would benefit the most from soft law measures, such as guidelines. Nevertheless, companies affirmed that the impact of legal requirements on the level playing field would be neutral (21% of the respondents), positive (14% of the respondents) or very positive (17% of the respondents). In this regard, 6% of the companies reported that the impact would be negative or very negative and the remaining companies could not provide any answer. Moreover, according to 41% of the companies, legal requirements would have a negative or very negative impact on the compliance and adjustment costs, while 24% of the companies would expect a neutral impact on these costs and 24% a positive impact. One company interviewed, which has already developed guidelines internally, stressed the fact that they would benefit from soft law measures only if they provide short and clear information with practical examples.

Review issue 'Catch-all controls'

The most common effect of the differences in application/interpretation of catch-all controls across the EU is the legal uncertainty (44% of respondents); the impact of the degree of divergence in the way EU Member States apply the catch-all clause on companies is generally negative, above all in regard to the level playing field and the company's exports.

Review issue 'Optimisation of licensing architecture'

Most of the chemical companies would expect to highly benefit from an EUGEA for low-value shipments as it would have a positive economic impact on exports and compliance costs. During the in-depth interviews, both SME and large enterprises confirmed that they often send samples to customers and research partners and that an EUGEA for low value shipments would therefore make the licensing process more efficient. One quarter of the companies declared that they would benefit also from an EUGEA for intra-company technology transfer for R&D, with a positive impact on investment and production. This was confirmed during 50% the consultation with companies and business associations that stressed the importance of having an EUGEA for transfer of technology in the affiliated group for research and development and for other exchanges within the group.

8.3 Space sector

8.3.1 Sector profile and importance of dual-use

The aerospace sector comprises two components, namely a) the aviation sector and b) the space sector.[404] In terms of manufacturing, the aerospace sector therefore covers a wide and diversified range of activities, from the design, construction and assembling of complete aircrafts (including helicopters and spacecraft) to major subsystems (i.e. landing gear, engines) and specific electronics systems such as navigation aids and earth observation devices and technologies.[405]

A defining characteristic of the aerospace industry is that some of its leading industrial actors, such as Boeing and Airbus, are present simultaneously in the civilian and military markets; they also cater to the needs of both commercial and military aviation clients, as well as commercial and military space customers. This reflects the fact that major 'consumers' of aerospace products are public entities (ministries of defence, space agencies) as well as private actors (commercial airliners, satellites operators). Because of this double market 'anchoring', the aerospace sector, and especially its space component, is considered as one which has a very large array of dual-use applications.

Although aviation and space are generally conflated by countries' industrial classification systems into one sector, available market analyses tend to separate space activities from aviation ones: for the aviation segment, they also distinguish revenues derived from sales to military and to commercial customers.[406] According to the consultancy firm PWC, the aerospace sector has experienced five years of consecutive growth, registering record revenues of 729 billion USD (approximately 654 billion €) in 2014.[407] The central driver of this expansion is commercial aerospace, especially increasing demand in emerging economies.[408] This trend is also widely expected to continue to support increases in major original equipment manufacturers (OEMs) sales for 2015. However, PWC, Deloitte and other consultancies also note that global military demand for aerospace products has been either stable or declining, reflecting the constrained fiscal environments of major military spenders following the 2008 economic crisis.

Figures supplied by the European Aerospace and Defence Industry Association of Europe (ASD) also highlight a strong growth trend of 37.8% for Europe from 2009 to

[404] ASD-EUROSPACE,'The state of the European space industry in 2014', SIM WG Position Paper, June 2015.
[405] Chris Rhodes, David Hough and Matthew Ward, The aerospace industry: Statistics and Policy, Library of Commons Standard Note, 5 March 2015.
[406] For the space segment, lack of transparency due to the sensitivity of the activities of intelligence agencies in space makes it very difficult to assess the share of military customers in this market.
[407] PriceWaterhouseCooper (PWC), Aerospace and Defense. The year 2014 in Review and 2015 Forecast, 2015, http://www.pwc.com/en_US/us/industrial-products/assets/pwc-aerospace-defense-2014-year-in-review-and-2015-forecast.pdf
[408] India, China, Brazil are most often mentioned see: CapGemini, The changing face of the aerospace and defense industry, 2015, https://www.at.capgemini.com/resource-file-access/resource/pdf/The_Changing_Face_of_the_Aerospace___Defense_Industry.pdf

2013 for military and civil aeronautics, with an upward trend of 21.6% for space activities for the same period, for a total aerospace turnover of 149.2 billion € in 2013.[409] Considering the dynamism of the commercial aviation market, employment[410] has also been increasing in the sector and is estimated at 605,000 for 2013, up from 526,000 in 2009.[411] Estimates provided by info graphics from the World Economic Forum show world regional shares of global civilian aerospace revenues to be as follow for 2020: 33% North America, 33% Europe, 15% Asia Pacific and the rest divided equally between Middle-East, Latin America and Africa. For defence aerospace revenues, shares for North America are higher with estimated 37%, followed by Asia Pacific 12% and the rest split evenly between Latin America and the Middle East.[412]

Considering the fact that space activities are largely considered highly strategic by states for both their economic and their security interests, figures are often provided specifically for the space manufacturing industry by the ASD. The space subsector is generally broken down into three major subcomponents, namely commercial satellites (for telecommunication, for instance), launch systems and ground systems. For 2014, total revenues for this industry amounted to 7.25 billion €, and direct employment was estimated at 38,233. Sales have also been increasing at a good pace, but the rate is still lower than the one for aerospace as a whole, with 21.6% (see above).

The space manufacturing industry, embedded in the larger aerospace and defence industry, designs, develops and builds space systems (launchers, spacecraft and the related professional ground segment[413]) for public and private customers in Europe and across the Globe.

In 2014 final sales[414] worth €7.25 billion and direct industry employment amounted to 38,233 FTE. Both figures increased by 6% from the previous year. The core business of the European space industry is with European public customers, amounting to more than half of sales. Public and private European customers represent more than 75% of total sales.[415] Sales to European institutions grew by €240 million in 2014, mostly due to the European Space Agency (ESA) and national programmes including defence. Sales associated to EU programmes managed by ESA have been very slightly receding.

[409] Aerospace and defence industry association of Europe (ASD), Facts and figures 2013, http://www.asd-europe.org/fileadmin/templates/images/publications/Facts___Figures_2013.pdf

[410] National employment figures in the aerospace sector, both direct and indirect, must be considered broad estimates and taken cautiously. As they are often based on companies reported sales, the addition of sales figures by company tends to create a double, and in some instances, a triple counting of the number of jobs, therefore overestimating the total.

[411] Calculations based on ASD data

[412] World Economic Forum, Aerospace Industry Info Graphics: Flying High: Value, Skills, Jobs, 2013, http://reports.weforum.org/manufacturing-growth/aerospace-industry-infographics/

[413] According to standard definitions the space manufacturing industry does not include service activities, such as that of satellite operators (Eutelsat, Inmarsat...) or launch service providers (Arianespace). These entities are customers to the manufacturing industry.

[414] Eurospace measures industry sales to final customers invoiced in the year. This measure ensures that intermediate sales are eliminated to avoid double counting.

[415] The importance of institutional revenues can vary greatly between companies and countries. Indeed, only a few companies have significant exposure to the commercial market. They are found mostly in France, then Germany, UK, Italy and Switzerland.

Exports increased by €195 million in 2014 and were mainly directed to government programmes outside of the EU. Overall, the industry exported €397 million worth of space system parts for integration in non-European built satellites and launchers. In 2014 commercial markets were worth €3.3 billion, representing 46% of industry sales. These markets are composed of three main sub-segments:

- The commercial satellite systems segment (€2 billion), mostly composed of telecommunications systems (€1.6 billion) and, to a lesser extent, Earth observation (€0.21 billion) and scientific systems (€0.15 billion). In the commercial telecommunication segment, customers are mostly commercial satellite operators (69%) while in the commercial Earth observation and science segments, customers are mostly government entities outside Europe (66%).
- The operational launch system segment (and related industrial services at launch site - €829 million).
- The ground systems and services segment (€219 million). This includes professional ground stations and associated services, as well as specialised equipment for space systems integration and testing.

Concerning the importance of dual-use exports, 69% of the companies that responded to the survey indicated that the share of turnover generated by the export of dual-use items to non-EU countries is less than 10%. The most important destination countries in terms of value of exports during the last five years were USA and China.

8.3.2 Dual use export controls - compliance issues

The types of licences

The two types of licences used to export dual-use items are individual licence and the EU general licence. The efficiency of the export control process is considered lower for individual licences than for EUGEAs: 43% of the companies rated the efficiency of individual licences as high or excellent while all companies (100%) provided similar scores for the efficiency of EUGEAs.

The organization and process to obtain a licence

Almost all the companies that completed the survey (89%) have a formalized ICP and, consequently, the obtaining and managing of licences for dual-use items is done internally with dedicated staff. 75% of the companies can apply for licences electronically and they significantly benefit from it.

Based on the information provided by the companies interviewed, the export control process usually starts with the negotiation of the contract with the customer and the analysis of the type of licence requested to export the dual-use product. Due to the complexity of the products exported (e.g. satellites, sensors) most of the time companies have other subsidiary suppliers, typically in the EU and the USA. For this reason, the preparation of the application can involve three actors in the value chain: the suppliers of inputs, the company that produces the dual-use item, and the final users. In this case the application documents include detailed information related to all these actors. The companies consulted declared that they check the likeliness of obtaining a licence, sometimes consulting the licensing authorities, before applying for a dual-use licence and signing the contract with the customer.

Companies usually add a clause to the contracts with the customers, which makes the validity of the contract or delivery time of the product subject to obtaining an export licence.

8.3.3 Economic, social and environmental implications of dual-use export controls

The compliance costs

Two associations out of six estimate that the share of the compliance costs for dual-use export controls in total turnover at industry level is less than 5%; the others were not able to provide this information.

Three companies provided information on the number of FTE employees in charge of dealing with the export control process that range from 0.1 to 5.[416]

The costs of complying with dual-use export controls are related to the administrative burden associated with classifying dual-use items and/or checking if a licence is required and with obtaining licences for dual-use items.

Besides the cost of staff that manage the licensing process, companies face costs for both ICPs, such as software and databases, and third party costs. Companies interviewed reported two main types of compliance costs: costs for trainings and for the IT systems to make them compatible to the different IT systems used in various Member States. Moreover, they organise internal training on the EU export control regulations for all employees, even the ones not directly involved in export controls. One company interviewed stressed that after the US reform that changed the classification of many products from defence to dual-use, the staff involved in the licensing process had to invest more time on the dual-use export control process.

According to the survey results, half of the companies did not experience any changes in the cooperation with brokers/freight forwarders/transporting companies. The other half of the companies indicated that transactions have been delayed and administrative requirements have increased.

The impact of export controls on competition and sales

According to ADS-EUROSPACE,[417] in recent years competition on commercial markets in the space sector has become harsher. US competitors are challenging European positions and emerging competition (from China, Japan, etc.) is increasingly targeting the commercial markets.

[416] Companies did not provide any estimation of the costs for staff input and of other costs.
[417] ASD-EUROSPACE,'The state of the European space industry in 2014', SIM WG Position Paper, June 2015.

According to some associations representing the aerospace industry, the current dual-use export controls affect competition as they give rise to significant distortions between companies located in different EU Member States and between EU companies and third country competitors, such as the USA and India. One company reported that they experienced a case where they received a denial for a licence application when another non-EU exporter fulfilled the deal through an identical export.

The main competitors in the EU are located in France and Germany, and outside the EU the main competitor country is the USA. The competition from non-EU countries is relatively limited due to the fact that this sector is characterised by high-tech products, although this may change in the future, given the investments in the sector in several emerging economies. Companies interviewed reported that there are differences in the application process and in the length of time needed to obtain a licence among Member States, but they could not provide more information in this regard. According to a company interviewed, export controls are a key element for international competitiveness.

According to the survey results, seven companies out of nine have never experienced a denial for a licence application. Moreover, four companies out of eight have never lost a deal due to the length of time it took to obtain licences for dual-use items, two companies experienced it only on very few occasions and the remaining two experienced it sometimes or very often.

Four out of eight companies reported having lost money only on very few occasions due to the length of the process, two experienced it sometimes and one company very often. The remaining company has never lost money for this reason. Finally, six companies out of nine experienced delays at customs when seeking to export dual-use items.

Concerning the impact of export controls on investment and relocation, one company reported that it opened a plant in a non-EU country, but according to the compliance officer without being fully aware of the dual-use export control regulations that affected transfers from the EU to this specific plant. Due to export control issues (e.g. the need to obtain a specific licence for all the tangible and intangible products sent there), the company experienced delays in the production process, negatively impacting the company's business.

The impact of the export controls on research and innovation

According to ASD-EUROSPACE, technological readiness and innovation are essential for the sector to face competitors.[418]

78% of the companies participating in the survey work with research partners and academia. Concerning the impact of export controls, 29% of the companies affirm that export controls are currently affecting this cooperation and 43% state that export controls affect the innovative capacity of companies. The main reasons are related to

[418] ASD-EUROSPACE,'The state of the European space industry in 2014', SIM WG Position Paper, June 20151.

national restrictions hampering the exchange of technologies, IT access restrictions and the lack of awareness of dual-use compliance issues with respect to research and innovation. Companies indicated that export controls must be taken into account at any design level to minimize and/or avoid export constraints, which could limit product innovation in companies.

The impact of production, trade and final use of dual-use items on society and the environment

According to four associations out of six, positive effects on security result from the use or consumption of dual-use items. Three associations affirmed that the use or consumption of the dual-use items generate mainly positive environmental effects. No further specific information was obtained during the in-depth interviews.

8.3.4 Some comments on the review options

Review issue 'Private Sector Partnership'

In view of supporting and facilitating the dual-use export procedures, 88% of the companies indicated that they would benefit the most from soft law measures such as guidelines, including a list of compliance standards. The remaining companies (12%) did not know how to respond to this question. This is confirmed also by the results of the business associations' survey. In this regard, one company suggested that if there were legal requirements, it would be important that these have a strong correlation with the requirements of other relevant initiatives/regulations (e.g. the Authorised Economic Operator, AEO and Intra-Community Transfers, ICT Directive), in order to avoid inefficiencies. The impact of legal requirements would be negative on the level playing field, exports and innovation and research, but slightly positive on cooperation with research partners, compliance costs and reputational benefit, investment and production. However, according to a company interviewed, legal requirements could prevent companies from supplying goods without first communicating that these are dual-use.

Review issue 'Catch-all controls'

The most common effects of the differences in application/interpretation of catch-all controls across the EU is the legal uncertainty and distortion of competition (43% of respondents); the impact of the degree of divergence in the way EU Member States apply the catch-all clause on companies is generally negative, above all in regard to the company's exports.

Review issue 'Optimisation of licensing architecture'

Five companies out of seven would expect to highly benefit from an EUGEA for low-value shipments, with a positive/very positive impact on exports, and for intra-company technology transfer for R&D. The latter would have a general positive economic impact on companies, especially on the level playing field. The companies confirmed the importance of the introduction of these two types of EUGEAs during the in-depth interviews, especially in regard to spare parts and technologies that have no clear value. One company pointed out that the requirements for the EUGEAs differ from one Member State to another.

Review issue 'Legal clarifications/amendments'

Three out of six companies see a need for legal clarification on basic notions, control of technical assistance and control of intangible technology transfer. An interview brought to light the lack of knowledge of the company's suppliers: more clarifications, guidelines and training would help these companies reduce the risk of not complying with the export control system.

9. Conclusions

This project developed a methodology for collecting data and information to support the European Commission's impact assessment in the framework of the review of the dual-use export control system. It then undertook a data and information collection exercise and analysed these in the context of the baseline (the current system) as well as in scenarios based on the different review options, from the perspective of different stakeholders. While extensive quantitative data were gathered, the exercise clearly showed the limitations of current data, due to (a) the type of information currently collected in the private and public sector; and (b) inherent data collection challenges the diversity of sectors and actors directly and indirectly affected by the current system and potential changes. While the former limitations could at least party be addressed through changes in data collection methods and priorities, the second challenge is more complex, and underlines the very challenge of effective export controls, which can only function through effective preventive rather than punitive measures. This in turn requires the identification of all actors concerned and potentially concerned, and second an understanding on their part of the logic underlying controls. Moreover, due to the tight timeline of this project, combined with limited resources and busy meeting schedules in Member States, data could not be collected from all governments.

This summary presents key results with regard to economic, social and environmental impact of the baseline (the current system) as well as in scenarios based on the different review options.

Data and information related to economic impact

Compliance costs

The stakeholder consultations have shown that most companies have an internal compliance programme (ICP) in place, whether it is formal or informal. It also became clear that the costs related to complying with dual-use export controls do not only relate to the costs for applying for licences, but that there are also other types of costs to be considered (e.g. costs for related software and databases). The size of the costs and type of costs seem to be determined more by the size of the company rather than the sector it operates in. For example, in larger organisations with many transactions, the process of checking (potential) customers is more formalised and part of the tasks of compliance officers who sometimes buy databases or hire external organisations, while in SMEs often the sales people will collect the information on their customers. In larger organisations, especially multinational enterprises, training of internal staff is more important than in SMEs.

It should also be noted that costs can differ each year, depending on the number of transactions outside the EU, and that companies do not have information on compliance costs readily available. The in-depth interviews revealed that the figures provided in the survey are rough estimates, and in many cases are either overestimated (because export-related costs not linked to the EU Dual-use Regulation are included), or underestimated (because not all costs were taken into account, e.g.

the time of the technical and sales departments to provide information needed for the application form). These factors also explain the large variation in responses of the survey, which nevertheless provide some indication of the compliance costs.

77% of the companies declared that they have up to 10 full-time employees (FTE) in charge of dealing with the export control process and that related costs range from €500 to €4 million per year. For SMEs, these inputs are lower, as would be expected, with up to 4 FTEs with a maximum related cost of €200,000 per year.

The other costs are mainly related to aspects of the internal compliance programmes, such as software and databases, which are relevant for 88% of large companies and 68% of SMEs. Also costs for third parties, such as outsourcing and training, are relevant for 81% of the companies, with no significant differences between large companies and SMEs. In the companies that responded to the survey, the costs for ICPs (excluding staff) range from €2,000 to €300,000 and the costs for third parties from €2,000 to €100,000 per year.

Given that no details are known about the review options, we cannot quantify the effects of the different review options and the consequences will also vary considerably according to the type of company. For example, legal requirements are likely to affect larger companies less than SMEs, because their ICP is already more formalised (although both groups expect to be negatively affected). On the other hand, EU General Export Authorisations (EUGEAs) for intangible transfers of technology (ITT) are likely to reduce compliance costs more in multinational companies than in SMEs, given the general importance of product and knowledge transfers between different offices. However, we can provide some figures from the survey. With respect to introducing a legal requirement relating to the ICP, 41% of the company respondents expected this to (very) negatively affect compliance costs. The introduction of EUGEAs is considered (very) positive for low-value shipments (79% of respondents), for encryption (84%) and intra-company technology transfers (84%).

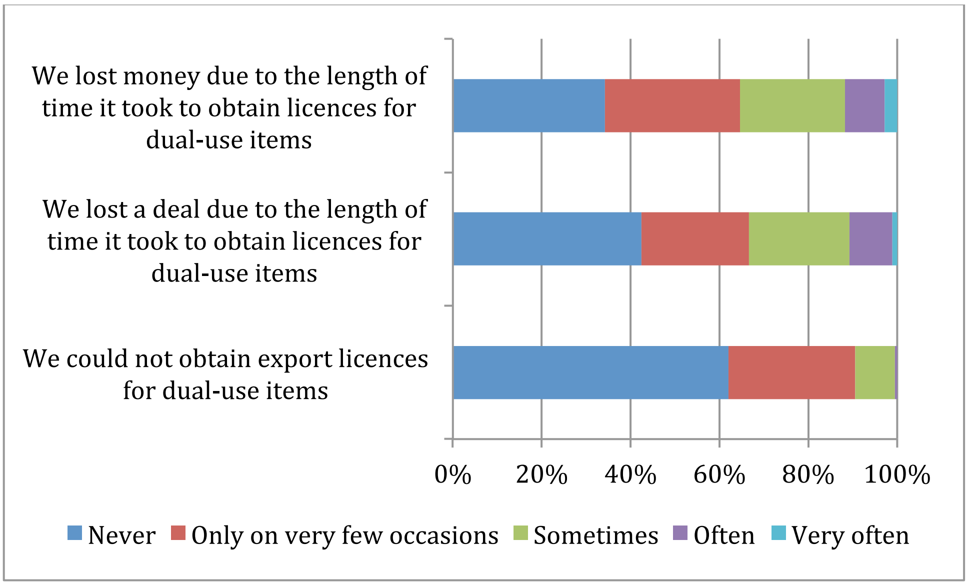
With respect to licensing authorities, the total budget of the export licensing authority (as per Art.9 of the EU Dual-use Regulation) differs a lot from one Member State to another, both in terms of total budget and the share of this budget that is spent on dual-use export controls. The budget spent on dual-use export controls varies from less than €100,000 to almost €6 million. This is likely to vary depending on the importance of the dual-use industry in each country, the extent to which these products are exported outside the EU and the number of dual-use licence applications. In line with these findings, the number of staff working on dual-use export controls also varies between Member States, although most licensing authorities have less than 20 people directly involved (either full time or part-time), Germany being the notable exception. Similarly to what we found for business, staff at licensing authorities also spend a lot of their time on activities other than issuing licenses. On average between 20% and 50% of their time is dedicated to the activity of issuing licences, including going back to applicants for more information due to mistakes or insufficient information. Other activities include, for example, providing advice, responding to pre-enquiries and information management.

Licensing authorities identified resource constraints as the biggest challenge in implementing dual-use export control. It was also highlighted that most of the review options would have implications for staff resources – in some cases positive (e.g. more EUGEAs), in some cases negative (strengthened ITT controls and enhanced information exchange between EU Member States). At the same time, some of the cost savings were expected to have a negative impact on security (see below), thus presenting a trade-off between two different types of impact which would need to be explored more fully once the details of the review options are on the table.

Competition and sales

Although compliance costs are directly affected by the Dual-use Regulation, it can also lead to more indirect costs, such as costs associated with waiting times. 66% of the respondents in the company survey indicated that they had lost money due to the length of time to obtain an export licence, while 58% of the respondents even lost a deal due to the time it took to obtain a licence. It should be noted that in general, this does not seem to happen often (see figure 9.1)

Figure 9.1. Impact of dual-use export controls on sales and competition of companies



Total respondents=177-179

Source: SIPRI/Ecorys company survey

When a company is unable to obtain a licence (which happened to 38% of the company respondents, see above), this has a direct affect on trade, and more indirectly also on production. Given that this also does not occur often, this effect is likely to be small. However, the costs associated with having your products covered by export controls are often more subtle and harder to measure than the preparing of licence applications and the issuing of denials. One industry representative noted that the most serious problem that companies face in terms of compliance costs relate to the ‘friction’ generated by the application of export controls. In particular the process of requiring customers to sign and comply with EUCs can have a chilling effect on the search for new business. Others pointed to the uncertainty generated by not knowing which markets to pursue when seeking to export your products.

The costs related to compliance with dual-use export controls can in turn also impact trade, production and investment, linked to distortions of the level playing field. The degree to which this is the case differs however, depending on the specific product and the competition from third countries. With respect to competition, it is clear that EU companies are put at a disadvantage if countries competing for the same markets have no dual-use export controls in place, both in terms of cost levels and lead times. At the same time, competition is not only determined by these factors, as issues like quality and reliability also play a key role. The more technologically advanced a product is, usually the price is less of a key determining factor for the purchasing decision. Therefore, a high-tech product that only faces competition from the United States, for example (which also has dual-use export controls for essentially the same dual-use list), will be less effected in terms of exports and production than a more standardised product that faces competition from countries with no or less comprehensive dual-use export controls (e.g. China). In our case studies, we saw examples of both the first (e.g. certain aerospace products) as well as the last (e.g. less sophisticated machine tools). It should be noted that even if price competition is important for a product, differences in costs related to dual-use export controls are likely to be smaller than for example, a difference in labour costs in the case an EU company competing with an emerging economy. Even within sectors there can be big differences depending on the specific product, and hence it is difficult to make general statements on the effect of dual-use export controls on competition and sales.

With respect to the level playing field within the EU, several stakeholders have indicated that there are differences in the implementation of the regulation between Member States. This can lead to differences in the time needed to obtain a licence or differences in the ease of obtaining a licence. In addition, the situation in which a certain type of licence (individual, national general or global) is offered also differs between EU Member States. Moreover, companies reported that in some cases a company in a certain Member State was unable to obtain an export licence, while a company from another Member State was able to do so and therefore close a deal. Overall, however, these seem to be exceptions rather than regular problems.

With respect to investment, all stakeholders interviewed indicated that dual-use export controls only play a very small role in the decision to invest (e.g. opening a plant or R&D centre somewhere), and we did not encounter any examples of relocation of production as a result of the Dual-use Regulation. On the other hand, we did encounter an example of a company opening a plant outside the EU, where according to the compliance officer, the impact of export control issues was apparently underestimated by management in the investment decision. Similar to the lack of awareness of the importance of dual-use controls among business associations, this shows that there can also be lack of awareness within companies.

A final indicator identified in the inception phase to be possibly affected by dual-use export controls is reputation. Stakeholders did not raise this as an important element. However, certain companies producing cyber-surveillance technologies did note the reputational benefits that can be generated by having products subject to export controls. In addition, it was also noted that the application of export controls can help to generate a certain amount of economic and political support should a contract need to be cancelled because of its misuse by the end-user. However, such views were far from universally shared by companies in the cyber-surveillance sector and many focused exclusively on the negative implications of being subject to controls.

With respect to the review options, there seems to be limited support for legal requirements related to the ICP, as this is expected to negatively affect exports according to 38% of company respondents, although only 6% think it will also negatively impact on reputation, production and investment. The introduction of an EUGEA for low value shipments, encryption and ITT is expected to have a positive effect on exports, production and investment and the level playing field by the majority of respondents.

Research and innovation

Half of the companies work with academia and research institutes and, according to one third of them, export controls affect this cooperation and the innovative capacity of the company. In this regard, the survey results reveal that large enterprises indicated that they are affected more often than SMEs. This can be explained by the fact that larger companies work more often with research institutes and academia outside the EU, and that intra-company transfers of dual-use items or technologies are also subject to dual-use export controls, e.g. for a company that has an R&D centre in Asia.

With respect to the review options, notably the introduction of an EUGEA on ITT or other ways to facilitate intra-company knowledge transfers is considered to have a positive or very positive effect on research and innovation by the interviewed stakeholders.

Data and information related to social impact

With respect to social impact, the main social impact is related to security and human rights. In addition to the perspectives from companies and licensing authorities summarised below, stakeholders from the academic, notably the biological sectors, also indicated a potential impact on the right to health and academic freedom.

Company perspectives on security and human rights

28% of the associations indicated that the use or consumption of dual-use items generate positive effects on security. About half of the companies that produce cyber-surveillance technologies are aware that exports of these technologies from the EU and from third countries may pose a threat in terms of security or pose a risk of human rights violations. Self-regulation, an electronic list of blacklisted customers or institutes, clear rules on modern IT infrastructure and increased clarity in legislation were considered to have a strong positive security impact.

Licensing authority perspectives on security and human rights

Security and human rights would benefit from all the review actions under the option 'implementation and enforcement support'. The actions proposed to achieve catch-all convergence would have a positive impact on security and human rights. The actions proposed to optimise the licensing architecture, such as additional EUGEAs would negatively impact security and human rights, while legal clarifications and amendments would have a general positive impact on each aspect. A critical re-evaluation of intra-Community transfers is expected not to have an impact on security, and for human rights neutral to slightly negative.

The security and human rights impacts associated with the implementation and potential expansion of controls on cyber-surveillance technologies were investigated but are – naturally – hard to quantify. There are clear cases where cyber-surveillance technologies supplied by EU-based companies have been directly implicated in serious violations of human rights and – to a lesser extent – threats to EU security. Exerting stronger controls in this area could help to reduce these risks. However, there are also security threats associated with implementing stronger controls in this area if it leads to a reduction in collaboration between EU Member States and LEAs and intelligence agencies in Africa and the Middle East.

The concrete impact of exerting stronger controls in this area will vary depending on the extent to which they are suppliers outside the EU that are willing and able to fill any gaps created by reduced supplies from EU based companies. However, the need to align standards in this area with EU policies and values in the field of human rights is an important consideration that should not be forgotten.

A significant debate is currently taking place in relation to the potential impact of controls on intrusion software. Many have argued that the controls – as currently drafted – apply to companies providing software and training on 'penetration testing' and the processes by which individuals or organisations make ICT companies aware of software 'vulnerabilities' or 'exploits'. To date, the concrete impact upon companies, researchers and academics working in IT security who believe they are subject to these controls is hard to quantify. If their fears prove accurate – or even if a mistaken perception persists that they are accurate – they could have an impact on work in the field of IT security and – indirectly – Member State security.

Employment

In addition, dual-use export controls may have an effect on employment, both in terms of compliance staff and as a result of the effects of the export controls on production. As shown above, more than three quarters of the survey respondents indicated that they have up to 10 FTEs dealing with dual-use export controls compliance. The overall employment effect from this perspective is therefore small.

The impact related to the impact of the Dual-use Regulation on production is more difficult to estimate, but also not considered to be large.

The economic burden associated with the implementation and future expansion of controls on cyber-surveillance technologies was investigated. As with all areas of the 'dual-use industry', this varies significantly depending on the technology, producer company, and licensing authority concerned. Several reports have noted that companies have left the EU as a result of stronger controls on cyber-surveillance technologies. However, the number of documented cases where this has happened remains small.

Depending on how they are drafted and implemented, several companies noted that expanded controls in the field of cyber-surveillance and the application of additional assessment criteria in relation to human rights, security or human security could create additional economic impacts. For example, a number of stakeholders noted that introducing expanded controls on Lawful Interception systems – particularly systems that that have a 'mediation function' – would potentially impact exports of communications networks, which form a significant chunk of the EUs ICT economy. Moreover, the recently introduced controls on intrusion software could have effects for companies working in IT security (see above).

Data and information related to environmental impact

With respect to environmental impacts, these are found to be largely indirect, either stemming indirectly from production or from the use of the dual-use item. Overall, these impacts were not found to be significant, although we found very few stakeholders who could provide details on this. Those that did comment often only indicated that they comply with the EU requirements in this field. Given the weak and very indirect link between dual-use export controls and environmental impact, no significant impact on the environment is expected from any of the review options.